Alma Mater Studiorum – Università di Bologna
in cotutela con University of Luxembourg

DOTTORATO DI RICERCA IN

Law, Science & Technology

Ciclo 35

Settore Concorsuale: Area 12/H3 Scienze Giuridiche

Settore Scientifico Disciplinare: Ius/20 Filosofia del Diritto / Informatica Legale

TITOLO TESI

Big Data Analysis Systems in IoE environments for Managing Privacy and Data Protection: Pseudonymity, De-anonymization and the Right to Be Forgotten

Presentata da: Emanuela Podda

Coordinatore Dottorato
Prof. Monica Palmirani

Supervisore
Prof. Monica Palmirani

Co-Supervisore
Prof. Mark David Cole

Co-Supervisore
Prof. Massimo Durante
Università degli Studi di Torino

Esame finale anno 2023

UNIVERSITÉ DU LUXEMBOURG

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

PhD-FDEF-2023-013
The Faculty of Law, Economics and Finance *Department of Legal Studies*

DISSERTATION

Defence held on 30/03/2023 in Bologna
to obtain the degree of

DOCTEUR DE L'UNIVERSITÉ DU LUXEMBOURG

EN DROIT

AND

DOTTORESSA DI RICERCA

IN LAW, SCIENCE & TECHNOLOGY

by

Emanuela PODDA
Born on 28 June 1984 in San Gavino Monreale (Italy)

BIG DATA ANALYSIS SYSTEMS IN IOE ENVIRONMENTS FOR MANAGING PRIVACY AND DATA PROTECTION: PSEUDONYMITY, DE-ANONYMIZATION AND THE RIGHT TO BE FORGOTTEN

Dissertation defence committee

Dr Mark David Cole, dissertation supervisor
Professor, Université du Luxembourg

Dr Monica Palmirani
Professor, Alma Mater Studiorum Università di Bologna

Dr Dianora Poletti, Chairman
Professor, Università di Pisa

Dr Gianclaudio Malgieri
Professor, Free University of Bruxelles

Dr Edoardo Raffiotta, Vice-Chairman
Professor, Università Bocconi di Milano

To M.G.B.

Big Data Analysis Systems in IoE Environments for Managing Privacy and Data Protection: Pseudonymity, De-anonymisation and the Right to Be Forgotten

Index

Acknowledgments

First, I would like to express my gratitude to my supervisors Professor Monica Palmirani, Professor Mark David Cole and Professor Massimo Durante for their support and guidance in this research journey, the thoughtful comments, recommendations on this dissertation and, most of everything for their patience.

I am grateful to Professor Jorge Bernardino, for his encouragement and support.

I am also thankful to my colleagues who represented a remarkable source of inspiration with their studies and ideas, during these three years. A special mention to Francesco Vigna for his constant availability in brainstorming.

I cannot forget to thank my family: my parents for their constant efforts in satisficing my wishes, my sisters, my brothers in law and, most of everything, my nieces. In particular, Sofia with the wish to inspire her the love for books and studies.

I am extremely thankful to my friends spreads over this world, who kept me busy talking when I was not able to sleep. To Grace who filled my writing breaks with laughs, giggles, and beautiful smiles.

A special mention to Giulietta, who gave me the opportunity to rest, exploring other sides of my creativity, contributing to give a new life and providing an unexpected new blooming to a forgotten flower.

Thanks to Leo, for reasons that are partly known to me and partly unknown.

Abstract of the thesis

This thesis represents the conclusive outcome of the European Joint Doctorate programme in Law, Science & Technology funded by the European Commission with the Marie Skłodowska-Curie Innovative Training Networks actions as part of the H2020, grant agreement no. 814177. The grant supports the *Rights of Internet of Everything* project conceived as a multidisciplinary investigation of one of the major technological trends, going beyond the Internet of Things (IoT) era: the Internet of Everything (IoE). In its primary definition[1], IoE is conceived as the networked connection of people, process, data, and things. The main assumption of the project is that IoE requires knowledge which is not only limited to computer science and engineering, but also includes law, social sciences, philosophy, and ethics. It requests a multidisciplinary perspective. The investigation is organised into five (5) work packages (WP): Internet of Data (WP1), Internet of Things (WP2), Internet of Persons (WP3), Internet of Healthcare (WP4) and Internet of Money (WP5).

This thesis aims to cover the legal part of WP1 (Internet of Data), focusing on Big Data Analysis Systems in IoE environments for managing Privacy and Data Protection: pseudonymity, de-anonymisation and the right to be forgotten.

It is structured in six chapters, and it is based on empirical legal research and legal analytics.

The first chapter aims to present the subject matter and the research strategy, framing the research context, and defining the research questions. Moreover, it presents the methodology of the research, defining the research method.

Chapter two presents the main characteristics of Big Data and Internet of Everything environments and investigates the challenges posed to privacy and data protection by such technologies. It defines the legal framework in force, discussing the meaning of identification and the consequent issue of de-anonymisation/re-identification, in light of Article 17 of the General Data Protection Regulation (GDPR) that grants the right to erasure (*right to be forgotten*). The chapter elaborates on the impasse created by Art. 17 in force and the issue of de-anonymisation, as due to technological development, coordinating law with reality becomes challenging. Therefore, it presents an explorative literature review on the issue of de-anonymisation/re-identification, discussing the technological development of such issue.

[1] Cisco and Qualcomm where among the first companies providing a definition of Internet of Everything. As references: https://www.cisco.com/c/dam/en_us/about/business-insights/docs/ioe-value-index-faq.pdf ; https://www.qualcomm.com/news/onq/2015/05/13/internet-everything-works-everyone

This chapter lays the ground for an objective and subjective analysis on the feasible level of data anonymity in the light of the issue of data de-anonymisation/re-identification, respectively presented in Chapter three and Chapter four.

The Chapter three investigates the issue from an objective perspective, questioning on the meaning of identification and re-identification on a semantic level, as defined in the GDPR and in the Free Flow Data Regulation (FFDR). Starting from the main difference above which the whole legal system on data flow is built, personal data and non-personal data, the chapter questions how to grant anonymity relying on the data processing models introduced by the GDPR: anonymisation and pseudonymisation. The analysis is carried out considering not only the interaction between GDPR and FFDR, but even in the light of the new regulation on data governance, the Data Governance Act (DGA).

The Chapter four explores the issue from a subjective perspective, focusing on how to grant data anonymity with the proliferation of roles and responsibilities among stakeholders involved in the processing and reuses of data. Analysing the different models proposed in the DGA, it investigates the span of the de-anonymisation/re-identification issue in data reuses as framed in the DGA, considering the main technological novelties introduced by the new regulation. In addition, it briefly explores the dialectic tension between the general interest in DGA and the public interest in the GDPR.

The Chapter five presents a legal empirical observation of the data de-anonymisation spectrum in further data processing and data sharing, providing empirical evidence on the reasonability of the in-force art. 17 of the GDPR in the light of the legal framework, considering the forthcoming implementation of the DGA and Data Spaces.

Finally, the Chapter six presents the conclusions of the thesis.

List of Acronyms and Abbreviations

CHF Cryptographic Hash Function

DGA Data Governance Act

DP Differential Privacy

FFDR Free Flow Data Regulation

GDPR General Data Protection Regulation

IOE Internet of Everything

IOT Internet of Things

M2M Machines to Machines

MAC Message Authentication Code MAC

NSI National Statistical Institutes

P2M People to Machines

P2P People to People

RNG Random Number Generator

SDC Statistic Disclosure Control

SMC Secure Multiparty Computation

List of figures

Chapter 1. *Subject Matter and Research Strategy*

Chapter Index

Short Abstract of the Chapter

This chapter presents the research framework, providing the research background and explaining its main legal premises. The methodology and methods of the research are then presented, which is further supported by an empirical legal observation of technological development on the risk of de-anonymisation/re-identification.

1.1. Research Context

The thesis investigates the *Rights of Internet of Everything* (IoE), conceived as a multidisciplinary perspective of one of the major technological trends going beyond the ongoing Internet of Things (IoT) era [1]. In its primary definition[2], IoE represents an interconnected world, a networked connection of people, process, data, and things.

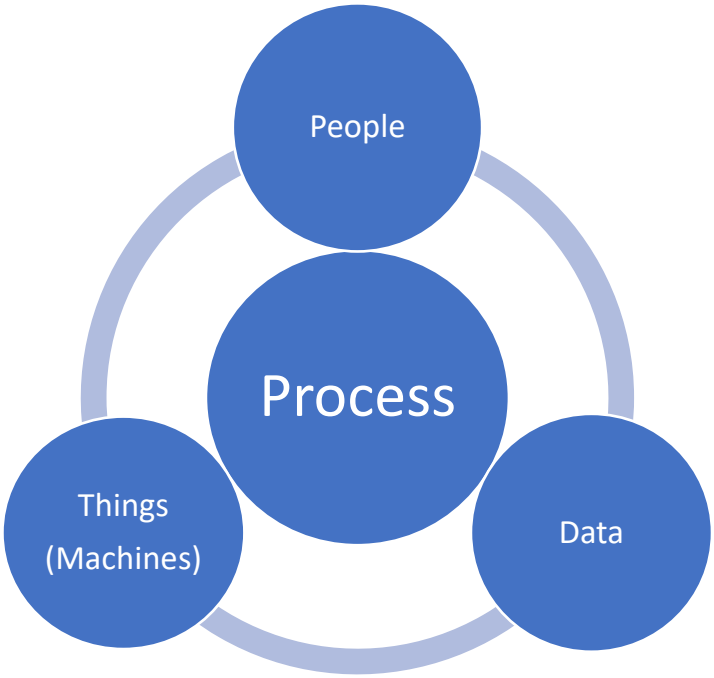


Fig. 1. Internet of Everything (IoE) connecting People to People (P2P), Machines to Machines (M2M) and People to Machines (P2M) relying on Big Data Analytics and granting Knowledge Processes

IoE represents a new paradigm in data processing, extracting, and analysing real-time data collected from heterogeneous sources [25]. Despite the unquestioned potential of IoE, few issues and challenges have been identified, especially regarding insights about the knowledge process [2–4]. This generates the need to design and implement appropriate IoE environments, from the initial phase [5], investigating the relationship between data, information, and knowledge. IoE represents a source of data allowing its processing, analysis, and reuses, to

[2] Cisco and Qualcomm were among the first companies to provide a definition of Internet of Everything. As references: https://www.cisco.com/c/dam/en_us/about/business-insights/docs/ioe-value-index-faq.pdf ; https://www.qualcomm.com/news/onq/2015/05/13/internet-everything-works-everyone

discover patterns, as well as to infer information. In the IoE, the network captures data related to individuals, as nodes of the network connected with non-human objects, like sensors and actuators. As such, from a mere legal point of view, the network captures data related to individuals which, by legal means, are considered personal data as defined in art. 4 of the General Data Protection Regulation[3] (GDPR) like *any information related to an identified or identifiable natural person*.

De facto, according to the European legal framework in force, data management requires the nature of data to be assessed to consequently identify the rules to be applied. While non-personal data can freely flow in the Digital Single Market, personal data can flow provided that some conditions are met. The GDPR imposes certain requirements and limits the free circulation of personal data. Only if the processing grants *anonymity*, thus impacting the nature of data, changing it from personal to non-personal, such requirements and limits no longer apply and the GDPR becomes no longer applicable, giving way to the Free Flow Data Regulation[4] (FFDR).

However, the border line between anonymity and identifiability introduced in the GDPR, albeit in its non-compulsory part, in *Recital 26*[5], seems uncertain and unclear [6, 7]. Moreover, in line with the accountability principle, the GDPR does not request any specific control, or audit on the anonymous nature of data for allowing further processing. As anticipated, anonymised data will fall outside of the scope of the regulation, provided that personal data are rendered *anonymous in such a manner that the data subject is not or no longer identifiable*.[6]

[3] Regulation (EU) 2016/679 of the European Parliament and Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[4] Regulation (EU) 2018/1807 of the European Parliament and Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union.

[5] Recital 26 of the GDPR states: "*The principles of data protection should apply to any information concerning an identified or identifiable natural person.*
Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person.
To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly.
To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.
The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.
This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes."

[6] See Recital 26 of the GDPR.

Therefore, the importance of exploring this field lies in the growing need to ensure data re-uses without sacrificing privacy and data protection.

In recent decades, the most traditional technical approach for rendering data anonymous has been anonymisation. It stemmed from the statistical community with the establishment of National Statistical Institutes (NSI), but recently, it has been proven that such an approach does not work effectively in many cases [8–11]. However, the GDPR still recalls it with pseudonymisation, as one of the two models for granting compliancy while protecting data and privacy of the data subjects.

In this sense, current trending topics in the field mainly investigate new technologies for granting data anonymity, allowing sharing and reusing, or eventually developing new models and methods that are able to measure information loss, quantify and measure the grade of anonymity.

Among the first, mainly investigated by the computer science communities, we can name blockchain technology [12], federated learning [13], and secured multiparty computation [14]. The scientific communities welcome these technological novelties with enthusiasm; however, they are subject to obsolescence. Moreover, as said, it should be taken into account that even the technological environment that these technologies rely on are in constant evolution, challenging their limits and potentials.

Among the second, mainly investigated by the statistical and mathematical communities, are some projects based on new models of anonymisation, which test the output of anonymised dataset, measuring the efficiency and extent of anonymisation[7].

From a mere legal point of view, tumultuous legislative activity in the digital field provides a dynamic ground. On one hand, it confirms that anonymisation is not a totally reliable model for protecting data [15] or for safeguarding people' privacy, while on the other believing that a feasible trade off can always be reached [16], especially if combined with a context-dependant evaluation [17].

This situation can be considered as characterised by techno-legal uncertainty: if on one hand it grants a certain flexibility in reusing data, on the other hand, it represents the root of many risks in the context of data protection and privacy.

Among these, the thesis aims to specify the investigation of the risk of *de-anonymisation*/*re-identification*, considered as the possibility of matching anonymous data (de-identified data,

[7] Among the projects: https://amnesia.openaire.eu/ ; https://arx.deidentifier.org/

thus processed personal data) with other available auxiliary data (publicly or privately available) [18, 19]. It is a risk mainly inherent to data sharing and data re-uses, implying appropriate designs of data governance for granting security and protection of data.

Such a risk is mentioned in Recital 9[8] of the FFDR, considered as the possibility of matching anonymous data (de-identified data, thus processed personal data) with other available auxiliary data (publicly or privately available). This practice is made possible using modern technologies such as Internet of Things, Artificial Intelligence, and Machine Learning.

In this regard, the legal approach to technological development is mainly based on soft law, relying on non-binding tools to prevent a hindrance to innovation.

Therefore, granting privacy and data protection in the IoE environment becomes challenging. In this sense, the European legal framework recalls a linear reality - *requesting to assess the nature of data referring to personal and non-personal data* – which, in practice, appears to be remarkably difficult to ascertain.

Data has a physiological nature to be streamed, processed, shared and re-used, thus its processing constantly impacts its nature. Moreover, it must be said that the de-anonymisation risk can pertain not only to processed personal data, but also to mixed datasets composed of both personal and non-personal data.

In keeping these premises, the thesis aims to investigate the de-anonymisation/re-identification risk in the evolution of the data policies and legislations proposed by the European Institutions. It focuses on the need to not sacrifice the potential of data sharing and data re-uses, unlocking the potential of *big data*, and analysing the tension between privacy and data protection posed by the risk of de-anonymisation/re-identification.

As a case study, the thesis provides a legal empirical observation on the technological development behind such risk, questioning the extent of the currently in-force art. 17 of the GDPR, the right to erasure (*right to be forgotten*).

Investigating the tension between data protection and privacy on the one hand, and the need to grant further uses of processed personal data, the thesis out lines the technological development of the de-anonymisation/re-identification risk, with an explorative literature review. After

[8] Recital 9 of the FFDR states: "*The expanding Internet of Things, artificial intelligence and machine learning, represent major sources of non-personal data, for example as a result of their deployment in automated industrial production processes. Specific examples of non-personal data include aggregate and anonymised datasets used for big data analytics, data on precision farming that can help to monitor and optimise the use of pesticides and water, or data on maintenance needs for industrial machines. If technological developments make it possible to turn anonymised data into personal data, such data are to be treated as personal data, and Regulation (EU) 2016/679 is to apply accordingly.*"

acknowledging its extent, it questions whether a certain degree of anonymity can still be granted, focusing on a double perspective: an objective and a subjective perspective. The objective perspective focuses on the data processing models *per se*, while the subjective perspective investigates whether the distribution of roles and responsibilities among stakeholders can have a role in ensuring data anonymity.

The objective perspective investigates the models of data processing as regulated by the GRPR, namely anonymisation and pseudonymisation. It frames the state of the art in the evolution of these data processing models and the degree of anonymity recognised by the various scientific communities (as anticipated, e.g. statistical, computer science). According to this perspective, it questions the relations between the traditional binary category of *anonymisation/irreversibility* and *pseudonymisation/reversibility*. In this sense, a new studied approach based on pseudonymity is introduced, discussing a new paradigm of data protection and privacy, still based on the semantic legal dichotomy between personal and non-personal data[9].

Conversely, the subjective perspective investigates whether a certain degree of anonymity can eventually be granted, relying on the proliferation of roles and responsibilities among stakeholders, analysing data governance models and especially in Government to Business (G2B) data sharing. In this investigation, the focus is on the European Data Governance Regulation COM/2020/767[10], the Data Governance Act presented as a natural evolution of the data policies in data flow.

To this end, the thesis investigates the legal framework that has been in force since 2018[11] when, confident of having settled the main ground for the protection of citizens' rights with the GDPR, the European Commission began to brainstorm new models of data sharing. In 2020, with the Data Strategy[12], it stressed a main *subjective* point, highlighting that "*Citizens will trust and embrace data-driven innovations only if they are confident that any personal data sharing in the EU will be subject to full compliance with the EU's strict data protection rules".*

A decade ago, [20] data governance was perceived and understood to be control over and management of data, connoted by a mere internal interest, as a company task granting clarity

[9] In this sense: http://infolegproject.net/

[10] https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52020PC0767&from=EN

[11] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2018:0232:FIN

[12] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European strategy for data, Brussels, 19.2.2020, COM(2020) 66 final.

of information. This concept has evolved over time and the literature has investigated a more holistic perspective [21]. Nowadays the concept *encompasses the entirety of transnational and trans-organisational data flows, from the macro-level of nation-states to the micro-level of citizens* [22]. Therefore, in the modern context, data governance can be organised differently, depending on the interests of the stakeholders involved.

The legal evolution in the technological domain is mainly based on soft law [23], mainly relying on non-binding tools for avoiding suffocating innovation. European legislation is mainly based on several hard law corpuses and on many soft laws [24]. This approach is aimed at avoiding overruling a sector, such the technological one, which is in constant development and in need of freedom in order to innovate. Moreover, traditional governance structures are becoming more difficult to impose, due to the ubiquitous nature of technology, as well as the ubiquitous nature of data. While fostering innovation linked to granting a certain freedom in the sector, such freedom might clash with other citizens' rights, with their fundamental rights.

Certainly, the increasing availability of data is impacting our societies and our economies, developing data-driven societies and data-driven economies. Every aspect of modern life is represented by data, allowing information to be derived from any kind of activity in the world - human and non-human - *captured* by the digital environment. With the increase of connected devices, the human presence – *per se* – will be captured by the digital environment and *datified.*

Regarding the need to investigate feasible policies in data governance, and overcome the initial perspectives on data ownership, the European legislator has refined traditional concepts of data access and data sharing for granting re-uses beyond the initial purpose of collection, and introducing the new legislation on Data Governance. Regulating the management of data and its availability, by increasing trust in data intermediaries and strengthening data-sharing across Europe and beyond, has impacted the research trend.

This thesis highlights the fragmentation of the topic, prior to the proposal presented in 2020: some publications addressed it with a specific focus on data quality, data security and data lifecycle year [21, 25, 26], while others focused on a review of the existing literature [21, 25, 27, 28]. Recently, the focus changed in favour of the balance between trust and accountability in developing new models of data governance, not only compliant with the GDPR but with technological development [22, 30–33]. In this regard, this research shows that a decade ago [20], data governance was perceived and understood as control over and management of data, connoted by a mere internal interest, as a company task granting clarity of information. This concept has evolved over time and academia has investigated a more holistic perspective,

referring to a concept which *encompasses the entirety of transnational and trans-organisational data flows, from the macro-level of nation-states to the micro-level of citizens* [26, 29]. Therefore, in a modern context, data governance can be organised differently, depending on the interests of the stakeholders involved.

Finally, the last part of the thesis proposes an empirical observation of the de-anonymisation issue, as recalled in the main document on anonymisation, the Working Party 29 Opinion 05/2014 on Anonymisation Techniques, strictly dependant on the legal dichotomy between personal and non-personal data. Using this approach, the thesis aims to perform an empirical observation of the semantic difference between personal and non-personal data broadening the perspective on the issue of de-anonymisation/re-identification, regardless of the infrastructure used.

Therefore, after analysing the extent of the de-anonymisation risk, the research aims to investigate the grounds on which the entire European system is built, namely the GDPR and the FFDR, which introduce the main semantic differences between personal data and non-personal data. In line with this premise, it questions the nature of data in the further uses of data and especially data sharing in Government to Business, as introduced in the new legislation on Data Governance. Overall, the thesis aims to evaluate two linked and underpinned vulnerabilities of the whole legal system regulating data flow in the Digital Single Market: the semantic difference between personal and non-personal data in granting anonymity, and the consequent issue of de-anonymisation in light of the right to erasure *ex* art. 17 of GDPR as a citizens' right granting anonymity.

The main new factor of the thesis is an empirical evaluation of the de-anonymisation/re-identification risk linked to identification and the right to be forgotten, as empirical legal studies on the topic are lacking. Moreover, in line with the last EU research foresight[13] the thesis prepares the ground for the future research and innovation policy, confirming that 2020 opened a transitional period based on the Digital Turn. Such change, where the dependency on technology is rapidly growing, imposes a multifaceted approach and a multidisciplinary perspective of the future challenges posed by technology, highlighting the importance of social sciences and empirical studies.

The need to develop new approaches for overcoming this issue is increasing over time, relying especially on perspectives which are not exclusively and purely technological, or legal, but is

[13] European Commission: After the new normal: Scenarios for Europe in the post Covid-19 world (2022).

a multidisciplinary approach which considers technology as the main basis to be observed reality.

1.1.1. Research Question

The research will be organised into two main questions and their sub-questions.

The first main question is the following:

- RQ1: In light of the increasing risk of de-anonymising data, turning non-personal data into personal data, are the two mutually exclusive definitions of personal and non-personal data relevant in tackling such a risk?

  This first question will be empirically researched, investigating the following sub-questions:

- RQ1.2: How does this semantic difference stands out in worldwide continental jurisdictions, in the research and development of de-anonymisation techniques based on singling-out, linkability and inference (as namely advised in the WP29 05/2014)?
- RQ1.2: How has the de-anonymisation issue evolved over time and what is the correlation between time and continental jurisdictions?

The second main question is the following:

- RQ2: How can the de-anonymisation risk be tackled from both an objective perspective (namely with reference to *privacy models*, *statistical disclosure control* and *encryption*) and a subjective perspective (with reference to the data governance models, especially G2B)?

The second main question leads to the following sub-question:

- RQ2.1: In light of the level of anonymity that data processing and data sharing can ensure, can the right to be forgotten still represent a remedy against the harmful disclosure of personal information?

1.2. Methodology

The research methodology is based on the merging of two methodologies: qualitative and quantitative.

The qualitative methodology relies on an analytical approach used for analysing all relevant European legislation in data flow. The analysis focuses on the main rules and principles to frame and investigate the risk of de-anoymisation/re-identification in modern digital environments, with a particular interest in legal terminology stemming from the *corpus* of the GDPR and the FFDR, namely referring to the concept of anonymous data and how to grant data anonymity for tackling the investigated risk. This approach develops a description of the processing from two different perspectives: one objective and the other subjective. The objective perspective explores the legal extent of terms relating to data processing, such as anonymisation and pseudonymisation, theorising on the extent of data anonymity. The subjective perspective explores the possibility of granting data anonymity, focusing on the proliferation of roles and responsibilities of the stakeholders involved in data processing, sharing, and reusing.

The qualitative methodology explains, interprets, and understands the issue of de-anonymisation/re-identification from a theoretical point of view, applying the rules and principles in force governing dataflow. Moreover, it sets the ground for the quantitative methodology, ensuring a further investigation of the de-anonymisation/re-identification risk from a practical perspective. The quantitative methodology is developed on the outcome of the qualitative one, performing a statistical analysis on the main premise of the thesis, the de-anonymisation risk in its global extent first of all, and secondly recalling the Working Party 29 Opinion 5/2014 on anonymisation techniques.

Merging both qualitative and quantitative methodologies aim to formulate the proposal of possible solutions to a real-life problem that require an action or policy decision, after an empirical observation of said problem.

Therefore, the research is built on the design of an empirical research which involves:

1- Defining the research questions
2- Theorising and extracting observable implications from the theory
3- Identifying rival hypothesis
4- Proposing solutions

1.2.1. Methods

The main method of the research is based on empirical legal research, involving a research design that relies on the collection of the relevant legal-tech terminology.
The research is focused on a systematic literature search in *Arxiv*, performing an explorative network analysis of keyword co-occurrences and a content analysis of these publications.
This approach allows an empirical observation of the technological development of the de-anonymisation/re-identification risk. A statistical analysis will be performed on the outcome of data collection, relying on a designed codebook [30] hereinafter described.

1.2.2. Codebook

The empirically searchable empirically searchable research question is the first one listed in the specific session, and its sub-questions above.
The empirical legal study is supported by the following main theory. Market and technological developments of Internet of Things, Artificial Intelligence and Machine Learning applications rely on a conspicuous set of data, which may comprise both personal and non-personal data. This situation expands the possibilities of de-anonymising data thus, the possibility of transforming non-personal data into personal data.
To this extent, art. 8(1)(a) of the FFDR namely establishes that *No later than 29 November 2022, the Commission shall submit a report to the European Parliament, to the Council and to the European Economic and Social Committee evaluating the implementation of this Regulation, in particular in respect of the application of this Regulation, especially to data sets composed of both personal and non-personal data in the light of market developments and technological developments which might expand the possibilities for de-anonymising data.*

The legislator explicitly recognises that processing personal data as *input* may not necessarily lead to non-personal data as *output*. Therefore, neither data quality nor security can be totally ensured, unleashing potential misuses and abuses in secondary uses of processed personal data.

The whole legal regime ruling data circulation is anchored to two mutually exclusive definitions: personal data and non-personal data. *Ex* Art. 4(1) of the GDPR[14], Personal Data is *any information related to an identified or identifiable natural person*, while *ex* Art. 3(1) of the FFDR[15], Non-Personal Data is *data other than personal data as defined in point (1) of Article 4 of the GDPR.*

As such, the *nature* of data determines the legal framework and the rules to be applied: while non-personal data can flow freely in the Digital Single Market, personal data can circulate provided that some conditions are met.

However, data processing, circulation and re-use naturally imply a change in the nature of data. Moreover, as anticipated, most of the time datasets are combined by both personal and non-personal data thus, ascertaining the nature of data and consequently the legal framework to be applied may be extremely complicated.

This difficulty has even been explicitly recognised by the European Commission[16] concluding that, in mixed datasets if the non-personal data part and the personal data part are '*inextricably linked*' the data protection rights and obligations stemming from the General Data Protection Regulation fully apply to the whole mixed dataset, also when personal data represent only a small part of the dataset. Despite that, the protection risks being merely fictitious due to the fact that personal data processing does not necessarily lead to non-personal data.

Coordinating law with reality is not easy and such open standards create legal uncertainties, especially as there is a total lack of *ad hoc* controls on the nature of data.

The main example of this uncertain scenario concerns anonymisation. The legislation in force recalls anonymisation as data processing able to determine a change in the nature of data: the *input data* (personal data) undergoing anonymisation leads to anonymous data as *output data* (thus, non-personal data). Consequently, data which have undergone a process of anonymisation fall outside the scope of data protection legislation, as they are considered

[14] Regulation (EU) 2016/679 of the European Parliament and Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[15] Regulation (EU) 2018/1807 of the European Parliament and Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Free Flow Data Regulation).

[16] Communication from the Commission to the European Parliament and the Council, Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union COM/2019/250(final).

anonymous data, not related to an identified or identified natural person. Eventually, as recalled in a non-binding part of the GDPR - Recital 26, *to ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.*

The objectivity of these factors is certainly questionable, especially in the global context. Case studies and research publications have shown how difficult it is to create a truly anonymous dataset [8][17] [31][18] [32][19] [33][20] [34][21].

This premise makes anonymisation one of the most controversial topics discussed in legal-tech literature, as the assessment of whether data is properly anonymised depends on specific and unique circumstances of each individual case.

It must be said that the legislation in force does not provide any specific check or control to confirm and assess this change in nature; nor is a *prescriptive* standard determined for anonymisation processing. There is a remarkable need to ethically audit data processing, ensuring not only the protection of data but also the quality of data.

The sole institutional reference to anonymisation stems from Opinion 05/2014 issued by the Working Party 29 (WP29) on Anonymisation techniques[22], although it is non-binding. In this Opinion, the WP29 *analyses the effectiveness and limits of existing anonymisation techniques against the EU legal background of data protection and provides recommendations for a cautious and responsible use of these techniques to build a process of anonymisation.*

The WP29 stresses the inherent risk in anonymisation, which has to be considered in assessing the validity of any anonymisation technique. Here it advises testing the effectiveness and limits of each anonymisation technique against three main criteria:

- Singling-out (it is still possible to single out an individual)
- Linkability (it is still possible to link records relating to an individual)

[17] It was demonstrated that the governor of Massachusetts could be re-identified from de-identified medical data by cross-referencing the de-identified information with publicly available census data used to identify patients.
[18] In 2009, Netflix released an anonymised movie rating dataset as part of a contest, and researchers successfully re-identified the users.
[19] In 2013, another study, conducted on anonymised cell phone data, showed that "*four spatio-temporal points are enough to uniquely identify 95% of the individuals*".
[20] In 2017, researchers released a study stating that "*web-browsing histories can be linked to social media profiles using only publicly available data*".
[21] Recently, studies have shown that de-identified data was in fact re-identifiable, and researchers at UCL in Belgium and Imperial College London found that "*99.98% of Americans would be correctly re-identified in any dataset using 15 demographic attributes*".
[22] Opinion 05/2014 on Anonymisation Techniques Adopted on 10 April 2014.

- Inference (information concerning an individual can be inferred).

Therefore, an effective anonymisation solution should *prevent all parties from singling out an individual in a dataset, from linking two records within a dataset (or between two separate datasets) and from inferring any information in such dataset*.

The main objective is to contain the risk of de-anonymisation which may prevent other correlated risks (e.g. profiling).

The empirical study aims at observing the technological development of the de-anonymisation issue from a legal perspective, considered as the possibility to turn non-personal data into personal data.

As a main reference for performing this observation, the three criteria listed by the WP29: singling out, inference, linkability, are used as words for filtering the papers published in an Open Access repository: Arxiv (https://arxiv.org/).

The observation will be performed over a span of 6 (six) years, from 2016 (data in which the two main regulations ruling on data flow entered into force) until 2022.

For each paper a number of 6 (six) variables (quantitative and qualitative) will be observed:

1. Year of publication in the timeframe 2016 to 2022 (transition period from the Directive 95/46/CE to the GDPR EU 2016/679).
   Qualitative Variable.
2. Jurisdiction (author's jurisdiction based on affiliation) as EU, US, Asia, Africa.
   Qualitative Variable.
3. De-anonymisation risks/technique as singling out, linkability, inference.
   Qualitative Variable.
4. The nature of data used for performing de-anonymisation as personal data (1), non-personal data (2), mixed data (3).
   Qualitative Variable.
5. The number of publications.
   Quantitative Variable.
6. The number of publications compared with the year of publication.
   Dummy Variable.

If the theory is correct, the empirical study would show whether the semantic difference - introduced by the legislation as a main filter of data protection - has an impact on the issue and risk of data de-anonymisation.

The observation of the variable concerning authors' jurisdiction may/may not eventually confirm that the semantic difference has/has no impact on tackling and containing the risk of de-anonymisation.

a) Outlining how the concepts can be measured

Selection of papers on de-anonymisation (by singling-out, linkability, inference) using an open access repository. A text analysis on each paper will be conducted, collecting the above-mentioned information.

b) Identifying the values of the measures

Variable n.1: 2016 to 2022

Variable n.2: Europe (1), America (2), Asia (3), Africa (4)

Variable n.3: Singling-out (1), Linkability (2), Inference (3)

Variable n.4: Personal Data (1), Non-Personal Data (2), Mixed Data (3).

Variable n.5: number of published papers

Variable n.6: relationship between the number of papers and the year of publication to observing whether implementation of the GDPR has generated an increase in the paper publications. Dummy variable as No (0), Yes (1)

The combination of qualitative and quantitative variables will allow a statistical analysis of the outcome to be performed.

c) Evaluating measures and measurement methods

c.1. Reliability

The nature of data, as indicated in the legal regulations (GDPR & FFDR), will allow the paper to be legally categorised. There may be a lack of reliability in the textual analysis as interpretation of the rules may prove challenging in some borderline cases.

c.2 Validity

As above: the nature of data as indicated in the legal regulations (GDPR & FFDR) will allow the paper to be legally categorised. There may be a lack of reliability in the textual analysis as interpretation of the rules may prove challenging in some borderline cases.

d) Data Collection

d.1 Target population

The analysis will be carried out by collecting and indexing papers published in one OpenAccess publications repository (*arxiv*) referring to the following keywords:

- Singling-out

- Linkage
- Inference

The observation period spans from 2016 to 2022.

d.2 Locating data

The dataset will be created based on the data collected in the previously mentioned OpenAccess publication repository and saved in the OneDrive belonging to Alma Mater Studiorum – Università di Bologna (shared file with main supervisor Professor Monica Palmirani)

d.3 Generating Data

The collection of data will be conducted using the following keywords:

- Singling-out
- Linkage
- Inference

Each paper that contains at least oneof these keywords should be included in the dataset.

A classification of the papers will then be conducted to grasp possible future relations and insights.

The parameters observed will be:

1 – year of publication
2 – continental jurisdiction (author's jurisdiction based on affiliation)
3 – nature of the data used for de-anonymise
4 – de-anonymisation risks/techniques as singling out, linkability, inference
5 – number of publications
6 – number of publications compared with the year of publication

d.4 Amount of data to be collected

The dataset will include all the data collected for the timeframe spanning from 2016 to 2022.

e) Coding, Analysing and Communicating results

The research will be based on both quantitative and qualitative data.

Therefore, both inductive and deductive coding techniques will be applied.

1.1 exhaustivity of variables' values

N/A

1.2 mutual exclusivity of variables' value

N/A

The collection of data using the above-mentioned parameters and observing the different variables will allow mainly exploratory data analysis and statistical analysis to be performed, using an Open-Source Data Analytics Platform: *Knime* https://www.knime.com/

The communication of data and results will be part of the penultimate chapter of the thesis, including graphs on statistical analysis for representing data after observation.

Chapter 2. *Governing Data Collected through Datafication: an Objective Perspective*

Index of the Chapter

Short Abstract of the Chapter

This chapter presents an objective perspective on the issue of deanonymisation.
Specifically, it investigates whether a certain degree of anonymity can be granted relying on the two main data processing methods considered by the GDPR: anonymisation and pseudonymisation.
It shows the state of the art of such data processing, investigating the extent of the anonymity they can grant.

2.1. The Represented Linear Reality of Personal Data and Non-Personal Data in the European Data Flow

The European data flow relies on a represented linear reality of personal and non-personal data, anchored to two mutually exclusive definitions.

These concepts are established into two different bodies of legislation:

- *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation),* hereinafter referred as GDPR
- *Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union,* hereinafter referred as FFDR.

These regulations introduce the main difference between personal and non-personal data, defining the rules for ensuring a proper data flow within the European borders and outside those borders. According to this framework, personal data is regulated by relying on a higher level of protection, while non-personal data can flow freely in the digital environment.

Therefore, ascertaining the nature of data is of paramount importance to determine the regulation and rules to apply: data taxonomy becomes crucial.

Art. 4(1) of the GDPR defines 'personal data' as "*any information relating to an identified or identifiable natural person ('data subject')* [...]".

In order to clarify this concept, the Working Party 29[23] stated that the contextual presence of 4 elements connotes personal data:

- *Any information*
- *Relating to*
- *An identified or Identifiable*
- *Natural Person*.

This specification certainly helps to determine the size of the concept but a broader view, in light of the risk of deanonymisation/re-identification as previously analysed, confirms the vulnerabilities which were originally highlighted in the Impact Assessment of the Regulation[99].

In fact, the difference between personal and non-personal data, as proposed in both regulations, seems to struggle if it takes into account data lifecycle and the physiological data attitude to be processed. Such processing modifies the status and nature of data, consequently, its definition and category.

In principle, the definition of personal data was coming from the centrepiece of EU legislation on data protection, Directive 95/46/EC adopted in 1995, with two main objectives: protecting the fundamental right to privacy and guaranteeing the free flow of personal data between Member States[24]. At that time, this definition of personal data had the advantage of providing a high degree of flexibility, and the possibility to adapt to various situations and future developments affecting fundamental rights. For this reason, the definition of "personal data" has been literally transposed into the GDPR, and by the majority of the Member States into their national laws.

However, since then, this broad, flexible definition has led to some diversity in the practical application of these provisions. For example, the issue of objects and items ("things" – referring to IoT systems) linked to individuals, such as IP addresses, unique RFID numbers, digital pictures, geo-location data and telephone numbers, has been dealt with differently by the various Member States.

[23] In detail: Article 29 Data Protection Working Party Opinion 4/2007 on the concept of personal data.

[24] The Directive was also complemented by several instruments providing specific data protection rules in the area of police and judicial cooperation in criminal matters (ex third pillar), including Framework Decision 2008/977/JHA

To this extent, the CJEU played, plays - and continues to play - an essential role in resolving these diversities, thus harmonising the legislation[25] and confirming that there is always room to shape the concept of personal data better.

Nevertheless, the core of the problem leading to legal uncertainty as a major area of divergence in the Member States, strictly linked to the data processing - and confirmed in the Impact Assessment of the Regulation (as mentioned above) - relates to the concept of *identifiability*. Specifically, it relates to the circumstances in which data subjects can be said to be "*identifiable*"; if data has been made "*anonymous*", so that data can no longer be related to the individual; if data has been "*pseudonymised*", where data can only be linked to the individual if one is in possession of a decoding "key".

Nowadays, the meaning and interpretation of *identifiability* still represents the main reason why the concept of personal data - and its interconnection with non-personal data - is widening and remaining problematic, especially in perspective of data processing, e.g. anonymisation, pseudonymisation.

Practically speaking, a person can be considered "identified" when she/he can be distinguished within a group of persons. In the case of identifiability this is not yet the case, however, it might be possible, e.g. by linking different data sets.

When transposed into the technological environment, as anticipated in the previous chapter, this perspective leads to the concept Personally Identifiable Information (hereinafter referred to as PII). Referring to the International Standards[26], ISO standard 27701[27] defines PII as "*any information that*

(1) *can be used to establish a link between the information and the natural person to whom such information relates, or*

(2) *is or can be directly or indirectly linked to a natural person*".

[25] To this aim, as an example, the judgment Case C-582/14: Patrick Breyer v Bundesrepublik Deutschland in which the Court ruled that dynamic IP addresses may constitute "personal data" even where only a third party has the additional data necessary to identify the individual.

[26] The European Commission's policy aims to align European Standards as much as possible with the international standards adopted by the recognised International Standardisation Organisations ISO, IEC and ITU. This process is called "primacy of international standardisation", meaning that European standards should be based on International standards (COM(2011)-311, point 7). For more info, cfr: https://ec.europa.eu/growth/single-market/european-standards/policy/international-activities_en

[27] ISO/IEC 27701:2019 (formerly known as ISO/IEC 27552 during the drafting period) is a privacy extension to ISO/IEC 27001. The design goal is to enhance the existing Information Security Management System (ISMS) with additional requirements in order to establish, implement, maintain, and continually improve a Privacy Information Management System (PIMS). The standard outlines a framework for Personally Identifiable Information (PII) Controllers and PII Processors to manage privacy controls to reduce the risk to the privacy rights of individuals.)

Contextualising these definitions in a dataset composed of different records, any kind of value can be a PII [100]. Consequently, it is possible to affirm that in the digital context based on big data, an "identity" [25] is any subset of attributed values of an individual person and, therefore, there is usually no such thing as "the identity", but several of them, as many as the number of the values combined with the same data-holder [101]. It goes without saying that the problem becomes greater if recalling the main premise of the data cycle, applied in the context of Big Data analysis systems in IoE environments, taking into account that any PII has a natural lifecycle [102] [103].

As specifically stated in the ISO standard "*from creation and origination through storage, processing, use and transmission to its eventual destruction or decay. The risks to PII can vary during its lifetime but protection of PII remains important to some extent at all stages. PII protection requirements need to be taken into account as existing and new information systems are managed through their lifecycle*."

To this extent, it can certainly be said that what is defined as personal data in *ex-ante* processing, cannot necessarily last and be confirmed at the moment of *ex-post* processing as non-personal and vice-versa, and also that there is certain clarity on the output data resulting from certain processing, e.g. anonymisation or pseudonymisation.

The investigation on the concept of personal data should be conducted while bearing in mind two different perspectives: the static, based on the reasoning of what can be literally considered as "personal data" and the dynamic one, thus what kind of status and nature modification data can have due to the processing, and the lifecycle.

After few years of the GDPR being in force, these vulnerabilities have been widely confirmed and discussed in academic debate [104] [37][105] [106] [94].

The importance in defining the concept of personal data is strengthened by the combined provisions of Art. 4 GDPR and Art. 2 FFDR, followed by Recital 26 of GDPR and Recital 8 of the FFDR.

With Article 4 GDPR and Art. 2 of FFDR, the legislator seems to acknowledge a mutually exclusive concept of personal and non-personal data. Moreover, Recital 26 of the GDPR and Recital 8 of the FFDR contains the acknowledgement that data processing can modify the nature of data, thus affecting the recognised protection and consequently placing on the shoulders of data processors and data controllers the responsibility of assessing the re-identification risk.

2.1.1. The GDPR and the FFDR in the perspective of the Data Governance Act (DGA)

The uncertainty linked to the two mutually exclusive definitions of personal and non-personal data impacts the development of future legislation. In fact, the GDPR and the FFDR settled the legislative ground for the European data flow before the definition of the data strategy presented by the European Commission in 2020[28]. However, despite the fact these pieces of legislation introduced the main difference on the *nature* of data, they did not provide a formal definition of data, which is only presented in the Data Governance Act[29]. Here, data is considered as *any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audiovisual recording.* Even here, this definition seems extremely broad and includes not only individual data, but also data *compilations* [107]. As a consequence, the DGA imposes a changeover in the meaning of the data concept from the syntactic level to the semantic one, including the whole content of digital means. In this regard, especially recalling *compilation* and without specification of whether it refers to databases, datasets, or even aggregate data, it imposes an investigation of the interplay between the contents of the DGA, the GDPR and the FFDR, especially on a semantic level.

Semantically speaking, it seems that the definitions of the nature of data do not have the same relevance they used to have before this new piece of legislation entered into force.

[28] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en

[29] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R0868

The DGA aims to set up a viable legal framework for data sharing, unleashing the potential of data flow. In this sense, the DGA seems to present a number of inconsistencies with the GDPR, most of which have also been investigated by the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS).

Specifically, in a Joint Opinion[30] the EDPB and the EDPS stress two main relevant points:

1. the blurring of the distinction between the processing of personal and non-personal data, and
2. the unclear relationship between the DGA and the FFDR.

Concerning the first point, the opinion confirms that the scenarios envisaged and desired by the *ratio* of the DGA increases the deanonymisation/re-identification risk for data subjects, as it proportionally increases the availability, re-uses and sharing of information, as well as the combination of personal data with non-personal data[31]. In this particular case, it is specified that different levels of safeguards can be deployed, even if it should be taken into account that with the increased availability of data and information, as well as the increase in its circulation, the risk naturally increases.

Concerning the second point of the relationship between the DGA and the FFDR, one of the main points of inconsistency emerged in relation to the *compilation* of data, namely in the combination of personal and non-personal data thus, the so-called *mixed datasets*.

[30] EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act) https://edpb.europa.eu/system/files/2021-03/edpb-edps_joint_opinion_dga_en.pdf

[31] In this sense: Explanatory Memorandum, page 3.

2.1.2. Mixed data and the definition of data in the DGA

Art. 2(2) of the FFDR states that "*In the case of a data set composed of both personal and non-personal data, this Regulation applies to the non-personal data part of the data set. Where personal and non-personal data in a data set are inextricably linked, this Regulation shall not prejudice the application of Regulation (EU) 2016/679*".

To clarify the concept of inextricability, the European Commission released practical guidance for businesses on how to process mixed datasets [108], contextualising the case and confirming that in most real-life situations, a dataset is however very likely to be composed of both personal and non-personal data (mixed dataset). In this case it confirms that it would be challenging and impractical, if not impossible, to split such mixed datasets.

In this sense, it is then clearly evident that the main premise of conceiving two mutually exclusive concepts of personal and non-personal data sclerotised the whole system and, to a certain extent, as pointed out by some authors [109], became counterproductive to data innovation.

The legal uncertainty linked to the definition of personal and non-personal data, and to their interconnections, was also pointed out in the process of the FFDR Impact Assessment (see above), and especially in the feedback provided by the stakeholders, namely the academic ones and, in time, has been confirmed.

Academics are still stressing a more proper evaluation of the differential element between personal and non-personal data, given by identifiability, on whether - and if so - under which circumstances personal data can be processed to become non-personal data [106].

Others [110], referring to the *Breyer* case (as above), consider that characterising the data should be context-dependent, stressing the fact that the concept of personal data has some limits and the line between personal and non-personal data is fluid and evolves over time. This

reasoning also applies to anonymised data, meaning that, over time, non-personal data can become personal data again, because the context changes over time [104]. Specifically, authors consider that contextual controls have been conceived as complementary to anonymisation (e.g. *sanitisation techniques*) by the drafters of the GDPR. The GDPR is also considered compatible with a risk-based approach when contextual controls are combined with sanitisation techniques.). Hence, in order to mitigate the gross risk of re-identification, contextual checks become essential.

For others [23], the broad notion of personal data and the mutually exclusive concept of non-personal data is not problematic and even welcome, but this will change in future when everything will be or will contain personal data, leading to the application of data protection to everything. This will happen because technology is rapidly moving towards perfect identifiability of information, where datafication and data analytics will generate a lot of information. Therefore, "*the intensive compliance regime of the General Data Protection Regulation (GDPR) will become 'the law of everything', well-meant but impossible to maintain. [...] and by then we should abandon the distinction between personal and non-personal data*".

The FFDR complements the European legal framework on data processing, representing the natural continuation of the approach of the GDPR for personal data, introducing a smooth approach for the circulation of non-personal data. However, the semantic difference between personal and non-personal data seems to be remarkably difficult in practice, especially in the case of mixed big datasets. Moreover, apart from that, it must be stated that personal data can be generated from non-personal data as well, relying on deanonymisation techniques, as mentioned above.

In any case, personal data and non-personal data are often difficult to distinguish and a specific binding regulation on mixed dataset is lacking.

Moreover, in the above-mentioned guidance, the European Commission specifies that if non-personal data and personal data are inextricably linked, the GDPR prevails [111]. For the time being, the concept of inextricability has not yet been explored or investigated, opening up to a very broad concept of it.

In such a particular case, distinguishing only between personal and non-personal data may not necessarily grant proper protection to other types of data generally included in the main category of non-personal data, such as IP rights and namely trade secrets, copyrights, patent and confidential information.

To this extent, the Data Governance Act seems to confirm such an opening, unleashing the potential of many kinds of data. In defining the scope of application of the DGA, Article 3 refers to data held by public sector bodies which are protected on grounds of:

(a) *commercial confidentiality, including business, professional and company secrets*;

(b) *statistical confidentiality*;

(c) *the protection of intellectual property rights of third parties*; or

(d) *the protection of personal data, insofar as such data fall outside the scope of Directive (EU) 2019/1024*.

With such an approach, the DGA tends to go beyond the semantic dichotomy of personal and non-personal data as it extends the amount of data held by Public Sector Bodies that can be re-used, creating an ecosystem of trust [29], overcoming the main focus on the *nature* of data as in the GDPR and the FFDR.

It introduces new measures aimed at tacklng substantial issues posed by data reuses, such as *the lack of cross-sectoral interoperability, the limited ability to obtain reusable data, and the uncertainty about data quality*.[32]

In line with these premises, the questions posed by the concept of *inextricability* seems to represent an old perspective of and approach to data, outclassed by a new approach which relies on designing data stewardship entities for granting and advancing data access [112], on the assumption that technological development cannot be contained, thus it is better to deploy subjective solutions over the objective one. In this regard, some elements in the new DGA Regulation may eventually confirm this approach, such the prohibition of sharing data by default, the evaluation on the nature of data, the re-purpose of data and many more points that will be investigated in the following chapter.

[32] Commission Staff Working Document, Impact Assessment Report accompanying the DGA proposal, SWD (2020) 295 final https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020SC0295&from=EN

2.1.3. Processing and granting anonymity: certain grades of uncertainty

In spite of the mentioned different layers of legislations and their inconsistencies, there is one central point which seems to be granted in all them, in the GDPR, in the FFDR and in the DGA. These pieces of legislation recall anonymisation and pseudonymisation as the two main data models for implementing privacy by design and data protection, that are two different and independent models. Both impact on the identifiability of the natural persona to whom data refers.

However, in practice, there is often some confusion between the two models, their notions and application, especially on the perception of pseudonymised data as anonymous data [113].

In looking for a definition of anonymisation, the GDPR does not provide one, and neither does the FFDR or the DGA. The Working Party 29 Opinion 05/2014 on Anonymisation Techniques [114] explicitly considers this model as "*further processing*". As such, it must comply with the test of compatibility in accordance with the guidelines provided by the Working Party 29 Opinion 03/2013 on purpose limitation [115], and with the deanonymisation risk test as per the Working Party 29 Opinion 05/2014.

Differently, with regard to pseudonymisation, art. 4(5) of the GDPR defines pseudonymisation as "*the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person*".

This definition requests the presence of two main elements:

- the removal of the attribution link between the personal data and the data subject
- its replacement with new additional information.

When contextually considered by the legislation in force, these two elements make data always re-identifiable therefore, personal data.

In switching from the legal context to the technological one, namely recalling ISO 29100 for anonymisation[33] and ISO 25237 for pseudonymisation[34], the main difference between the two types of data processing is *irreversibility/reversibility*. Here, while anonymisation is considered an irreversible data model processing, pseudonymisation is considered a reversible data model processing. However, due to the available technology and the technological development, this dichotomy has eroded, at least regarding the irreversibility of anonymisation. This awareness can also be found in the legal framework, and namely in Recital 26 of GDPR[35] and Recital 9 of the FFDR.[36]

It is indeed generally recognised that, despite the investments and the different implementations by several interested communities (statistical, informatics, electrical engineering), in general, it is not possible to perform perfect anonymisation, and the span of the deanonymisation issue is rapidly increasing. This perception is confirmed by the academic debate which, at least regarding anonymisation seems to be polarised, focused on questioning whether anonymisation could - or could not - be a proper tool for protecting data. On one hand, some academics [15] [116] [117] [118] believe that it is not possible to grant proper, irreversible anonymisation while at the same time maintaining the data useful, or vice-versa. Others [16] [119] consider that, despite the awareness of the deanonymisation issue, a compromise between the commercial, social value of sharing data and some risks of identifying people should always be reached - even if producing consequences for personal privacy and data protection.

Thus, the traditional academic debate on anonymisation seems to be represented by a relation of *inverse proportionality* between data utility and data protection, as follows:

[33] International Standard Organisation (ISO/IEC) 29100:2011 Information technology – Security techniques – Privacy framework (*Technologies de l'information – Techniques de sécurité – Cadre privé*).

[34] International Standards Organisation (ISO/IEC) 25237:2017 Health informatics — Pseudonymisation. It contains principles and requirements for privacy protection using pseudonymisation services for the protection of personal health information.

[35] "*The principles of data protection should apply to any information concerning an identified or identifiable natural person.*
[...] The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable."

[36] "*The expanding Internet of Things, artificial intelligence and machine learning, represent major sources of non-personal data, for example as a result of their deployment in automated industrial production processes. Specific examples of non-personal data include aggregate and anonymised datasets used for big data analytics, data on precision farming that can help to monitor and optimise the use of pesticides and water, or data on maintenance needs for industrial machines. If technological developments make it possible to turn anonymised data into personal data, such data are to be treated as personal data, and Regulation (EU) 2016/679 is to apply accordingly".*

$$x \cdot y = k$$

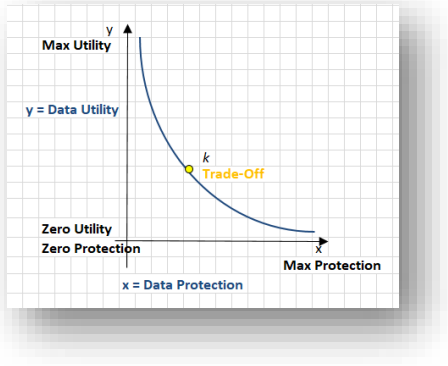


Fig. 2. Graph representing the inverse proportion between utility and protection in data anonymisation

Differently, with regard to pseudonymisation, research has increased in expanse and time, with an increasing interdisciplinary character, especially after being included in the GDPR as a data security measure.[37]

In the WP29 Opinion 04/2015 on the Anonymisation Techniques, pseudonymisation is defined by negation as "*not a method of anonymisation* [...]. *It merely reduces the linkability of a dataset with the original identity of a data subject and is accordingly a useful security measure*."

Some researchers have focused their attention on the risks linked with the choice of including it as a security measure [120], preparing the ground for an intense debate on the ambiguity surrounding the concept of pseudonymisation in the GDPR [121].

[37] GDPR - Article 32. Security of processing.
1. *Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:*
a. the pseudonymisation and encryption of personal data; [...].

The choice made by the legislator, to include pseudonymisation among the data security tools to be improved and designed in line with the principles of privacy by design, the debate on pseudonymisation has even increased.

Despite some contrasts in the definitions as anticipated, the growing potential of pseudonymisation now seems to have been recognised, and data utility and data protection seem to be in a relation of *direct proportionality*, as follows:

$$y / x = c$$

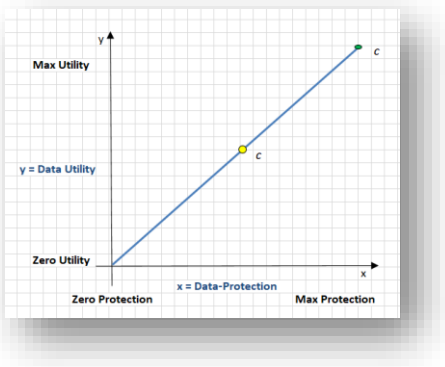


Fig. 3. Graph representing the direct proportion between utility and protection in data pseudonymisation

The remarkable importance given to these two models of processing data relies on the fact that both can be used to grant anonymity and protecting personal data. However, in line with the developments highlighted by the state of the art, anonymisation seems to be an obsolete model which was tailored for microdata (especially for the statistical needs of privacy preserving data publishing) and, as such, no longer suitable for big data analytics except for particular cases.

Differently, pseudonymisation seems to unfold its potential in big data analytics leading to overcoming the traditional objective approach (reversibility/irreversibility) and opening a new interpretation based on a subjective approach to data processing models, which involves all the stakeholders involved in the generation, collection and processing of data.

2.2. Anonymisation, deanonymisation and the trade-off between data utility and data protection

Anonymisation can be generally considered as the fact or process of rendering something anonymous; in this context, the main reference is to data, to rendering data anonymous thus not referring to a natural person. From a legal point of view, anonymous data should be considered non-personal data.

In providing specific examples of non-personal data, Recital 9 of the FFDR states *aggregate data* and *anonymised data* used for big data analytics. The Recital specifies, "*If technological developments make it possible to turn anonymised data into personal data, such data are to be treated as personal data, and Regulation (EU) 2016/679 is to apply accordingly*".

This specification clearly confirms the legislator's awareness of the deanonymisation issue the analysis of which is increased and completed in Recital 26 of the GDPR. Here, after stressing identification as an essential connoting element of personal data (personal data is only the one in which the data subject is *identified* or *identifiable*) the legislator determines the rules to assess whether anonymised data (thus, non-personal data) can be turned into personal data.

As anticipated, Recital 26 of GDPR clearly specifies that "*to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly*."

Thus for determining the nature of anonymised data, it becomes necessary to perform a case-by-case evaluation.

It is then clarified that "*to ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments*."

In line with what is considered in the Recitals, the cost, the time, the available technology, and the technological developments represent objective factors in the analysis of the possibility to turn anonymised data into personal data. Only this assessment determines the level of protection granted to anonymised data, on the awareness that deanonymisation represents an issue and a risk.

Therefore, anonymised data cannot be considered by definition or by default as non-personal data: its nature has to be ascertained taking into account objective factors such as cost, time, available technology and technological development. The outcome of anonymisation does not determine *per se* the nature of data, as the identifiability of the natural personal to whom the data pertains can be anyway compromised.

2.2.1. Anonymisation in the soft-law: singling-out, linkability and inference

In the last two decades, the academic debate has registered a change from the past: rather than questioning whether anonymisation was a proper tool or not for protecting data and privacy, academics are currently demonstrating the possibility of reversing the process of anonymisation, exploring and studying its correlated techniques.

The attention is focused on the concrete possibility of deanonymising data that have undergone a process of anonymisation, relying on the available technology and technological development (no matter the anonymisation techniques used).

Concerning the legal framework in force, despite several mentions of anonymisation in the GDPR, FFDR and the DGA, the legal analysis confirms that European legislation does not provide an explicit regulation on anonymisation, nor a specific identification of the techniques, or how the process should be/could be performed. The legal focus is not on the tool *per se*, rather on its outcome, stressing the need to assess whether the outcome of anonymisation confirms the anonymity of data, impacting the re-identification of the natural person to whom the data pertains.

The only institutional reference stems from the Working Party 29 Opinion n. 05/2014 on Anonymisation Techniques (as mentioned above). Here the WP29 recommends that it is necessary to test the anonymisation techniques against the deanonymisation risk. To this extent, three declinations of this risk are mentioned:

- singling out an individual,
- linking different data

- inferring data.

Here, the WP29 considered solely the potential risks linked to this data processing, recalling the two main anonymisation techniques: randomisation and generalisation, which were the main anonymisation models used for structured data, thus becoming remarkably challenging with unstructured Big Data and increasing the risk of deanonymisation (Chapter 2).

Randomisation alters the veracity of data, weakening the links between values and objects (data subject), and introducing a casual element into the data. This result can be concretely accomplished using a few techniques: permutation, noise addition and differential privacy.

In permutation, the values are not modified: the unique association between the identifier and quasi-identifiers will be decoupled, to be associated with the quasi-identifiers of another identifier (object) randomly chosen. Lastly, the values of a person will be associated with another person. Permutation has the benefit of not modifying values, which are maintained as such, thus the analysis of aggregated data is still possible and useful.

In noise addition, noise refers to an automatic program called "*pseudorandom number generator*" also known as a "*deterministic random bit generator*" (DRBG), which introduces a random variable, perturbing the value and making it less accurate. For this reason, the database loses its utility and this technique, consequently, is considered vulnerable.

In the differential privacy, an algorithm analyses a dataset and computes statistics about it and "*it is said to be differentially private if by looking at the output, one cannot tell whether any individual's data was included in the original dataset or not*" [122][123]. This technique seems to make sure that information about participants in the database, is not leaked, even if academics from the statistical community have just pointed out its vulnerability [124].

Differently from randomisation, generalisation dilutes the attributes of a table, by modifying the respective scale or order of magnitude. Consequently, the scale of magnitude will be modified to the point in which more rows of the table will finally have the same combination of generalised attributes. All the records in the table with the same combination of generalised attributes are called equivalence class. The bigger the equivalence class, the smaller the possibility of re-attributing the value to the data subject.

Generalisation can be performed using the following techniques: aggregation and K-anonymity, L-diversity and T-closeness.

In aggregation and K-anonymity [125], all the equivalence classes have a cardinality higher than a certain K value and the generalisation scheme is called K-anonymity. In this case, the

attribute values are generalised to such an extent that each individual shares the same value. K-anonymity has been implemented with several algorithms [125][126][127].

L-diversity extends k-anonymity: it is ensured that in each equivalence class every attribute has at least L different values, thus relying on the fact that the deterministic inference attacks are no longer possible. However, L-diversity seems to be vulnerable and subject to probabilistic inference attacks [128].

T-closeness represents a refinement of L-diversity, and it creates equivalent classes that are very similar to the initial distribution of attributes in the table, thus it is mostly used when there is a need to keep the data as close as possible to the original one [129].

Certainly, the state of the art seems to confirm that anonymisation methods face big challenges with *real* data. Anonymisation methods, *such as k-anonymity, are highly dependent upon spatial locality to effectively implement the technique in a statistically robust way* [130].

To this extent, in light of the limits raised by different scientific communities on anonymisation models for structured data, new models of anonymisation are explored, with the aim of overcoming the limits of traditional anonymisation techniques with unstructured data. Among many, we can mention the model of "*functional anonymisation*" which is based on the relationship between data and environment within which the data exist, the so-called "*data environment*" [131] [17], relying on a pure statistical approach. Here, researchers provide a formulation for describing the relationship between the data and its environment that links the legal notion of personal data with the statistical notion of disclosure control [132][133][134][122].

Moreover, if perfect anonymisation has failed, others[135] remark that while the debate on deanonymisation remains vigorous and productive, "*there is no clear definition for policy*", arguing that the best way to move data release policy is focusing on the process of minimising risk of re-identification and sensitive attributes disclosure, rather than trying to prevent harm.

2.3. Pseudonymisation and Pseudonymity

Recalling the main premise, in pseudonymisation there are two main elements:

- the removal of the attribution link between the personal data and the data subject
- its replacement with new additional information.

As for anonymisation, the legal framework does not provide any detail on the techniques but provides orientation in terms of context. Specifically, the GDPR only recalls it in two different articles: in Art. 25 as an *appropriate technical and organisational measure designed to implement data-protection principles*, and in Art. 32 listing it, with the encryption, as a *security measure* that should be implemented by the data controller and the data processor.

These specific collocations explicitly confirm that data must undergo pseudonymisation processing in order to grant its security and, such processing can be adapted with other security measures to protect the dataset, implementing *privacy by design principles*.

A more precise description of pseudonymisation techniques stems from the European Agency for Cybersecurity (ENISA). It lists this data processing model among its priorities of the Programming Document 2018-2020 and provides recommendations on shaping technology according to GDPR provisions. Specifically, complete guidance can be found in four different recommendations[38]thus, as such, not legally binding, confirming the same approach followed by the WP29 Opinion 04/2015 on the Anonymisation Techniques.

[38] ENISA, Recommendations on shaping technology according to GDPR provisions. An overview on data pseudonymisation, November 2018, https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions ; ENISA, Pseudonymisation techniques and best practices. Recommendations on shaping technology according to data protection and privacy provisions, November 2019, https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices ; ENISA, Data

In the ENISA Recommendations, different techniques are described, on the assumption that pseudonymisation can relate to a single identifier, but also to more than one. The pseudonymisation can be performed with the following techniques: Counter, Random Number Generator (RNG), Cryptographic Hash Function (CHF), Message Authentication Code (MAC), and Encryption.

Counter represents the simplest pseudonymisation technique, wherein a number chosen by a monotonic counter substitutes the identifiers. Its simplicity makes it a proper technique for small datasets. The Random Number Generator (RNG) is like the counter, with the difference that a random number is assigned to the identifier, relying on a mechanism that produces values unpredictably selected.

The Cryptographic Hash Function is directly applied to the identifier obtaining the corresponding pseudonym, taking input strings, and mapping them to fixed length outputs. Similar, except for introducing a secret key to generate the pseudonym, is the Message Authentication Code (MAC), where the knowledge of the key is essential for mapping the identifiers and the pseudonyms.

Lastly, the encryption that relies on a symmetric encryption algorithm for generating the pseudonyms and for which the same secret key is needed as for the decryption. Asymmetric encryption algorithms can also be used in specific cases for pseudonymisation purposes.

However, as anticipated, not all the pseudonymisation techniques are equally effective and the possible practices vary. They can be based on the basic scrambling of identifiers, or to the advanced cryptographic mechanism. Their level of protection may vary accordingly.

In any case, especially for the hash function there is doubt as to the extent it represents an efficient pseudonymisation technique, especially under certain circumstances such as the case in which the original message has been deleted, thus granting irreversibility. In this case indeed, the hash value might even be considered as anonymised[39], based on the dichotomy of *reversible/irreversible* processing [106]. In line with this consideration, academics have started considering that anonymity can be granted not only with anonymisation models, but also with pseudonymisation, questioning the semantic approach imposed by the GDPR.

Pseudonymisation: Advanced Techniques and Use Cases, January 2021, https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases ; ENISA, Deploying pseudonymisation techniques, March 2022, https://www.enisa.europa.eu/publications/deploying-pseudonymisation-techniques

[39] In this sense, a first innovative approach came from the Spanish Data Protection Authority: AEPD, Introduction to the hash function as a personal data pseudonymisation technique, October 2019, https://edps.europa.eu/sites/edp/files/publication/19-10-30_aepd-edps_paper_hash_final_en.pdf

In fact, the GDPR considers that data that have undergone a process of pseudonymisation are still personal data, as its data processing is considered reversible as the additional information generated as pseudonyms can still be matched with the input data. In term of policy, this decision is of paramount importance to determine the compliance of rights recognised by the GDPR in certain types of processing (e.g., research, traffic data analysis, geolocation, blockchain and others).

However, in this regard, some authors consider that pseudonymisation can grant anonymity, as well as anonymisation, provided that some subjective conditions on the input data are met [121].

This vision confirms the reason the regulatory framework is still uncertain and that the zero-risk approach cannot certainly represent the final aim of any data processing, but can be the needed mind-set to navigate through the legal framework currently in force.

On the same note, some policy fragmentation in the Member States should be considered.

In some of them, Data Protection Authorities (hereinafter referred as DPAs) considered encoded or pseudonymised data as identifiable thus, as such, as personal data in relation to the actors who have means (the "key") for re-identifying the data, but not in relation to other persons or entities (e.g., Austria, Germany, Greece, Ireland, Luxembourg, Netherlands, Portugal, UK). In other Member States, all data linkable to an individual were regarded as "personal", even if the data were processed by parties who have no means for such re-identification (e.g., Denmark, Finland, France, Italy, Spain, and Sweden). DPAs in those Member States are “generally less demanding” regarding the processing of data that are not immediately identifiable, considering the likelihood of the data subject being identified as well as the nature of the data.[40]

Therefore, it should be noted that academics and DPA decisions are starting to break the traditional approach which tended to consider anonymisation as an irreversible approach and pseudonymisation as a reversible one. Consequently admitting that both impact on the identifiability of data, as well as, on anonymity.

[40] The extent of the issue is treated extensively in the Impact Assessment of the GDPR and confirmed by the first decisions of the DPAs, like the Spanish DPA referring to the ash function.

2.3.1. Granting anonymity relying on roles and responsibilities distribution among stakeholders

The state of the art concerning the two main data processing models recalled by the GDPR, anonymisation and pseudonymisation, shows that the objective perspective tends to be overcome. In fact, it is based on the data processing model *per se,* thus stressing on the fact that only anonymisation can grant data anonymity, while pseudonymisation cannot. Therefore, in the GDPR the traditional dichotomy of *anonymisation/irreversibility* and *pseudonymisation/reversibility* can be found.

However, the technological development helped to shape new interpretations of the GDPR that are able to question the above-mentioned semantic dichotomy.

Indeed, it is currently investigated and confirmed that as for anonymisation, even pseudonymisation can grant data anonymity if relying on the distribution of roles and responsibilities among stakeholders.

As anticipated, the first interpretation in this sense came from the academic debate, when scholars started questioning whether pseudonymised data were always personal data [121]. In this occasion, authors considered that *the definition of pseudonymisation given in Art.4(5) of the GDPR will not expand the category of personal data*. They believe that even pseudonymisation can render data anonymous, thus breaking the link between data and the natural person to whom the data pertain, using as a reference test Recital 26 of the GDPR.

Such an outcome can be achieved in a particular circumstance: if data that have undergone a process of pseudonymisation in one organisation are shared with a third party without the input data, thus rendered and remaining anonymous for such last third party.

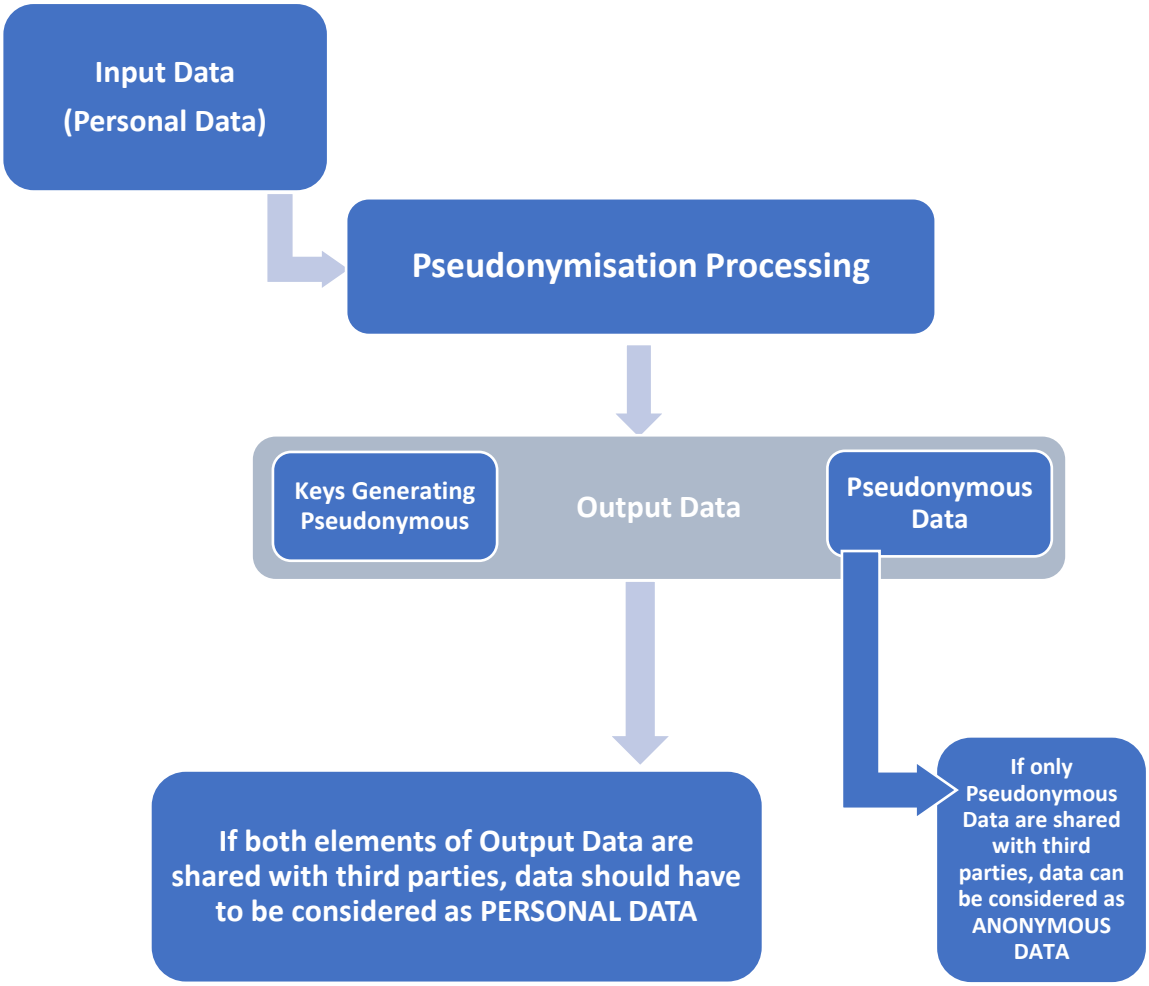


Fig. 4. Sharing pseudonymised output data with third parties

Therefore, in line with such reasoning, it can be considered that the sharing of pseudonymous data only should be subject to the deanonymisation/re-identification risk test based on Recital 26 of the GDPR. Moreover, if data are considered anonymous, the third party may process data at her/his best convenience as the link between the personal data and the natural person to whom the data pertain (data subjects) should be considered broken.

In this sense, the DGA can be considered as developing a new subjective approach on data semantics, overcoming the initial and traditional imprinting of the GDPR.

Chapter 3. *Big Data and IoE as Hybrid Human-based and Device-based Environment*

Index of the Chapter

Short Abstract of the Chapter

This chapter explains the main legal premises of the research, defining its technological context based on Big Data and the Internet of Everything. On one hand, it presents the main advantages of such technologies while, on the other hand, it also investigates the main risks and threats posed by such technologies in terms of privacy and data protection. Considering the datafication phenomena, this chapter discusses the feasibility of the right to be forgotten and how it can eventually be coordinated with the above-mentioned phenomena.

The main perspective investigated is the further processing of data, as it is considered to be a higher stage of the first processing where poorly processed personal data can increase the risk of de-anonymisation/re-identification.

Lastly, the chapter presents an explorative literature review on the issue of de-anonymisation/re-identification.

3.1. Big Data and Internet of Everything for Cutting Out the Middleman

In recent decades, the evolution and development of technology has registered a remarkable growth, increasing the possibility of substituting the human intervention in the communication between machine-to-machine, people to people and people to machine [35]. Big Data [36] and Internet of Everything have played an essential role in this change, leading to the automation of many processes, *determining the inter-penetration of the 'real' and the so-called 'virtual'* [37].

Internet of Everything uses Big Data to empower the automation of electronic equipment in the surrounding environment. The vast collection of data is stored locally on devices (*things*), or possibly in the cloud, enabling data processing and data aggregation on a large scale. Data pertains to the digital environment, as well as to the users. Due to said technological process, machines can learn how to customise better services for the users, inferring information from data and, consequently, generating knowledge.

The combination of these technologies avoids human intercession in the process of collecting, storing and processing data, making human intercession superfluous.

As anticipated, in the IoE the public and the private sphere have merged [2], impacting the human space and generating a more globalised environment, which automatically collects analyses, and mines information about places, object and people. This environment constantly expands its perimeter, increasing its technological capacity.

The remarkable opportunities of Big Data and Internet of Everything have been comprehensively investigated by the scientific and business community, boosting the capacity of data analysis. The more information is multiplied and shared, the more concerns arise in terms of tracking, profiling, discrimination, exclusion; moreover, loss of control and surveillance risks.

Internet of Everything generates a remarkable amount of data and relies on data, processes, people and things connected in a network, including machine-to-machine (M2M), person-to-machine (P2M), and person-to-person (P2P) systems. Therefore, handling such amount of data requires more sophisticated techniques and tools, giving way to artificial intelligence (AI). In comparison to traditional data techniques and platforms, AI techniques provide more accurate, faster, and scalable results in big data analytics, and they can be used to transform big data into smart data, providing more accurate results [39][40]. Among these advanced techniques we can mention machine learning (ML), natural language processing (NLP), computational intelligence (CI), and data mining. These were designed to provide big data analytic solutions as they can be more accurate, more precise and faster for massive volumes of data, discovering information, hidden patterns, and unknown correlations.

The extraordinary societal benefits of big data—including breakthroughs in medicine, data security, and energy use—must be reconciled with increased risks to individuals' privacy. As is often the case, technological and business developments in big data analysis have far outpaced the existing legal frameworks, which date back from an era of mainframe computers, predating the Internet, mobile, and cloud computing.

These technological developments have also challenged the boundaries of fundamental rights, privacy and data protection. Despite efficiency in the process, the increase in the level of automation implies an increase in the vulnerability of such systems, thus impacting privacy and data subject protection.

Due to its volume, the amount of data generated is vulnerable to security breaches and, to this purpose, it became of paramount importance to secure the data at all levels from the initial source, transfer, storage and final output.

Many technologies have been implemented to secure big data analytics such as anonymisation, pseudonymisation, encryption, and others. In this sense, the European legislation keeps evolving, trying to provide guidance on the issue as well as trying to avoid suffocating the technological development.

In such intent, the European legislator dedicates specific attention to the evolution of the market, specifying in its Data Strategy its aim of *creating a single market for data that will ensure Europe's global competitiveness and data sovereignty. Common European data spaces will ensure that more data becomes available for use in the economy and society, while keeping the companies and individuals who generate the data in control* [41].

From a mere legal point of view, it appears particularly challenging to regulate the evolution of such technological capacity due to the clash with data subjects' fundamental rights and liberties. Mainly, the right to privacy is the first generally considered; not only considered in its first conception of the *right to be left alone*, but also the right to self-determination, avoiding any kind of interference in the private sphere. As such, the right to data protection is conceived as the empowerment of data subjects to exercise their control over the collection, use and disclosure of their personal information. These rights find an explicit recognition in the European Convention of Human Rights (ECHR), in Article 8 on the right to respect privacy and family life. The Charter of Fundamental Rights of the European Union reproduces - in Art. 7 - the content of Art. 8 of the ECHR, while Art. 8 raises the protection of personal data to the status of a fundamental right. Both of these rights interact in multiple ways, especially as the right to data protection represents the main tool by which the right to privacy is protected. The central importance of privacy and data protection in the digital environment is therefore not merely due to the fact that digital systems record what happens in 'real life'.

3.2. Datafication and the Right to be Forgotten in Streaming Structured, Semi-Structured and Non-Structured Data

The IoE accurately captures the environment to which it pertains, converting the outcome of such capture in data, thus in valuable information. In fact, digitalisation facilitates the datafication process, which is considered to be the representation of most aspects of our daily lives with data [42]. Digital technologies have accelerated such a process, automating the historical practice of databasing, analysing and generating knowledge and inferring information for creating value. Especially with IoE, data does not exclusively refer to humans

[43], but also to the environment to which technology pertains, recalling the broadest concept of environment.

The datafication process has been questioned since the 1960s and 1970s, especially in the United States [44] [45] [46] [47]. The increasing capabilities of technology to store information, give it a meaning and render it ready for subsequent uses has fuelled the first debate on privacy. Originally, such debate concerned only government and large private institutions as the only ones capable of collecting personal information in computerised databases: namely, citizens' tax, health, educational and social security benefits in the welfare state. This practice responded to the need for population management, developing into more modern forms of state bureaucratic administration[48]. Gradually, the debate expanded its focus, no longer limited to government and public institutions, but extending it to private companies running their major businesses on data [49].

On the same note, since the 1970s, the debate has also matured in Europe, confirming that datafication precedes digitalisation, using technology as an *instrument* for accelerating such a process [50].

In this sense, it can be argued that there is no shift of paradigm, rather a constant evolution of the one on which datafication is built: the collection of personal information represented by data.

Therefore, in some parts, the evolution of the legislation doesn't appear to take into account this expansion. Considering the current legislation on data, specifically the GDPR, it is unquestionable that some rights and freedoms mentioned here are unfeasible for enforcement in the digital environment and academics continue to debate their root and content [51] [52] [53] [53] [54] [55] [56]. In this regard, the right to erasure (*right to be forgotten*) is one of the most studied and questioned [57] [58]. As a matter of fact, the development and evolution of technology keeps challenging the implementation of the balancing test between competing rights of privacy and data protection, and free expression and access to information. However, the significant body of European jurisprudence on the matter provides a guideline for the implementation of the right to be forgotten. Indeed, almost a decade ago, the Court of Justice of the European Union recognised the individual's right to ask search engines (e.g. Google) to remove results for queries on a certain user's name (ECLI:EU:C:2014:317)[41]. As anticipated, scholars have long debated the right to be forgotten, its balancing test and the legitimacy and

[41] https://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=IT

transparency of search engines as private actors responsible for the implementation. These debates have confirmed that the right to be forgotten raises fundamental questions, not only in terms of personal data, but also in terms of media freedom, and on the impact of deletion. Specifically, technological development seems to confirm that the challenges in the implementation of the right to be forgotten increase the risk of de-anonymisation/re-identification [59] [60]. Such a right seems to be evolving towards being artificial, as it follows a technology-agnostic approach, as it does not allow laws to be coordinated with the state-of-the-art technologies in computer science and technology information.

In fact, big data comes in a variety of shapes and form, generating many difficulties in coordinating the protection and security of the information, and therefore increasing the unfeasibility of granting deletion (erasure, *forgetting*). Modern digital environments using big data struggle to handle the process of analysing and erasing [61]. Data is unable to be handled and processed by most current information system methods as *the most traditional data mining methods or data analytics developed for a centralised data analysis process may not be able to be applied directly to big data* [62]. Especially in IoE environments, the dataflow is constant, and the variety, diversity and volume of data are different. If, for example, considering only the structure of data, the fact of having structured, semi-structured and unstructured data poses many challenges for ensuring protection and security. Data can be made of only numerical or categorical attributes, or usually, as a mix of numerical and categorical attributes.

Preferable data is structured, but not necessarily. Unstructured data refers to data which does not adhere to conventional data models, thus not easily searchable. It comes with formats like audio, video, and social media postings, usually collected with powerful Artificial Intelligence applications. More than 80% of generated data are unstructured and this percentages grows by 55-60% every year[42]. Despite the structure, data can be organised into microdata or macrodata, it can be static or dynamic. The variety of data has a remarkable impact on the design of modern technologies from its embryonal phase, creating risks in terms of privacy and data protection, the reason that justified the integration of such rights in modern legislations[43].

[42] https://mitsloan.mit.edu/ideas-made-to-matter/tapping-power-unstructured-data

[43] In this sense, the statistics of the United Nations Conference on Trade and Development, showing that with the increase of the social and economic activities places online, the importance of privacy and data protection increases as well. Data confirms that 137 out of 194 countries had put in place legislation to secure the protection of data and privacy. Moreover, still according to data, Africa and Asia show different level of adoption with 61 and 57 per cent of countries having adopted such legislations. In detail: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

3.3. Privacy and Data Protection in Further Data Processing

The modern digital environments are implemented through big data, such as IoE, which imposes the integration of privacy and data protection principles from policy to engineering. The GDPR requests that *data controllers implement appropriate technical and organisational measures to protect personal data and avoid unlawful disclosure*, above all when the process involves the transmission of data over a network.

In determining the framework of these technical and organisational measures, it is essential to clearly define the concept of privacy and data protection, in order to better understand the extent of data controllers' responsibilities.

Data protection appeared as an *offspring of privacy* [50] and the two rights seem inextricably linked. Scholars tend to agree that data protection and privacy share a common characteristic: both are confronted with remarkable interferences in contemporary information society.

The debate among European scholars focused on whether data protection represents an autonomous fundamental right, thus separate from privacy, or whether it can be considered as a mere aspect of privacy [63]. Despite this aspect of the debate, data protection and privacy certainly interact and the European Constitution reserves separate roles to these distinct rights and considers data protection as a legal instrument adding something to privacy [64].

In Europe, the first legislations on data protection were issued in Germany[44] and Sweden.[45]

Since then, the concept of data protection has been distinct from the concept of privacy. The latter used to be considered as a *broad concept that embodies a range of rights and values, such as the right to be let alone, intimacy, seclusion, personhood, and so on according to the various definitions* [50]. Over time, it has emerged that such right cannot have strict boundaries and, due to the technological development, its concept keeps expanding. On the other hand, data protection emerged as a set of interests further to privacy, concerning the security of the information systems – data security – and its data quality [65]. Consequently, data protection emerged to serve fundamental rights other than the ones protected by privacy. As anticipated, such confirmation came from the Europe Constitution where data protection arises at the level of other fundamental rights, alongside privacy [66] [67]. Therefore, the inclusion of data protection in the European Charter of Fundamental Rights is a point of arrival in a process started almost fifty years ago, which culminates with this inclusion, as well as with the discussion, promulgation and entry into force of the General Data Protection Regulation [68].

Such pieces of legislation have imposed many principles and rules for granting the protection of data in the engineering of information systems, since its first design. Two requirements among the main instruments tailored by the legislator for protecting data subjects since the first collection of data, are particularly relevant in the context of IoE and big data: consent and purpose [69]. Both of these requirements have been analysed by the Working Party 29[46].

[44] Datenschutzgesetz, Oct. 7, 1970, § 6, 1 Gesetz- und Verordnungsblatt für das Land Hessen 625 (1970).
[45] Datalagen (Swedish Data Act) of May 11, 1973, entered into force July 1, 1973.
[46] The requirement of consent has been analysed in the Guidelines on consent under Regulation 2016/679, Adopted on 28 November 2017 and last revised and adopted on 10 April 2018 (17/ENWP259 rev.01); the

Defined and regulated from Article 6 to Article 8, consent has animated the scholars' debate since the first discussions of the GDPR. In time, the criticalities of such a requirement emerged and scholars remain sceptical on its efficiency if applied to big data [70], as most of the time consent forms are very difficult to navigate for data subjects [71], thus tending to legitimise dark patterns [72] and other issues, even in the event it is revoked [73]. Moreover, another essential requirement is purpose. In this regard, there still appears to be room to investigate the different declinations of purpose, especially in conjugation with consent for secondary uses of data, for further processing.

More issues seem to arise in further processing of data[74] (justifying secondary data uses): a typical case could be when data are legitimately collected but poorly processed. In principle, academics have long investigated this criticality in the context of research [75] and health data [76], trying to find certain benchmarks in ensuring data quality. However, this issue seems to be as difficult to handle as after the first processing. In application of the data minimisation principle [77], processed personal data, for which the purpose of collection has been reached, should be erased or anonymised. Therefore, it is outside the scope of application of the GDPR and the loss of its protection.

The notion of further processing is closely linked to the concept and scope of initial processing. The GDPR provides a broad concept of processing in Article 4.2 as "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*".

The European Court of Justice has further specified[47] that processing "*may consist in one or a number of operations, each of which relates to one of the different stages that the processing of personal data may involve*". This specification considers the various stages of the data lifecycle, even in secondary uses of personal data.

Moreover, the concept of further processing is strictly connected to the requirements and conditions under which the initial processing is undertaken. As anticipated, consent, as well as purpose, play an essential role in framing the legal basis for collection and processing personal

requirement of purpose has been analysed in Opinion 03/2013 on purpose limitation adopted on 2 April 2013 (00569/13/ENWP 203).

[47] Case C- 40/ 17, Fashion ID.

data. Consent and purpose of the first collection shape the boundaries of the secondary processing.

Recital 50 recalls further processing as processing of personal data *for purposes other than those for which the personal data were initially collected*.

The GDPR requests that any purpose for processing personal data should be clearly specified and accepted by the data subject. Personal data cannot be accumulated for secondary uses.

To allow recycling, repurposing and re-contextualisation [74], personal data should be further processed in compliance with specific principles and requirements, aimed at tackling the above-mentioned risks. As a general rule, according to art. art. 5(1)(b) GDPR, personal data cannot be processed for further purposes which are incompatible with the one justifying the first collection. The only exception is given by Art. 89 of the GDPR, introducing *safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes*.[48]

3.3.1. Compatibility test *ex* art. 89 GDPR: data aggregation, statistical purposes and data sharing

Art. 89 recalls the reason of substantial public interest for implying certain derogations in the secondary processing of data. Among these, the case in which personal data are processed for

[48] In detail, Art. 89: Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

1. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

2. Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

3. Where personal data are processed for archiving purposes in the public interest, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18, 19, 20 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

4. Where processing referred to in paragraphs 2 and 3 serves at the same time another purpose, the derogations shall apply only to processing for the purposes referred to in those paragraphs.

statistical purposes *ex* Art. 89. Union, or Member States' law may provide for derogations from the mandated disclosures, contained in Articles 13[49] and 14[50] of the GDPR.

[49] In detail: Article 13. Information to be provided where personal data are collected from the data subject
1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:
(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;
(b) the contact details of the data protection officer, where applicable;
(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
(d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
(e) the recipients or categories of recipients of the personal data, if any;
(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international
organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable
safeguards and the means by which to obtain a copy of them or where they have been made available.
2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:
(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
(c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
(d) the right to lodge a complaint with a supervisory authority;
(e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible
consequences of failure to provide such data;
(f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.
4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.
[50] In detail: Article 14. Information to be provided where personal data have not been obtained from the data subject
1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:
(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;
(b) the contact details of the data protection officer, where applicable;
(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
(d) the categories of personal data concerned;
(e) the recipients or categories of recipients of the personal data, if any;
(f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

Statistics is included among these derogations. Statistics, namely, public statistics, is necessary for the performance of EU activities, as confirmed in the Treaty on the Functioning of the European Union (TFEU)[51].

Generally carried out in the public interest, this kind of processing is usually performed by public authorities. Their legal status makes them naturally trustworthy in tackling the risks. If we think, for example, of National Statistical Offices (NSOs), thirty years ago they were the only ones gathering data on citizens and they were naturally trusted as data controllers. For this

2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:
(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
(b) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
(c) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;
(d) where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
(e) the right to lodge a complaint with a supervisory authority;
(f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;
(g) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
3. The controller shall provide the information referred to in paragraphs 1 and 2:
(a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;
(b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or
(c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.
4. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.
5. Paragraphs 1 to 4 shall not apply where and insofar as:
(a) the data subject already has the information;
(b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;
(c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or
(d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

[51] To this purpose, Art. 338 clarifies that the European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall adopt measures for the production of statistics where necessary for the performance of the activities of the Union.

reason, the statistical activity conducted by NSOs is even regulated with a specific legislation that represents the main legal framework for national statistics.[52]

Nowadays, however, business entities also perform data processing for statistical purposes. For example, economic actors focused on the development of Artificial Intelligence applications and Data Analytics models (including Machine Learning, Deep Learning and other techniques). They rely on statistical models built with a remarkable collection of statistical data. Due to its descriptive function, statistics reveals patterns and infers information observing data, granting a solid base for the development of the statistical models needed by this industry. Therefore, data controllers can be also private entities, therefore it appears more than reasonable to question the level of trust citizens should recognise, especially in light of the risks for privacy and data protection[78].

The implications for data controllers pursuing data processing for statistical purposes, dealing with aggregate data for the development of Artificial Intelligence applications, do not seem to be clear, exposing data subjects to the risk of deanonymisation/re-identification when data are poorly processed, thus impacting the quality. Therefore, it is reasonable to ask whether art. 89 of the GDPR applies to private companies as well, relying on statistical data for developing data analytics models [79].

To this extent, it can be noted that the taxonomy of the GDPR does not specifically define statistical data, but considers aggregate data as non-personal data, as the output of personal data processed for statistical purposes.

The Regulation defines processing for statistical purposes as "*any operation of collection and the processing of personal data necessary for statistical surveys or for the production of statistical results*". Moreover, the FFDR states that specific examples of non-personal data include aggregate and anonymised datasets used for big data analytics.[53]

[52] Regulation 223/2009 on European statistics. For microdata access: Regulation (EU) No 557/2013 on access to confidential data for scientific purposes. Separate laws in the EU/EEA/EFTA countries: https://ec.europa.eu/eurostat/web/ess/latest-news

[53] See extensively Recital 9 of the FFDR, literally: *The expanding Internet of Things, artificial intelligence and machine learning, represent major sources of non-personal data, for example as a result of their deployment in automated industrial production processes. Specific examples of non-personal data include aggregate and anonymised datasets used for big data analytics, data on precision farming that can help to monitor and optimise the use of pesticides and water, or data on maintenance needs for industrial machines. If technological developments make it possible to turn anonymised data into personal data, such data are to be treated as personal data, and Regulation (EU) 2016/679 is to apply accordingly*.

The literal and contextual interpretation introduces a presumption on the nature of aggregate data as non-personal data: as such, aggregate data do not fall under the scope of application of the GDPR.

However, while this approach may be effective for aggregate data resulting as the output of processing non-personal data (farm and agricultural data, for example), it is not the case for the output of processing personal data. A distinction should be made in terms of the nature of the input/output data. In this regard, the European Data Protection Supervisor (EDPS) specified that aggregate data is not the same as anonymised data, and not necessarily non-personal data[54], however recalling Recital 26 as a main tool for ascertaining the risks, but which is still not a certain method of assessment.

Apart from these critical points, which certainly deserve attention from the data controller perspective, the GDPR imposes a compatibility test to be carried out in order to evalute whether secondary processing can be considered compatible. In this sense, Art. 6(4) of the GDPR follows, providing a series of criteria to determine whether the processing for a purpose other than that for which the personal data have been collected, is to be considered compatible with this initial purpose.

The GDPR requires a compatibility test for further purposes to be carried out.

[54] European Data Protection Supervisor, Opinion 3/2020 on the European Strategy for Data.

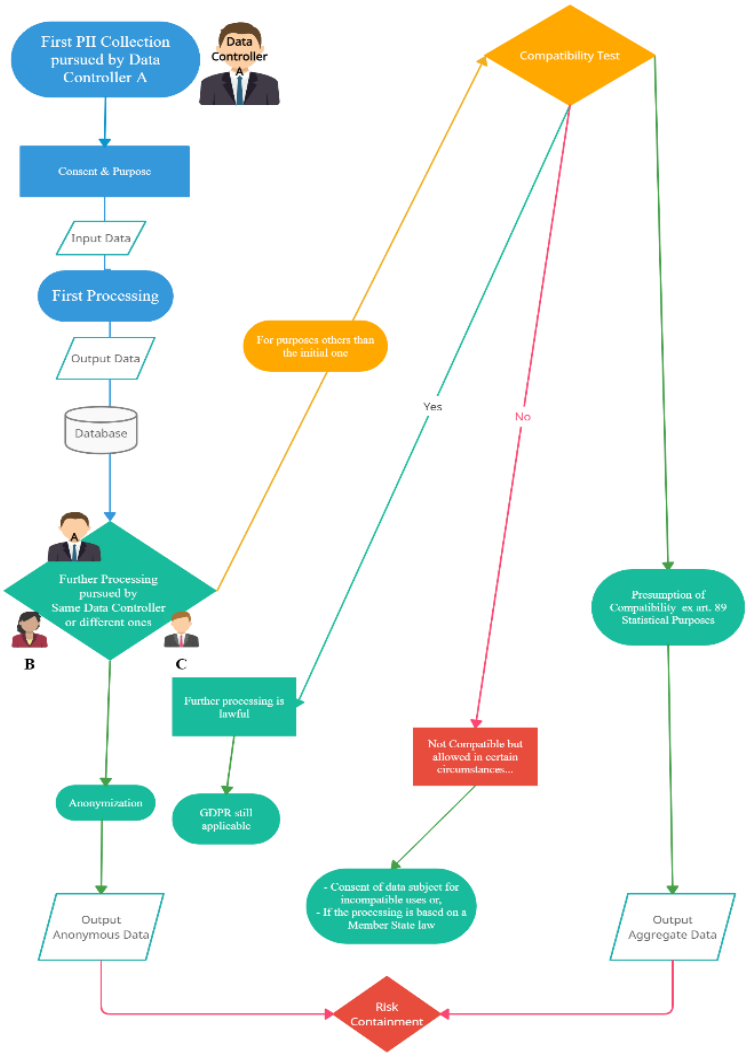


Fig. 5. Data processing in light of the GDPR perspective, with a particular focus on further processing and secondary uses of data

Two basic scenarios may occur with the compatibility test:

- The purpose is compatible; thus, the further processing is lawful and GDPR still applies to the further processing. In this case, recycling, repurposing, and re-contextualising is lawful.
- The purpose is not compatible; thus, the further processing is unlawful (unless consent has been obtained for incompatible uses, or the Member States law allows further processing).

Article 89 deserves a specific focus, as it lists other cases in which the compatibility test is not required, based on the presumption that the processing is considered compatible with the initial purpose. This is the case of *processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes*.

All these exemptions are somehow related to statistical processing, research included, for which scholars are currently exploring its boundary [80] [75][81], output which – as anticipated - is considered as non-personal data (aggregate data), thus outside the scope of application of the GDPR.

In this regard, especially from a legal-technological perspective, data aggregation is poorly investigated. Aggregation allowing secondary uses of data poses certain risks when poorly performed: disclosure, re-identification, and profiling.

The aggregation process has the advantage of transforming sets of microlevel data (thus PII referring to each single statistical unit) into macrolevel data [82] representing a summary of Personally Identifiable Information (PII) [83] .

From a purely legal point of view, the interaction between data protection, data aggregation and statistical purposes can be very controversial.

Data aggregation plays an essential role in data processing and data management. In the modern information systems, it allows information to be inferred from unusual patterns [84], bandwidth and energy costs to be reduced [85], and storage space to be saved [86]. Aggregate data is the main source of IoT systems, Cloud environments, Artificial Intelligence and Machine Learning applications and products. Within such systems, different aggregations may have various requirements to be satisfied by the design. For instance, while one aggregation receives data passively from a data source, another aggregation must actively collect data from a database which is shared concurrently by other processes [87].

This heterogeneity represents a challenge in designing a suitable solution with multiple aggregations, certainly increased when processing data of a different nature (considered from a legal point of view). Certain products and services built on aggregate data cannot even be developed without processing personal data, and data cannot always be directly acquired for individuals with informed consent[55].

When Article 89 recalls processing for statistical purposes, it lists such processing together with a broad range of processing activities: archiving, historical and scientific research. These are somehow related to the statistical processing which serves public interest.

However, there are many other types of activities that certainly cannot be considered as undertaken in the public interest, but they may also fall under this provision, especially if the

[55] This might eventually be the ratio behind Article 14 of the GDPR: Article 14 GDPR - *Information to be provided where personal data have not been obtained from the data subject*.

presumption of compatibility - as mentioned above, is considered. This has also been specified by the Working Party 29 Opinion 03/2013 on purpose limitation.[56]

The level of protection, between the public and the private sector, might be very different.

In the field of statistics performed in the public sector, the principles of statistical confidentiality and functional separation[57] impose certain measures to ensure that personal data processed for statistical purposes cannot be used for non-statistical purposes.

As already mentioned, some authors [79] have already pointed out that corporations might not have the same level of ethical and institutional safeguards in place as the public sector. Furthermore, corporate secrecy and opaque algorithms in AI research might create barriers to oversight. These are the limits faced by Article 22 of the GDPR on automated individual decision-making and right to explanation.

With this scenario, defining a proper risk assessment may be very difficult but the function of data protection should not be neglected, and an oversimplified approach should not be applied [88].

Therefore, aggregate data should require an appropriate risk test, which should be mandatory when performed by private entities.

As anticipated, the GDPR only imposes that such processing should be subject to appropriate safeguards for the rights and freedoms of the data subject. The application of these derogations implies that it must be "*likely to render impossible to or seriously impair the achievement of the specific purposes, and such derogations should be necessary for the fulfilment of those purposes*".

Member States should determine the scope of the derogations, however this creates fragmentation between policies, thus creating disparities within the Digital Single Market[58].

---

[56] Working Party 29, Opinion 03/2013 on purpose limitation, adopted on 2 April 2013.

[57] Regulation (EC) No 223/2009 on European Statistics defines statistical confidentiality as "the protection of confidential data related to single statistical units which are obtained directly for statistical purposes or indirectly from administrative or other sources, implying the prohibition of use for non-statistical purposes of the data obtained and of their unlawful disclosure". See also Article 20(1) and (2) of the same regulation which sets out that "confidential data obtained exclusively for the production of European statistics shall be used by the [national statistical institutes] and other national authorities and by the Commission (Eurostat) exclusively for statistical purposes unless the statistical unit has unambiguously given its consent to the use for any other purposes". Further, see Article 338 of the Treaty on the Functioning of the European Union ('TFEU'), which requires that "the production of Union statistics shall conform to impartiality, reliability, objectivity, scientific independence, cost-effectiveness and statistical confidentiality".

[58] As an example, the case of the Italian Data Protection Authority (Garante per la Protezione dei Dati Personali) can be recalled, which has issued two notes introducing deontological rules regulating processing for statistical purposes, equalizing the rules to be applied when processing for statistical purposes in both the public and private sector, even if specifically determining the level of aggregation. Cfr: Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del Sistema Statistico nazionale pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101 - 19 dicembre 2018 [9069677]; Regole deontologiche per

In addition, Article 89 requests that technical and organisational measures are in place to ensure respect for the principle of data minimisation. To this aim, the article seems to emphasise a kind of circular reasoning typical of the GDPR, where rules and principles are repeatedly recalled, posing uncountable doubts and challenges. Namely, Article 25 on Data Protection by Design and by Default, as well as Article 5 on Data Minimisation.

In both cases, data protection methodologies and rigorous PETs (Privacy Enhancing Technologies) should be created, while recalling a very broad view of these "*technical and organisational measures*". Certainly, there is no doubt that the legislator favoured broad statutory language, avoiding any specification on technologies and methodologies, in favour of technological neutrality. However, it actually becomes very difficult for companies to navigate through the principles of data protection. These open standards might represent a remarkable limit for small medium enterprises.

With regard to the part in which Article 89 overlaps with Art. 25 - in the technical and organisational measures - the legal uncertainties pertaining to Art. 25 spill over into Art. 89 [89].

Secondly, regarding minimisation techniques, academics [77] have already discussed the edges of the data minimisation principle in the current structure of the GDPR[59]. Again, the regulation is not providing a pragmatic view of data hygiene: determining how and where to start with data minimisation becomes very difficult.

How can the GDPR's core principles be translated into concrete design requirements and data protection methodologies? How can a compliant internal policy, for small-medium enterprises, be technologically designed?

With regard to aggregation, can all these questions possibly be solved determining ex-ante how large the aggregate should be, before the data cease to be personal? Is it feasible to determine such a benchmark? Or, somehow, does it appear to be impossible to determine it, due to the available technology and the technological development in the digital context?

It should be clearly specified how data protection principles relating to data minimisation and purpose limitation should apply to processing for statistical purposes. The main need is

trattamenti a fini statistici o di ricerca scientifica pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101 - 19 dicembre 2018 [9069637].

[59] Literally, the authors confirm that *purpose limitation and data minimisation remain feasible albeit challenging in the context of data-driven personalisation, profiling and decision-making systems. While the longer-term research problems await their solutions, practitioners might employ a variety of organisational best practices and off-the-shelf tools that minimise data even if not explicitly developed for minimisation purposes.*

overcoming the legal uncertainty which surrounds the GDPR and its further application of rules and principles, which appear as open standards.

Theoretical solutions and explanations are required, especially in the light of the growing phenomena of data deanonymisation/re-identification.

Recent developments and legal initiatives, namely the new Data Governance Act or the new proposal on Artificial Intelligence (AI ACT proposal), have demonstrated that several AI-related questions do not find an explicit answer in the GDPR. In the Data Governance Act, the European legislator proposes data altruism processing with supervision by data sharing services. In the AI Act proposal, the data management supporting AI applications and products should be documented and archived with particular regard to training, validation and testing data aimed at demonstrating that the AI tools remain within the limitation of the purposes defined *ex-ante*. This situation of legal uncertainty, and imperfect integration with different legislation initiatives probably led by different industrial market interests, creates an overburden for data controllers applying indeterminate concepts, vague clauses and open standards, particularly challenging for small-medium enterprises, which can be penalised. In addition, it increases the risk of deanonymisation/re-identification for data subjects.

It appears noticeable that, if data controllers cannot determine and quantify the residual risk linked to a data lifecycle, the GDPR may be reduced to a mere bureaucratic procedure based on a checklist, performed with automatic tools, from which big corporations can take advantage, as evidently more resourceful. In this situation data subjects would appear to be penalised.

To this extent, determining the clear boundaries of the risks seems to be the most practical solution for tackling it.

3.4. An explorative literature review on data deanonymisation

While the collection of personal data provides for a better definition of personal profiles, improving efficiency, on the other hand profiles can be used not only for granting access to certain services, but also to refuse it. The same data collected for tailoring a 100% satisfactory customised service can be used for decisions based on opacity.

One of the main risks linked to secondary uses of poorly processed personal data relies on the possibility of reverse-engineering the process of data protection and re-identifying the subject to whom the data refer.

In this regard, the European Union and the Member States has implemented many policies aimed at containing these risks. The evolution of the legislation in the last decade shows that, as a first step, the legislator blazed the path for approaching the issue from an objective perspective thus, recalling certain safeguards on the data processing *per se*. In this sense, with the GDPR having imposed the basic principles of data processing (art. GDPR) such as minimisation and erasure, or introducing certain guidelines aimed at countering the dark side of data protection: deanonymisation and re-identification. Finally, in recent years, the European legislator implemented new policies focused on a subjective perspective, aimed at empowering and instilling responsibility in actors involved in the data processing. The Data Governance Act represents a step towards data circulation and data sharing aimed at granting data reuses, while protecting data and data subject's privacy.

Therefore, in a digital ecosystem where data subjects generate data, data collectors use data, the ideal situation would be:

- allowing data subjects to limit the information collected about them
- granting the maximal potential on the reuse of data collected and processed to data users.

This paragraph aims to frame the technological development of the deanonymisation/re-identification risk, querying *Arxiv* (https://arxiv.org/), an Open Access archive for scholar pre-prints in the fields of physics, mathematics, computer science, quantitative biology, quantitative finance, statistics, electrical engineering and systems science, and economics, thus merely referring to the technical field and not to the legal one. Containing pre-prints, Arxiv is considered to provide a better representation of the topic development, establishing the main trends in the topic.

The exploratory literature review on the topic outlines the technological development on the topic, identifying the state of the art. A literature analysis leads to a better definition of the gaps in the body of the in-force legislation, understanding whether the legal framework is in line with the technological development.

In scientific literature the keywords deanonymisation and re-identification are used in an undifferentiated way (at least from an etymology perspective) [90], for referring to the practice of reverse-engineering the processing of personal data anonymisation [17, 91], identifying the natural person whose personal data have been processed aiming at reaching anonymity. Therefore, if such a process is reversed, the process of reaching data anonymity is impacted, producing effects on privacy and data protection of data subjects.

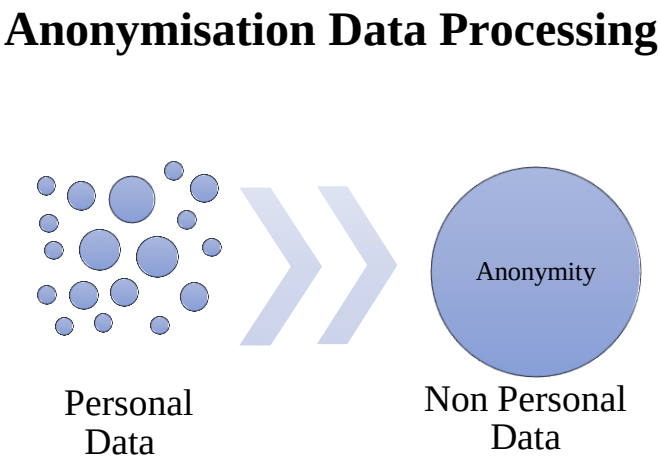


Fig. 6. The legal semantic process from personal data to non personal data

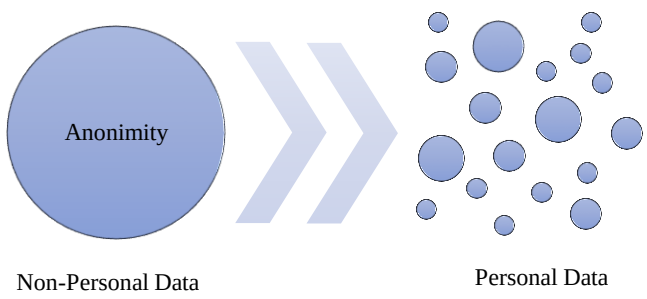


Fig. 7. The legal semantic process from non-personal data to non-personal data

Moreover, still considering the terminology, some scholars [17] highlighted that in some jurisdictions (such as US, Canada, and Australia), deanonymisation is used to mean what anonymisation means in the EU context. A literature review shows that the same approach is used for the two words re-identification (US, Canada, and Australia) and deanonymisation in the EU context.

First of all, it must be clarified that the technical literature on the topic does not refer to *personal data* solely in name – as usually referred in legal terminology. Specifically, it refers to Personally Identifiable Information (PII), with the same meaning as personal data. As anticipated, the concept of PII is particularly relevant in the context of data processing and data protection, as there is no unique definition [92] [93–95][94] [96][97].

In taking into account the GDPR, the definition of personal data contained in Art. 4 recalls *any information related to an identified or identifiable natural person*[60], in line with the previous definition recalled in Directive 95/46/EC of the European Parliament and Council of 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data[61], as the in-force legislation for data protection prior to the GDPR.

Both of these definitions of personal data have their roots in the 1980 OECD Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data[62] which has played a pivotal role in the development of policies for the protection of personal data, and remains an essential benchmark.

[60] Art. 4(1) specifies that, *for the purposes of this Regulation: 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*; […].
Moreover, in detail: Article 2, Article 4(1) and (5) and Recitals (14), (15), (26), (27), (29) and (30) of the GDPR; Article 29 Working Party Opinion 4/2007 on the concept of personal data; Article 29 Working Party Opinion 05/2014 on Anonymisation Techniques.

[61] Article 2 specifies that, *for the purposes of this Directive: (a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*; […].

[61] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

Since the OECD Recommendation, PII has not been defined *per se* by a list, but rather accounts for the possibility of deductive disclosure. Therefore, if taken into account the in-force legislation, PII can be considered as any *identifier* such as a

- *name*
- *identification number*
- *location data*
- *an online identifier*
- *one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity*

of a natural person.

In general, a common misconception on data anonymisation exists: removing all explicit identifiers from a dataset makes data anonymous. If this approach was considered to be true in the 70s, when Statistical Agencies used to apply anonymisation to microdata, with the advent of Big Data and its continuously increasing availability, anonymisation becomes a remarkable challenge to address, while rendering deanonymisation/re-identification easier.

According to these premises, the explorative literature review aims to determine the extent of the deanonymisation/re-identification risk.

The first outcome to be analysed is the number of publications per year, with a total of 1467 papers from 2016 to 2022.

	2016	2017	2018	2019	2020	2021	2022
Tot	70	109	189	259	324	345	171

Fig. 8. Total number of publications per year concerning the topic of deanonymisation/re-identification

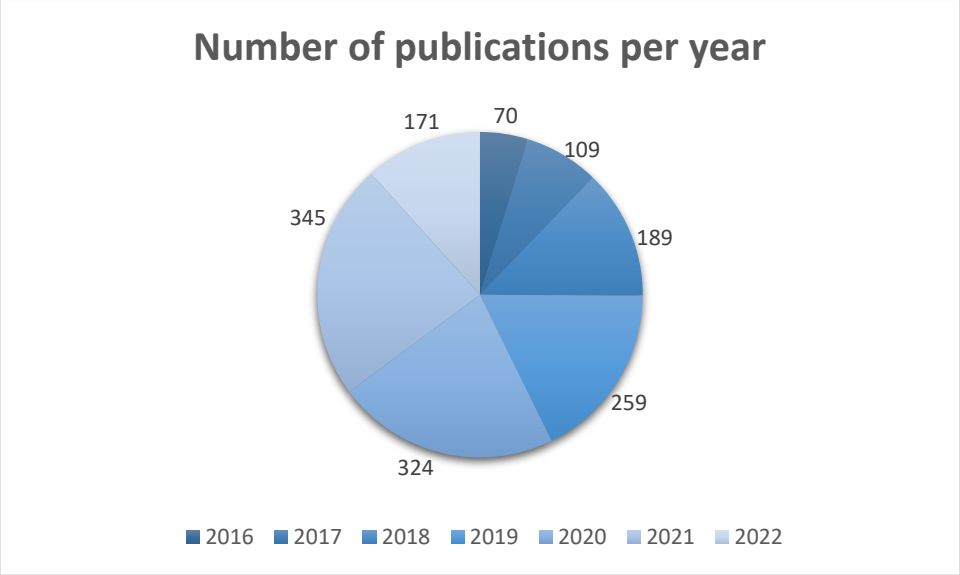


Fig. 8.a. Pie chart of the total number of publications per year concerning the topic of deanonymisation/re-identification

The pie chart shows that in the transition from the previous Data Protection Directive to the GDPR, from 2016 to 2018 – the year in which the GDPR entered into force – the technological development in deanonymisation/re-identification increased. Despite the GDPR introducing new and stricter rules for the protection of personal data, the majority of papers on the topic were published in between 2019 and 2022.

Concerning the keywords (deanonymisation/re-identification) used in the exploratory review, despite being used, as anticipated, in an undifferentiated way for referring to the same concept, scholars tend to prefer the use of the word re-identification.

	2016	2017	2018	2019	2020	2021	2022	TOT
de-anonymization	11	8	13	20	17	16	9	94
re-identification	59	101	176	239	307	329	162	1373
tot	70	109	189	259	324	345	171	1467

Fig. 8.b. Chart of the total number of publications per year based on keywords

As anticipated, in the technical domain, the words deanonymisation and re-identification tend to be used with the same meaning, even if a preference for the latter is registered.

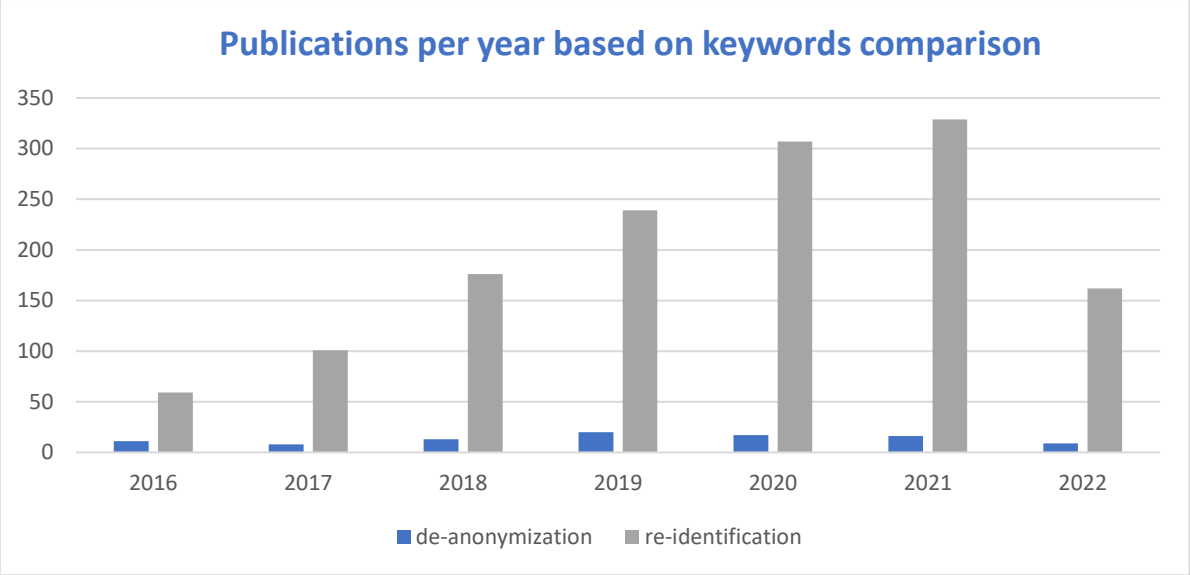


Fig. 9. Bar chart of the number of publications per year, based on keywords comparison

The content of the explorative literature review shows that deanonymisation/re-identification can be performed not only using auxiliary data (*seed-based deanonymisation*), thus data gathered in any kind of contexts private or public, but also with no auxiliary data (*seed-free deanonymisation*). Therefore, this consideration makes the semantic difference introduced by the European legislator between personal and non-personal data totally irrelevant.

Moreover, it shows that even in the case of sophisticated anonymisation techniques[63], the strength of protection is impacted more in structured data (such as microdata contained in databases and other repository) than in unstructured data. Rich auxiliary information, also called *background information*, is mainly available for structured data. Therefore, the state-of-the-art shows that most papers are focused on the deanonymisation/re-identification of structured data, therefore in these cases the techniques are more consolidated. However, it also shows several limitations such as the imprecision of the background knowledge used to deanonymise or the a possible lack of accuracy as they rely on limited structural data.

Such limitations and constraints represented the main background used to develop new deanonymisation/re-identification techniques without auxiliary knowledge (*seed-free or blind deanonymisation/re-identification*)[98], mostly tailored for unstructured data, between the early 2000s and 2022, most probably due to the increase in the Big Data technologies.

[63] In this regard, the main reference is to differential privacy which is currently considered one of the main data protection models, even if academics have already begun to question its efficiency. See in detail in Chapter 3.

Lastly, the technological literature analysis aimed to highlight the difference in the perception of the topic among technicians (IT, data scientist, statisticians etc.) and jurists.

The aim is to analyse the technological development provided with the articles using a legal lens, thus recalling the three main deanonymisation/re-identification technique mentioned in the unique institutional guideline (WP29 05/2014):

- singling-out
- linkability
- inference

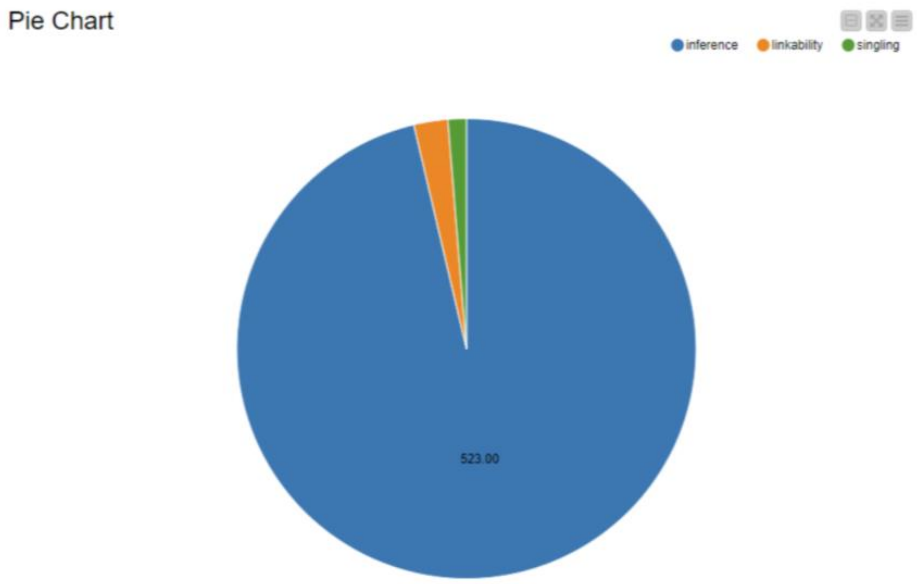


Fig. 9.a. Pie chart of recurrence recalled by the institutional guideline on anonymisation and consequent issue of deanonymisation/re-identification

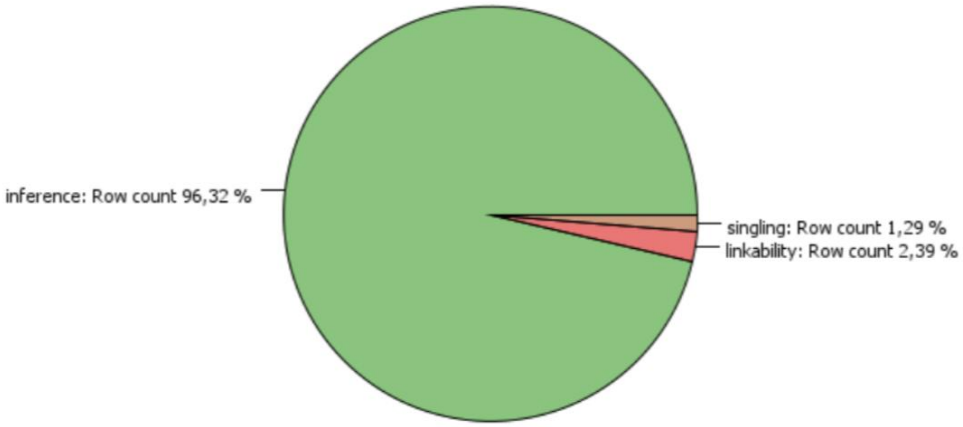


Fig. 9.b. Pie chart of the percentage of recurrence (singling out, linkability, inference)

As shown in Fig. 9.a. and Fig. 9.b. the word recurrence presents the highest percentage for inference, thus most likely the technique of singling out and linkability may be combined with inference to deanonymise personal data.

Chapter 4. *An Empirical Observation of Data Deanonymisation Spectrum in Further Data Processing: Forgetting by Reusing?*

Index of the Chapter

Short Abstract of the Chapter

This chapter provides a sample of the empirical legal research on the technological development of the deanonymisation issue, from 2016 to 2022, with a statistical analysis and a visual representation of the outcome by continental jurisdictions. The statistical analysis shows which continental jurisdictions invest more in researching the deanonymisation issue, and thus have a greater technological development. Moreover, it investigates the correlation between such trends and different continental approaches to data, namely centralised and de-centralised, demonstrating to what extent the right to be forgotten ex Art. 17 of the GDPR can

be granted. Moreover, the analysis investigates the evolution of the technological development before and after the entry into force of the GDPR.

The papers collected for the empirical legal research provided in this chapter are indexed and annexed to this chapter.

Based on the grounds of the explorative literature review on data deanonymisation presented in Chapter 2, this chapter analyses the deanonymisation issue in light of the sole institutional guidance on deanonymisation: the Working Party Opinion 05/2014 on anonymisation techniques. As such, papers are grouped into three main deanonymisation techniques: singling-out, linkability, inference.

As the European institutions consider presenting a new guidance on the issue in the forthcoming months, this chapter will integrate it with a comparative analysis.

4.1. Statistical Analysis of the Deanonymisation Spectrum Risk

As anticipated, the main institutional reference to the risk of deanonymisation/re-identification comes from the Working Party 29 Opinion 05/2014 on anonymisation techniques. Many things have changed the publication of this opinion, but, for the time being, this opinion still represents a guideline in the evaluation of the level of data anonymity granted using the anonymisation model in processing data.

Referring to Chapter 3 with regard to the specificity of each technique, this chapter focuses on the main declinations of the risk, as specifically recalled in the Opinion.

In fact, the WP29 request the testing of the robustness of the chosen technique against three declinations of the de-identification/re-identification risk, therefore whether:

- it is still possible to single out an individual
- it is still possible to link records relating an individual
- information concerning an individual can be inferred.

The anonymisation technique should prevent the risk of singling-out an individual, the risk of linking records and the risk of inference, thus respectively singling out an individual, or linking her/his data, or inferring knowledge from an individual with or without auxiliary knowledge.

In line with this premise, this paragraph aims to frame the technological development in these three declinations of deanonymisation/re-identification, as well as showing the spread of it among continental jurisdictions. Moreover, it pictures the trend in technological development in the transition from the previous legislation to the entry into force of the GDPR.

	2016	2017	2018	2019	2020	2021	2022	TOT.
Singling-out	7	5	11	9	21	22	15	90
Linking	38	42	58	58	94	91	62	443
Inference	19	31	64	105	204	312	208	943

Fig. 10. Table representing the number of publications per year

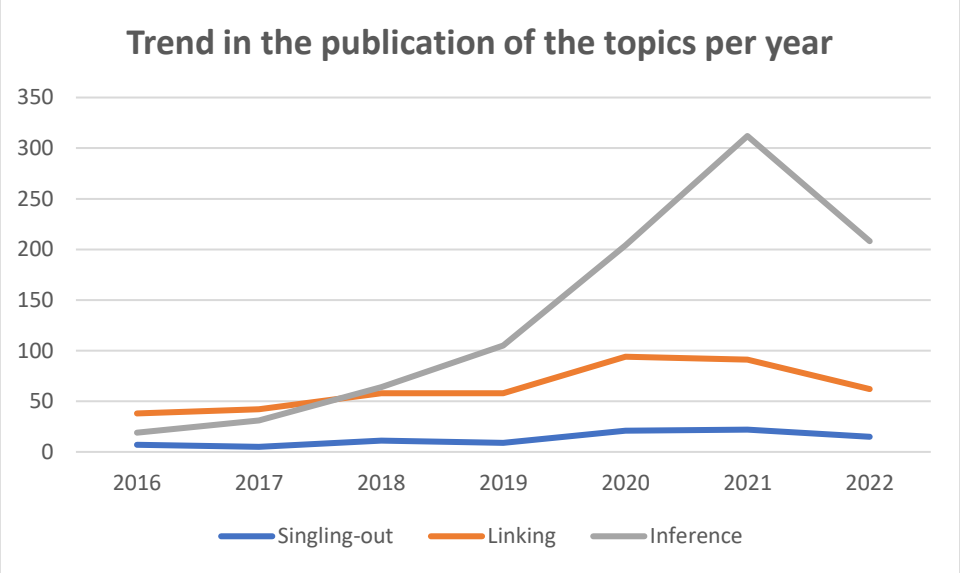


Fig. 11. Trend in the publication of topics per year

Figures 10 and 11 show the evolution of the topic in the number of publications.
The technological development of the techniques seems to be impacted differently in the transition from the previous legislation on data protection and the GDPR.
The technological development of singling out seems constant in time, registering a small increase between 2019 and 2022 but overall remaining constant. The same considerations are valid for the technique of linking multiple records relating an individual.
The technological development of the inference technique is remarkably different, which registered a notable increase, especially from 2019 to 2021.
Therefore, data shows that despite the GDPR becoming directly applicable in 2018, the technological development of deanonymisation/re-identification has not been impacted and the number of publications has continued to grow by year. The only exception is represented by the technological development of the inference technique, which registered a remarkable growth from 2019 to 2021.
Lastly, it should be considered that data was collected until August, thus the decreases registered from 2021 to 2022 may be linked to the incomplete representation of data.

The following charts and graphs represent the technological development of the deanonymisation/re-identification techniques as listed in the WP29 Opinion on Anonymisation Techniques no. 05/2014, namely singling out, linkage and inference.
The study is conducted collecting and analysing the number of publications by year and by continental jurisdictions.

	Africa	America	Asia	Europe	Multiple C	UK
2016	0	1	1	3	0	2
2017	0	0	1	4	0	0
2018	0	3	3	2	2	1
2019	0	5	4	0	0	0
2020	0	7	5	8	0	1
2021	0	8	7	7	0	0
2022	0	7	3	4	0	1

Fig. 12. Chart of singling out technological development values

This first chart collects the number of publications per year and continental jurisdiction, from 2016 to 2022. It is easily noticeable at a glance that such techniques are not common, and its technological development is lower compared to the other techniques.

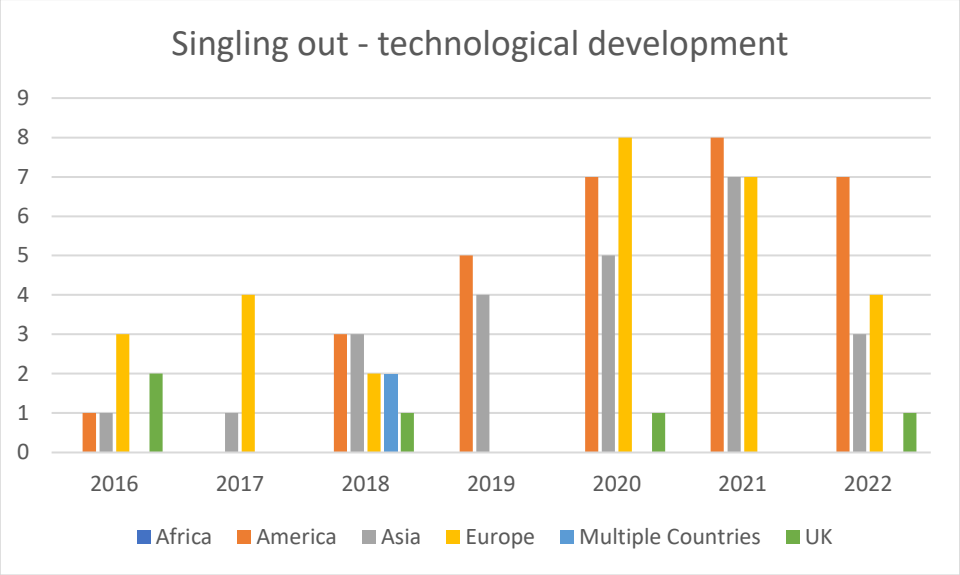


Fig. 13. Graph of singling out technological development by year and continental jurisdictions

The graph shows the comparison of continental jurisdictions per year, from which it emerges that America holds the highest number of publications, thus can be considered as the leading country in technological development and represents a trend setter. Asia and Europe follow the lead, while a lesser contribution is provided by UK and lastly, by Africa which seems not to take part to the academic debate.

	Africa	America	Asia	Europe	Multiple C	UK
2016	0	9	11	15	1	2
2017	1	18	8	11	0	4
2018	1	26	21	8	0	2
2019	0	25	16	12	2	3
2020	1	33	27	27	1	5
2021	0	27	34	25	0	5
2022	0	21	16	19	0	6

Fig. 14. Chart of linkage technological development values

Figure 14 shows the number of publications by year and continental jurisdictions of the linkage deanonymisation/re-identification techniques.

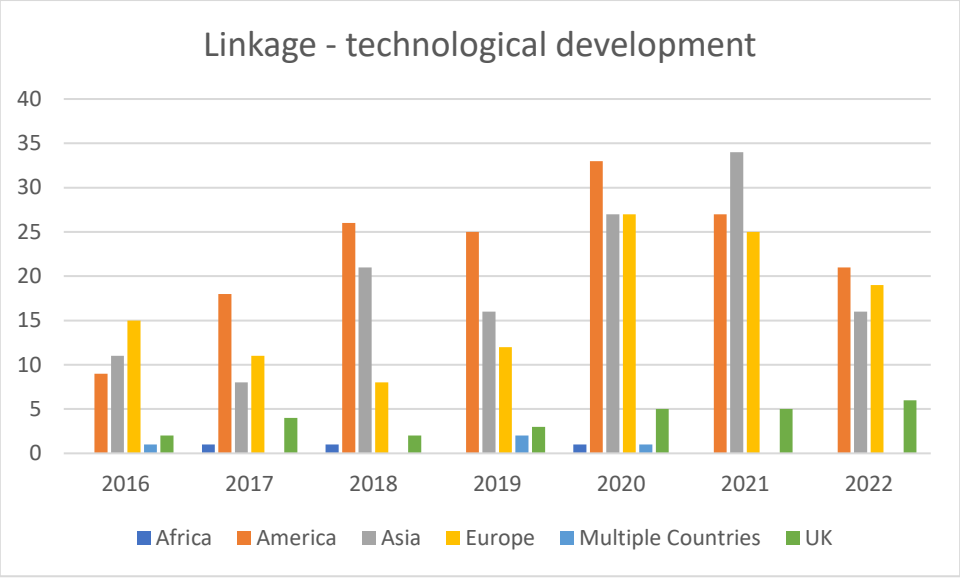


Fig. 15. Graph of technological development by year and continental jurisdictions

Figure 15 shows the comparison of continental jurisdictions by year, from which it emerges that Asia and America are the trendsetters in the technological development of data linkage. Especially from 2021, Asia has led the academic debate on this deanonymisation technique, followed by America and Europe which have almost proportional values. UK and multiple other countries are also participating in the debate, while Africa only has a small "voice" with only few publications.

	Africa	America	Asia	Europe	Multiple C	UK
2016	0	6	3	5	0	5
2017	0	18	2	5	1	5
2018	0	38	4	9	2	11
2019	0	52	18	21	3	11
2020	0	97	56	35	3	13
2021	0	150	83	60	3	16
2022	0	97	57	36	3	15

Fig. 16. Chart of inference technological development values

Figure 26 presents a chart on the technological development values on data inference from 2016 to 2022, among continental jurisdictions, from which it is evident that Africa is not taking part in the academic debate.

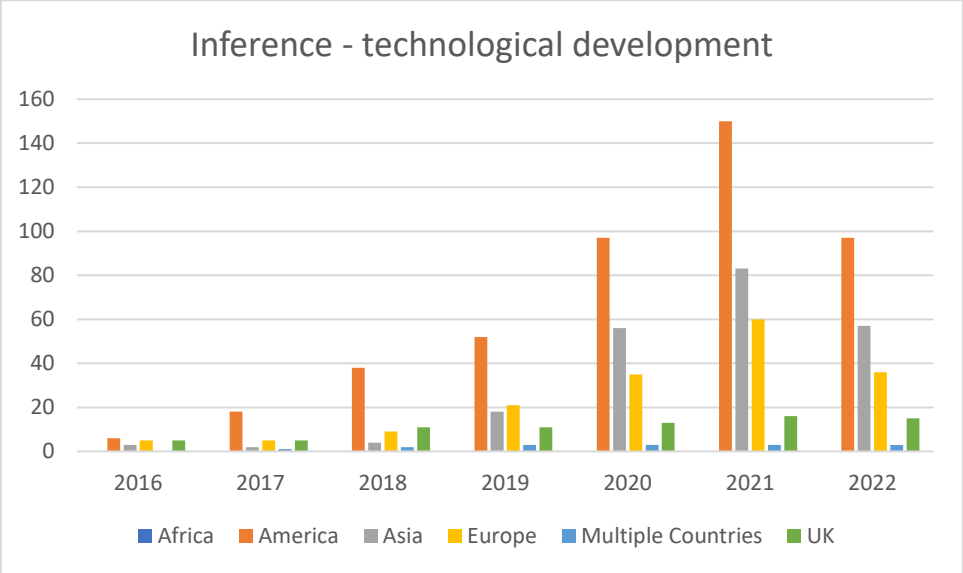


Fig. 17. Graph of inference technological development by year and continental jurisdictions

Figure 17 shows the comparative values between continental jurisdictions by year, from which it emerges that America is leading the technological debate, thus the technological development, on data inference for deanonymise data. It is followed by Asia and Europe, while UK and other countries give a smaller contribution. Again, Africa is not participating to the academic debate.

From the comparative analysis of the previous figures (in this paragraph) it can be inferred that America and Asia are leading the debate on data deanonymisation/re-identification, providing

the advance in the technological development of such techniques. Considering this evidence, it could certainly be beneficial to outlaw such techniques in Europe, especially considering the fact that Europe doesn't seem to have a central role in the debate. The know-how developed by the leading countries can make data of other countries vulnerable and almost everything can lead to difficulties in granting data subjects' rights protection due to misuses.

As a last note, the scientific literature gathered on the topic allowed an analysis on the term recurrence to be performed, recalling 3 (three) terms that represent personal data *ex* art. 4 of the GDPR: name, IP, location. The following pie chart shows the main words recalled:

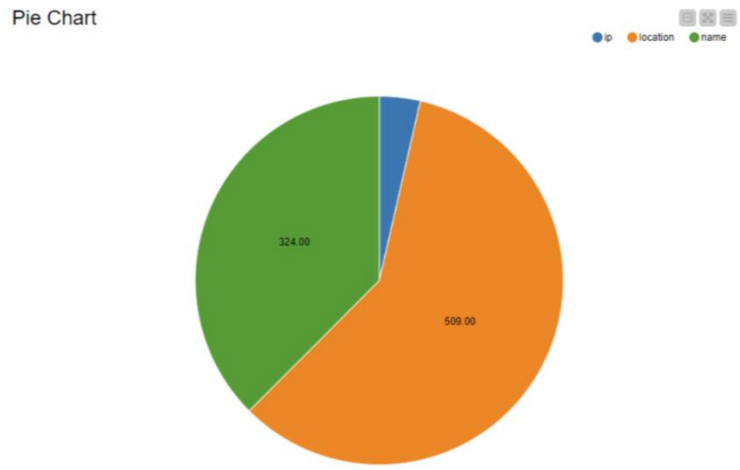


Fig 18. Pie Chart of term recurrence

In the following figure the related percentages are provided:

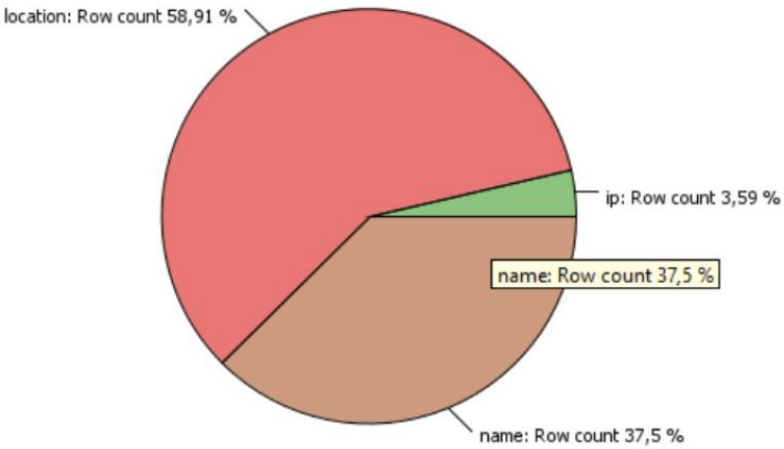


Fig. 18.a. Pie chart of percentage term recurrence (name, location, IP)

Figures 18. and 18.a. show that the major development of the deanonymisation/re-identification techniques pertains to location data with a percentage of 58.91%. The deanonymisation techniques used to deanonymise names recur less than the ones on location. Last are the ones used for the IP with 3.59%.

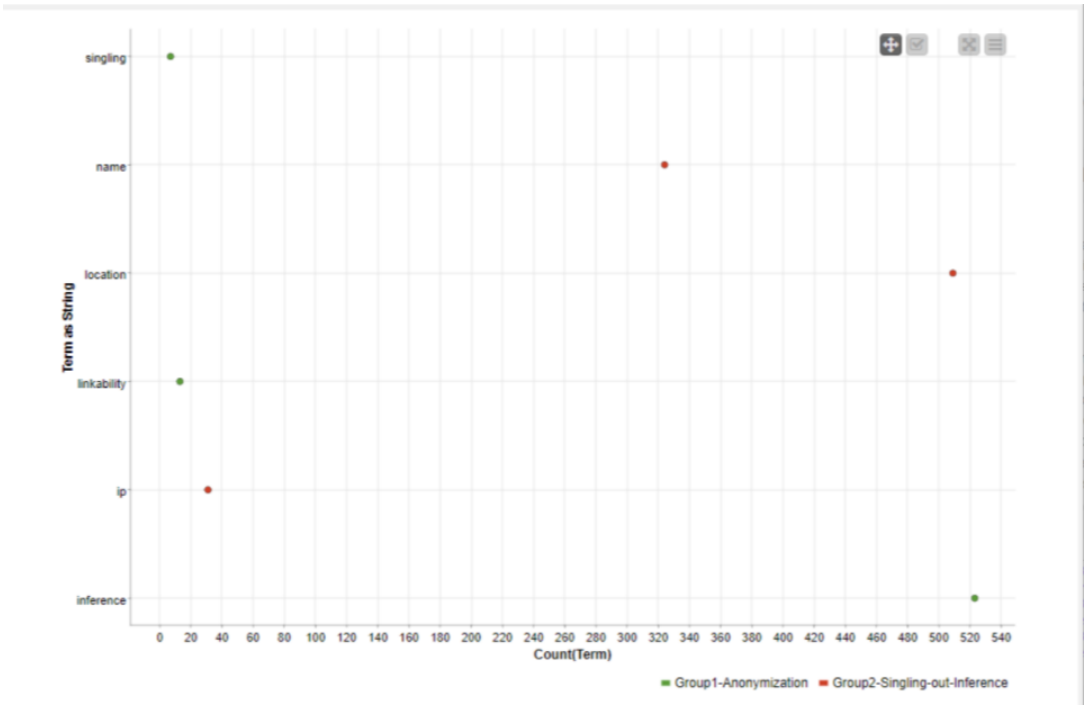


Fig. 19. Term recurrence comparison in the literature recalled in Annex I, II, III, IV and V.

4.2. Further Data Processing and Sharing: Forgetting or Not Forgetting? An Old Problem Under a New Guise

Data misuse certainly has an impact on the values introduced by the GDPR. The right to erasure (right to be forgotten) has been widelyanalysed and investigated in literature, as it raised interest not only in Europe but all around the world. Traditionally the right to be forgotten has been studied and investigated as the right recognised for data subjects to erase their information appearing online (personal data), that is considered harmful, therefore solely limited to personal data. This right must overcome many balance tests with other fundamental rights in trials, and still nowadays it seems that there is still room for this right to take shape. In fact, of the main problems of the right to be forgotten lies in the existing lack of hierarchy of the respected fundamental rights concerned [160]. In this regard, the Courts are certainly involved in defining the presumption of supremacy among fundamental rights[64] but, for the time being, there is no evidence of trials concerning the impact of the deanonymisation/re-identification risk on the right to be forgotten, and the risk of that becoming a dead letter in the GDPR.

There is no empirical evidence that data can be deanonymised thus, data subjects are not potentially able to ascertain any violation in this sense. From the opposite perspective, there is effective legislation punishing such practices.

Only a more efficient and clear legislation can help tackle such a risk, as non-personal data may be as harmful as personal data and the safeguards tools implemented in light of the GDPR have proved not to be sufficient.

In fact, is clear that the continuing technological development that allows non-personal data (processed personal data) to be turned into personal data represents a risk not properly addressed by the legislator. First, it must be said that the only institutional reference considering the risk and tackling it is limited to the Working Party Opinion 05 on anonymisation techniques

[64] In this sense, please refer to the following list of the European Court of Justice handling cases on the Right to be Forgotten: https://curia.europa.eu/juris/documents.jsf?nat=or&mat=or&pcs=Oor&jur=C%2CT%2CF&for=&jge=&dates=&language=en&pro=&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&oqp=&td=%3BALL&avg=&page=1&text=right%2Bto%2Bbe%2Bforgotten%2B&lg=&cid=1172581 or to the list provided in the database of the European Court of Human Rights: https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22right%20to%20be%20forgotten%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22]}

from 2014. Since then, technological development has evolved and the semantic difference between personal and non-personal data seems to be no longer sufficient to grant data protection. Consequently, rights granted by the GDPR, such as the right to be forgotten, risks becoming a dead letter.

Especially in the forthcoming implementation on data ecosystems allowing reuses of data, the remarkable availability of data in the infosphere may have an impact on the personal management of data subject representation in the infosphere. This may potentially lead to obscure decisions, discriminations, and inequality.

Therefore, it is deemed essential to continue investigating the technological development of the deanonymisation/re-identification risk as it provides a real perspective on data processing and further uses. As such, it allows a better understanding of the concrete feasibility of many principles set out in the General Data Protection Regulation, avoiding those practices violating data subjects' rights that risk falling beyond human control, from remaining unnoticed.

Lastly, it could certainly be beneficial to outlaw practices of turning non personal data into personal data, with fines and proper enforcement mechanisms able to *concretely* grant data subjects' protection.

Chapter 5. *Unlocking Data Re-uses through Proliferation of Roles and Responsibilities: a Subjective Perspective*

Index of the Chapter

Short Abstract of the Chapter

This chapter aims to provide a subjective perspective on the issue of deanonymisation. Specifically, it investigates whether a certain degree of anonymity can eventually be granted relying on the proliferation of roles and responsibilities among stakeholders, analysing data governance models and especially in Government to Business (G2B) data sharing. In such investigation, the focus is on the Regulation on European Data Governance COM/2020/7679 - the Data Governance Act - conceived as a natural evolution of the data policies in data flow.
In fact, since 2018, confident of having settled the main grounds for the protection of citizens' rights with the GDPR, the European Commission has begun brainstorming on new models of data. In 2020 the Data Strategy stresses a main subjective point, stating that "*Citizens will trust and embrace data-driven innovations only if they are confident that any personal data sharing in the EU will be subject to full compliance with the EU's strict data protection rules*".

5.1. Trusting the Middleman in the DGA: Data Stewardship and its Role in respect of the GDPR and the FFDR

After acknowledging the main strength of big data analysis systems in IoE (the possibility of cutting out the middleman in the dataflow and automating the process) scholars highlighted the issues linked to this strength as the vulnerability of such systems in terms of privacy and data protection [3] [136] [4][2].

Moreover, from a purely legal point of view, as investigated in the previous chapters, the objective perspective introduced by the GDPR on data anonymity and relying on anonymisation has been proven to emphasise such problems.

Therefore, a new interpretation has been proposed and new regulatory frameworks seem to offer new approaches to the above-mentioned risk, opening up to a new interpretation of the issue based on a subjective approach. In this sense, data intermediation and data stewardship represent a solution for integrating new leading figures in the analysis process, provided that some conditions and requirements are met.

Data stewardship is considered as the existence of mechanisms for responsibly acquiring, storing, safeguarding, and using data [112]. This concept is closely linked to data governance and intends to convey a trust (or fiduciary) level of responsibility toward the data [137].

As uncontrolled data access may have a detrimental impact, data governance conceptualises and frames data stewardship responsibilities, allowing secondary data uses and repurposing to be unlocked. The concept of data stewardship has its roots in the practice and science of data collection, sharing and analysis, recalling a typical approach to data management aimed at protecting data that can identify individuals [112].

Therefore, the main aim of the DGA is to introduce a scheme of trust which finds a balance between the legitimate interest of collecting data and the safe and secure data handling for secondary data uses.

Data stewardship represents the main approach of the DGA where the role of intermediaries is neutral, aimed at coordinating the interest of data subjects – who generate data – and data users – who create services and goods based on data.

The European framework designed in the DGA represents a hybrid model, as it lies in between the one based on data ownership and the one based on data access[26, 27][27].

The first incentivises data access through payment for information, thus recognising data ownership rights, while the second treats the information as a public good. In doing so, the information is available for use by entities structured and operated in accordance with the principle of data stewardship, imposing important limits on the use of data and transparent policy standards.

The DGA can therefore be considered as a hybrid model in between the ones mentioned above because it aims to

- make public sector data available for re-use, when such a right is subject to rights of others, granting access to data
- share data among business, even allowing data use on altruistic ground.

Moreover, according to the forthcoming legislation on data spaces[65], data is expected to be naturally reused, relying on secured processing environments supervised by the public sector.

Therefore, one of the main needs posed by the DGA is to supervise the purpose of reuses, define responsibility and liability exposure of public sector bodies, and define a formal approach to stewardship activities that support compliance and verification reporting to grant transparency.

Some academics [138] [139] stress the fact that, when considering the DGA interacting with other regulatory instruments, and especially with the GDPR, creates some legal uncertainty. The two regimes present several areas of inconsistency, on the distinction between personal and non-personal data as a key element of the data sharing practice.

In fact, even before the Data Governance Act proposal, academics [140] highlighted the tension between the principles set out in the GDPR and the FFDR, especially concerning data sharing for secondary and further purposes. However, now the DGA has been adopted, it seems that the same criticalities [141] [142] [138] [143] [144] persist, even being exacerbated by the new regulation.

In fact, the DGA seems to be built on the main semantic concepts of the GDPR and the FFDR (as investigated in Chapter 3) and, to some extent propagating the legal uncertainty and interpretation issues. Even the issue of a mixed dataset based on the semantic meaning of

[65] In this sense, please see the Staff Working Document of the European Commission, introducing the framework on Data Spaces: https://digital-strategy.ec.europa.eu/en/library/staff-working-document-data-spaces in which it is clarified that *The creation of EU-wide common, interoperable data spaces in strategic sectors aims at overcoming legal and technical barriers to data sharing by combining the necessary tools and infrastructures and addressing issues of trust by way of common rules. A common European data space brings together relevant data infrastructures and governance frameworks in order to facilitate data pooling and sharing.*

personal and non-personal data remains open, exacerbating the problem of having two mutually exclusive definitions of personal and non-personal data [145]. In addition, recalling the *compilation of data*, the DGA seems to leave room for *strategic behaviour of firms exploiting this regulatory rivalry* regarding the uncertainty on mixed datasets [145]. Therefore, we may consider the possibility that the European legislator deliberately avoided the issue, aiming to open the market and allowing dataflow in the Digital Single Market, relying on data stewardships. In this sense, it can also be added that the problem raised by the inextricability of datasets composed by both personal and non-personal data, being not technically feasible to be solved, could be overcome with the introduction of an additional actor in the dataflow.

Some authors [138] consider the fact that due to the inconsistencies in the regulatory framework, the ambitions and goals of the DGA will not be able to materialise.

On the same note, the joint Opinion of the EDPB-EDPS confirmed the risk of collision between the DGA, the GDPR, and the FFDR, mainly based on the concepts of personal data and non-personal data. This consideration led to consider the GDPR, upon which the DGA has been built, as *the elephant in the room of data economy* [146].

Some authors consider that instead of sorting it out, it builds upon it [138], therefore applying to any kind of data, personal and non-personal.

Apart from the objective perspective based on data semantics and investigated in the previous chapter, the DGA seems to rely on the introduction of new roles and responsibilities for the stakeholders involved in the dataflow, introducing trusted third parties that provide data sharing services, as represented in the following figure.

(1) Data Subjects

(2) Data Controller
& Data Processor

(3) Collection &
Primary Use(s) of Data

(4.a) Data Minimisation

(4.b.1.) Data Stewardship

(4.b) Secondary Uses of Data
Data Repository

(4.b.2) Data Sharing with third parties

Fig. 20. Introduction of trusted third parties in the data sharing flow

With data stewardship intended to convey a fiduciary (or trust) level of responsibility towards the data, the DGA introduces a new trusted thread in the data flow with the aim of ensuring re-uses in a common European data space, creating an Internal Market for Data[66].

In this sense, it creates two different cycles of reuse, based on the entrustment to competent bodies establishing them as data utilities or as data intermediaries acting in the general interest.[67]

These two cycles are respectively organised:

- relying on public sector bodies designated as competent under national law to grant or refuse access for re-use
- relying on neutral intermediaries as data intermediation service providers (which can be public or private).

Actually, both are required to further bridge the gap between the initial use of data and its re-uses as they licence the data for further and subsequent uses and covering an instrumental role in granting data re-uses for further purposes. They are entitled to establish the infrastructure for connecting data holders and data users, as well as creating data repositories enabling the exchange and exploitation of data[68].

Specifically, in relation to the first cycle which relies on public sector bodies, their role is instrumental to the opening to public sector data that does not fall under the scope of application of the Directive on Open Data and the Re-use of Public Sector Information[69]. These last ones are indeed pertaining to data held by public sector bodies, data that is not subject to rights of others.

[66] In this sense, Recital 3 of the Regulation species that it is necessary to improve the conditions for data sharing in the internal market, creating a harmonised framework for data exchange.

[67] This point is further investigated in the Explanatory Memorandum of the DGA at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52020PC0767

[68] Article 9 of the DGA further specifies that

[69] Directive (EU) 2019/1024 of the European Parliament and Council of 20 June 2019 on open data and the re-use of public sector information (recast) at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L1024

The DGA, conversely and as anticipated, opens the flow to data held by the public administration but subject to rights of others, like personal data.

In this case, the DGA requests that with the data flow opening, public sector bodies control the and monitor further data processing incentivising data access through the payment of information. Therefore, such a scheme seems to represent the recognition of data ownership rights by the public sector, conversely to the cycle which relies on data intermediation service providers, on neutral intermediators which can be private or public. In that context, the DGA confirms that the information is treated as public good, available for secondary uses in accordance with the principle of data stewardship and relying on transparent policy standards. According to these premises, we can agree with some academics who considered that the DGA opted for a hybrid data governance approach recalling the principles of data ownership, as well as the principle of data access [26][27].

5.2. Secure Processing Environments for Overcoming the Spectrum of Deanonymisation

Both cycles allow the data re-uses under different circumstances. Apart from the respective peculiarities, they seem to cope differently with the spectrum of deanonymisation, ensuring different safeguards for protecting personal data.

According to the Regulation, public sector bodies holding data that are subject to rights of others are the only ones providing secure processing environments. More specifically, Art. 5 clarifies that public sector bodies will ensure the protected nature of data is preserved, providing the following requirements:

a) to grant access for the re-use of data only where the public sector body or the competent body, following the request for re-use, has ensured that data has been:

> *i) anonymised, in the case of personal data; and*
>
> *(ii) modified, aggregated, or treated by any other method of disclosure control, in the case of commercially confidential information, including trade secrets or content protected by intellectual property rights;*

(b) to access and re-use the data remotely within a secure processing environment that is provided or controlled by the public sector body;

(c) to access and re-use the data within the physical premises in which the secure processing environment is located in accordance with high security standards, provided that remote access cannot be allowed without jeopardising the rights and interests of third parties.

Therefore, with regard to personal data, public sector bodies (or competent bodies) should ensure data access if data have been anonymised and, in the event of remote access or access to the physical premises, a secure processing environment should be provided.

In this regard, Art. 2 specifies that a secure processing environment is the *physical or virtual environment and organisational means to ensure compliance with Union law*, referring to the

GDPR.[70] A more detailed explanation of the point is provided in the Recitals. Specifically, Recital 7 clarifies that anonymisation, differential privacy, generalisation, suppression and randomisation, the use of synthetic data, or similar methods or other state-of-the-art privacy-preserving methods can contribute to a more privacy-friendly processing of data. It furthers specifies that these techniques, in combination with comprehensive data protection impact assessments and other safeguards, can grant safe reuses of data. However, it is explicitly mentioned that *in many cases the combination of such techniques, the impact assessment and other safeguards implies that data can be used only in a secure processing environment provided or controlled by public sector bodies*. In this case, as confirmed in the closing formula of the recital[71], the main recall is to the statistical context where the SDC has been proved as no longer being safe and secure for releasing statistical microdata, raising new approaches in Europe, contrarily to other extra -European countries [147]. Namely, regarding the European approach, national Statistical Agencies and Eurostat acknowledged that confidentiality and data protection in Official Statistics are evolving towards more dynamic solutions of SDC. To this aim, new approaches are developed, combined SDC with complementary solutions, especially the Secure Multi-party Computation techniques that are based on a cryptographic technique where multiple parties perform a joint computation without revealing the input provided by each party [148][149][150].

With the combination of such techniques and more advanced solutions of SDC, the public sector is making advances in providing services of data sharing and shaping new data ecosystems. As expressly recalled in the DGA, the main insight comes from the traditional scenario of data monopoly used in the National Statistical Offices (NSO)[151]. In fact, according to Regulation 557/2013 on European Statistics with regard to access to confidential data for scientific purposes[72] and expressly recalled in the DGA (Recital 7), apart from the data

[70] Art. 2(20) literally specifies that: *'secure processing environment' means the physical or virtual environment and organisational means to ensure compliance with Union law, such as Regulation (EU) 2016/679, in particular with regard to data subjects' rights, intellectual property rights, and commercial and statistical confidentiality, integrity and accessibility, as well as with applicable national law, and to allow the entity providing the secure processing environment to determine and supervise all data processing actions, including the display, storage, download and export of data and the calculation of derivative data through computational algorithms*; […].

[71] In this sense, Recital 7 states that "*There is experience at Union level with such secure processing environments that are used for research on statistical microdata on the basis of Commission Regulation (EU) No 557/2013(25). In general, insofar as personal data are concerned, the processing of personal data should be based upon one or more of the legal bases for processing provided in Articles 6 and 9 of Regulation (EU) 2016/679*".

[72] See Commission Regulation (EU) No 557/2013 of 17 June 2013 implementing Regulation (EC) No 223/2009 of the European Parliament and of the Council on European Statistics as regards access to confidential data for scientific purposes and repealing Commission Regulation (EC) No 831/2002 Text with EEA relevance at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013R0557

processing used for the output checking and aimed at data publication of National Statistical Data, National Statistical Offices provide a secure processing environment (in-premises) used for research on statistical microdata. The scenario is the following:

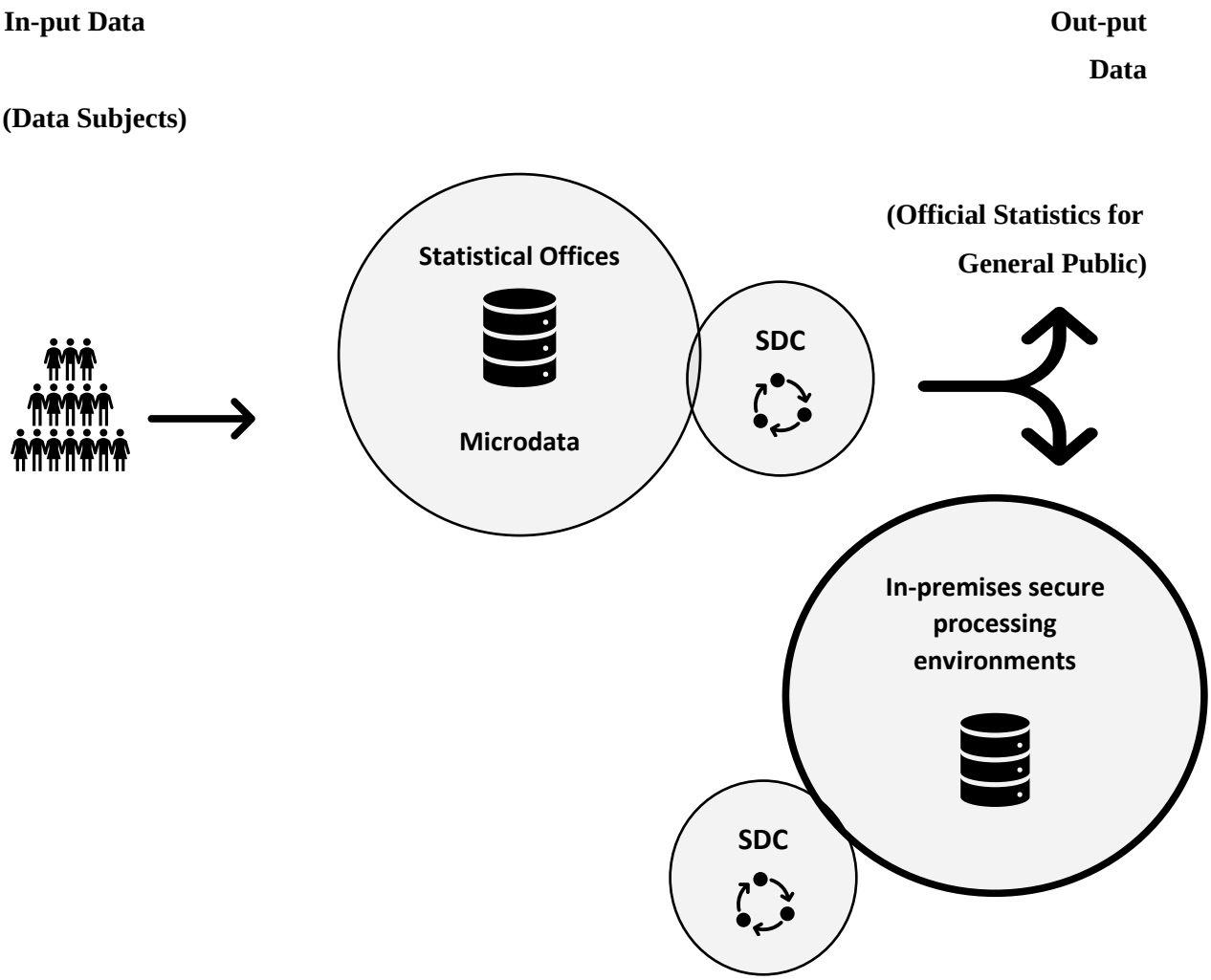


Fig. 21. Traditional Data Monopoly of National Statistical Agencies used for research on statistical microdata based on Commission Regulation (EU) n. 557/2013

Therefore, in light of the Regulation on National Statistics as regards access to confidential data for scientific purposes applied to Statistical Offices, the DGA recalls the same models for public entities holding data that are subject to rights of others, unleashing the potential of data held by public entities and allowing reuses.

In line with these premises, the scenario introduced by the DGA for data that is subject to rights of others and held by public entities relies on the creation of a data ecosystem provided and/or controlled by public entities, as shown in the figure below.

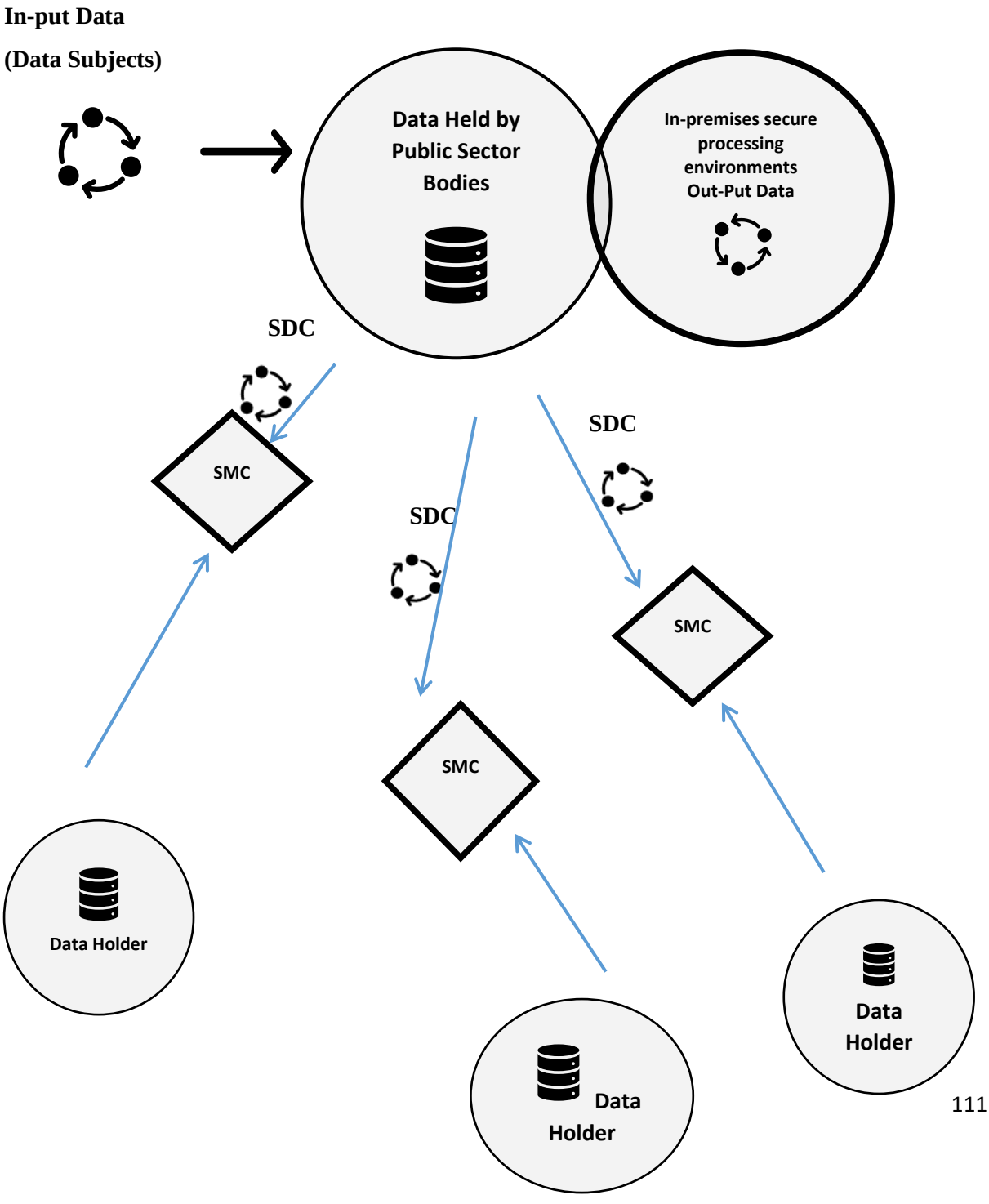


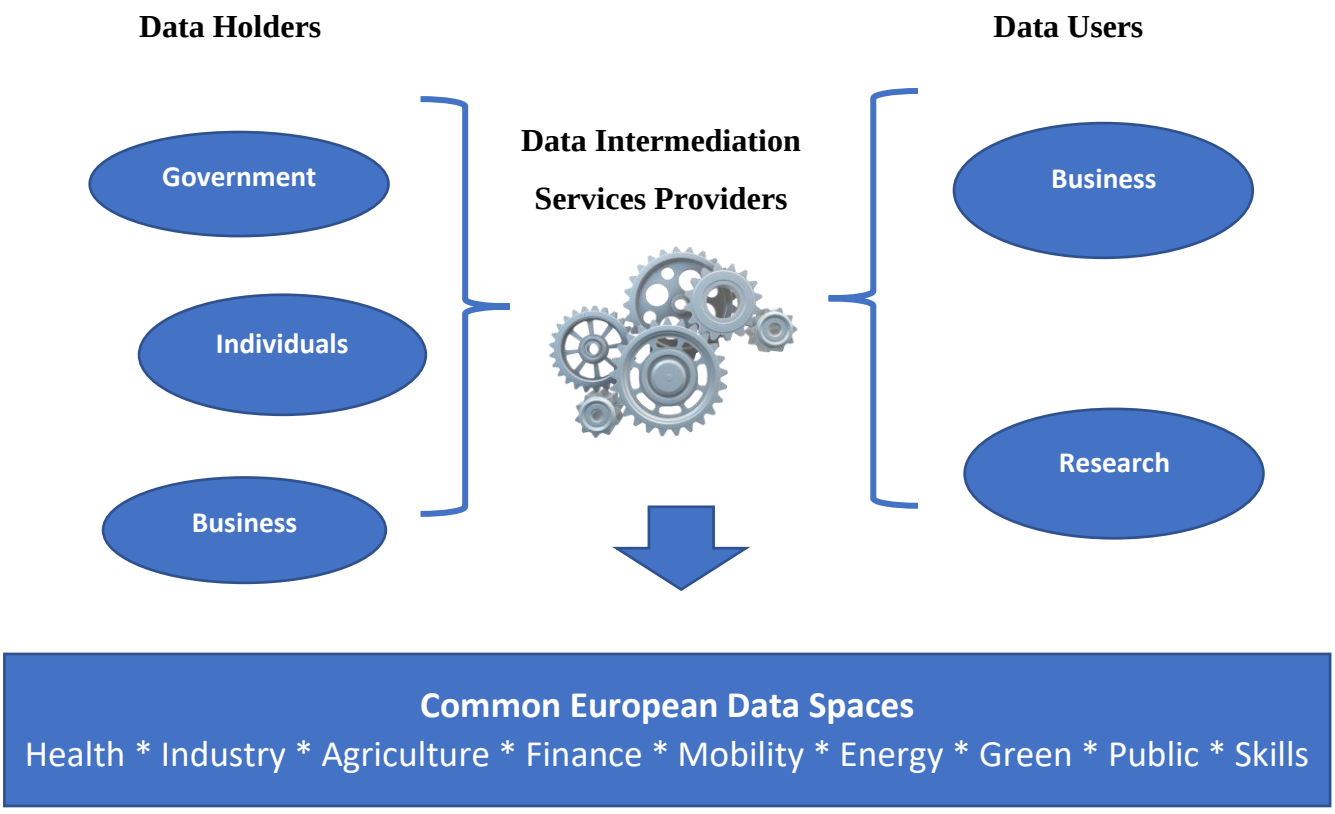
Fig. 22. New scenario introduced by DGA inspired by the traditional scenario (Fig.22) and based on public sector data ecosystem specifically applied for data listed in Art. 3.1(a)(b)(c)(d)

This scenario is better designed in Art. 5, Art. 6 and Art. 7 of the DGA, highlighting that the secure processing environment should be provided or controlled by public sector bodies.
However, it can be noted that the DGA does not provide theoretical solutions for the cases in which the re-uses can be granted *only* in secure processing environment, confirming that data processing models such as anonymisation, SDC, and other techniques combined with impact assessment are not sufficient against the risk of deanonymisation. Recital 15 only recalls the procedure of the GDPR (Articles 35 and 36 – consult the supervisory authority) in the event the provision of anonymised or modified data did not respond to the needs of the re-user, giving way to the secure processing environment, or eventually to the use of pseudonymous data.
In this sense, it introduces the design of new secure processing environments, but it leaves open the determination of the specific conditions under which this solution should be used.
In any case, the approach followed for data held by public entities is different from the one designed by the DGA for data intermediation service providers (which can be private or public). In this case indeed, as represented in fig. 13, the role of intermediator is key as it relies on data stewardship through the proliferation of roles and responsibilities among stakeholders, with the awareness that they cannot afford the cost of secure processing environments.

5.3. The role of Data Intermediation Services Providers in the DGA

In light of the Data Strategy[73], the forthcoming Data Act[74], and the initiatives proposed by the European Commission for the establishment of Common European Data Spaces[75], the DGA outlines the role played by Data Intermediation Services Providers.

In fact, they are demanded to play a neutral role in the evolving scenario, where new data ecosystems will naturally arise.



[73] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_273
[74] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0068&qid=1667038718753
[75] https://digital-strategy.ec.europa.eu/en/library/staff-working-document-data-spaces

Fig. 23. Role of intermediation service providers in pooling data in Data Spaces (DGA)

According to the DGA, data intermediation services providers are expected to play a key role in the data economy, especially in supporting and promoting voluntary data sharing practices. Therefore, their main scope is to create data pooling for facilitating bilateral and multilateral data sharing[76]. In this sense, academics [152] emphasise the fact that this natural intermediation creates an ecosystem of trust, allowing the issues linked to disruptive technologies to be overcome.

Therefore, simultaneously applying to personal and non-personal data, data intermediation services providers are made accountable and responsible for data processing in the interest of third parties. They are independent from any player with a significant degree of market power. In fact, according to the regulation, they are not allowed to use data they transact in the interest of third parties (cross-usage data prohibition), for any other purpose (Recital 33), imposing a separation between the data intermediation service and other services [153] [154] [141].

In this regard it is essential to highlight that, contrary to the objective perspective, the subjective perspective on data processing models seems to allow the risk of deanonymisation to be addressed in a better manner. In fact, data intermediation services providers are the only ones responsible for processing data and take care of roles, duties, and responsibilities in granting an acceptable level of anonymity for ensuring data reuses, offering temporary storage, curation, conversion, anonymisation and pseudonymisation. Therefore, the level of data anonymity seems to no longer pertain to data holders in the event they wish to reuse their data and, to some extent creating legal uncertainty even if concentrated on the figures of data intermediation services providers [138].

This approach is also confirmed when they are, for example, required to take all reasonable measures to prevent access to the systems where non personal data (e.g. processed personal data) are stored.[77]

[76] In this sense, Recital 27 specifies that data intermediation services providers have a facilitating role in the emergence of new data-driven ecosystems, and that this will be particularly important in the context of establishment of European Data Spaces.

[77] In this sense, Recital 23 states that data *intermediation services providers adhere to all relevant technical standards, codes of conduct and certifications at Union level*, confirming a certain interest in aligning their roles and duties within the Union, avoiding fragmentations.

The activity performed by data intermediation services providers is therefore subject to oversight by competent authorities[78] for ensuring compliance and they are concretely facilitating the exchange of data, especially in the light of the implementation of Data Spaces, where they play a key role in pooling data. The DGA clearly tailors a specific role for data intermediation services providers aimed at establishing commercial relationships among third parties, but also at ensuring standards in the processing of data and generating interoperability, even if their liability must be addressed based on national liability regimes.

Moreover, in providing such intermediation services for data subjects, in line with what is anticipated in Recital 30 of the DGA, they should be considered as a specific category, as they seek to enhance the agency of data subjects, or rather individual control over their data. To this aim, the DGA imposes that the business model of such providers should ensure there are no misaligned incentives to make individual data more available than is necessary in their interest, thus allowing any kind of business model in line with such condition. A specific recall is to data cooperatives, whose aim should be to strengthen individual positions and make them aware of better choices about their data. In this sense, academics [155] consider that data cooperatives certainly act as the fiduciary of their account holders' data, thus ensuring fair data access. However, they face two main challenges. The first pertains to participatory democratic governance as the *delegative democracy,* or *proxy democracy* [156] which require both elements of direct and representative democracy. The second challenge is linked to their funding, as they are self-representative entities thus, especially at the beginning of their activity, there is a consistent need of financial support.

In this regard, it seems that data altruism organisations, as introduced in the DGA, should aim to overcome such a challenge, as they might provide a governance and trust framework for data sharing and data donation in the primary interest of data subjects. However, some uncertainties remain.

[78] Recital 44.

5.4. Data Altruism Organisations for Allowing Re-uses on Altruistic Grounds

In the framework provided by the DGA, data altruism organisations seem to serve a different purpose from data intermediation services providers and, therefore, represent a different category.

In fact, they are not required to offer data intermediation services, nor to establish a commercial relationship between potential data users, data subjects and data holders.

Art. 2(16) of the DGA clarifies the concept of data altruism as the voluntary sharing of data based on data subjects' consent to process their personal data, or the permission of data holders to allow the use of their non-personal data (e.g., processed personal data), without seeking or receiving a reward going beyond compensation aimed at covering the cost they incur where they make data available for objective of general interest.

With this introduction, the EU legislator grants a strong potential to the use of data voluntarily made available and, even in this case – as in the case of intermediation services providers, there is a clear aim to contribute to pooling data in the Data Spaces, eventually allowing and enabling data analytics and machine learning, as expressively mentioned in Recital 35.

In this regard, the creation of data altruism organisations may be decisive in allowing a fairer use of data, especially in light of avoiding many practices based on the reward of data subjects for their data donation, which have been criticised [157].

A central role is played by Member States that are encouraged to facilitate data altruism through national policies and the implementation of a system of public registers.

The key element of such organisations is indeed their non-profit status, thus leading to the consideration that they are supposed to receive public funds for the pursuit of their purpose and, in such cases eventually generating conflict of interests among Member States, even if they may function as independent bodies.

Moreover, it seems that the data altruism organisation roles and duties may overlap with the data intermediation services providers offering their services to data subjects, especially because implementation of the Regulation may vary among Member States.
However, to a certain extent, as the DGA has only just entered into force and many amendments have been made to its first proposal, academic literature is lacking, and Member States are currently proceeding with implementation.
However, a single element keeps attracting major interest in academic literature: the general interest justifying the activity of data altruism organisations.

5.4.1. General interest in the DGA & public interest in the GDPR: a dialectic tension

Art. 15 of the DGA stresses the fact that the requirements applicable to data intermediation services shall not apply to *recognised data altruism organisations or other non-profit entities insofar as their activities consist of seeking to collect data for objectives of general interest, made available by natural or legal persons on the basis of data altruism, unless those organisations and entities aim to establish commercial relationships between an undetermined number of data subjects and data holders on the one hand and data users on the other*.
With this premise, the DGA sets out an exceptional framework for the above-mentioned activities, encouraging individuals and companies to make data voluntarily available for the common good, e.g., for a particular research project.
The main reference for this kind of entities is the pursuit of general interest activities. This concept seems to create a dialect tension with the public interest as recalled in the GDPR.
In this last case, academic literature shows there are different approaches to the notion of public interest, especially when investigated with reference to biobanking and scientific research [158]. Moreover, it emerged that in the GDPR, the concept is recalled roughly 70 times, but a specific and concrete definition is not provided. In this regard, the main reference to public interest may be the one relating to the lawful processing of personal data - Article 6(2) and Article 6(3) – or, for secondary purposes carried out in the public interest, the prohibition of processing personal data can be lifted – Art. 89 of the GDPR.
Therefore, the GDPR opted for an open formula for defining the public interest, even allowing Member States to define it on their own, determining their own policies, as anticipated in

Chapter 2. This approach has been heavily criticised in the Impact Assessment of the Regulation which used to recall the concept of "*high public interest*"[79], maintaining that with such a formula, the Commission could have had the opportunity to centralise control over Member States regarding exceptions in processing and, more generally, on the exception to the GDPR. However, despite such an expression was not retained in the final draft of the approved GDPR, some critics persist [159], the situation on secondary purposes of processing the situation may be problematic, as already investigated.

Specifically, the GDPR recalls cases of necessary processing for reason of public interest in art. Art. 9(2)(i) […] *in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy*;

9(2)(j) […] *for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject*.

Rather than presenting a definition, the DGA provides examples and contextualisation. For example, Recital 16 recalls *objectives of general interest as provided for in national law, where applicable, such as healthcare, combating climate change, improving mobility, facilitating the development, production and dissemination of official statistics, improving the provision of public services, public policy making or scientific research purposes in the general interest*.

Even in this case, it is not clear what the legislator intended by general interest. However, differently from the GDPR, the DGA imposes that entities seeking to collect data for objective of general interest based on data altruism should be registered in an *ad hoc* register kept by *competent public authorities*.

In this sense, DGA seems overcoming the legal uncertainty linked to the concept of public interest in the GDPR, recalling similar example but centralising the control on the hand of the public sector. The implementation of the DGA would reveal the evolution of the imprinting

[79] In this sense, please refer to the impact assessment of the GDPR, also extensively recalled in Chapter 3.

given by the DGA being certain, so far, that the evolution of the legislation seems propending towards a centralised approach over data processing.

In conclusion, three main points represent the pillars of the DGA:

- The introduction of rules aimed to ensure the widest availability of data held by public sector bodies thus granting re-uses
- A notification system and defined requirements for data intermediation services
- A registration system for data altruism.

Irrespectively on how the DGA will be implemented in the Member States, it is unquestionable that all of them are strictly anchored to public sector supervision, exposing data to public centralisation.

Chapter 6. *Conclusion*

This research investigated the foundations on which the whole European system is built, namely the GDPR and the FFDR, which introduced the main semantic difference between personal data and non-personal data. Specifically focusing on *further processing* in Big Data analysis systems in IoE environments, its aim was to question the semantic nature of data in the further uses of data and the consequent protection recognised for data subjects' rights. The investigation was carried out referring to two points of view that are considered to challenge the process of conciliate law with reality: the risk of deanonymisation/re-identification (allowing the turning of non-personal data - processed personal data - into personal data) and the right to erasure (*right to be forgotten*).

Scientific literature shows that the technological development of deanonymisation/re-identification techniques is growing remarkably, especially in some geographical areas which tend to invest more in such research.

Therefore, despite the fact that the GDPR is considered to be a gold standard in protecting data subjects, technological development certainly impacts on data subjects' rights, especially on the right to erasure *ex* art. 17 of the GDPR (*right to be forgotten*).

The two different perspectives, objective and subjective, investigated in the thesis confirm the above-mentioned impact. The objective one, questioning the extent of the protection granted by the two main data processing models recalled by the GDPR, namely, anonymisation and pseudonymisation, led to framing the limits of these models. Therefore, it demonstrates that anonymisation may represent a sufficient data protection model only in a few cases, but not necessarily for Big Data. Here, the diversity of the data consistently challenges the model and contextual evaluations are needed, in addition to a Data Protection Impact Assessment (DPIA),

aimed at better empowering data processors and data controllers in the processing of anonymised data.

Contrarily, pseudonymisation seems to satisfy the need to grant better data protection, ensuring a better level of data anonymity compared to anonymisation. Such an approach seems to be validated and endorsed in the evolution of the legislation, namely the DGA. In line with this point, the subjective perspective confirmed the potential of granting better protection by relying on the proliferation of stakeholders' roles and responsibilities, also with the introduction of new neutral intermediaries.

However, considering the fact that the DGA pins specific roles and duties on these new public entity figures, this type of approach is limited to generating a data ecosystem solely dependent on the public sector orientations, thus it may represent a challenge for democracy. This situation may be exacerbated by the lack of specification concerning general interest in the DGA and public interest in the GDPR, eventually leading to the concentration of data in the public sector challenging privacy and data protection of citizens. In this scenario, the right to erasure may evolve to a dead letter.

Moreover, the implementation of the DGA expected in the following months and implemented by Member States may generate the data subjection of some Member States in favour of others, in pooling data into the Data Spaces, thus justified by general interest and/or public interest.

In line with these considerations, it is considered that more work is required to control this possible drift. On one hand, improving the empirical research approach aimed at framing the new trends in the creation and evolution of data ecosystems. On the other hand, incentivising the establishment of legal entities aiming to represent data subject rights solely and uniquely, conjugate legal and technological knowledge in line with the technological development.

Annexes

Annex I. Deanonymisation

- Ali, Junade and Vladimir Dyo. “Cross Hashing: Anonymizing encounters in Decentralised Contact Tracing Protocols.” 2021 International Conference on Information Networking (ICOIN) (2021): 181-185.
- Arun, Venkat, Aniket Kate, Deepak Garg, Peter Druschel and Bobby Bhattacharjee. “Finding Safety in Numbers with Secure Allegation Escrows.” Proceedings 2020 Network and Distributed System Security Symposium (2020): n. pag.
- Azouvi, Sarah, Haaroon Yousaf and Alexander Hicks. “Incentivising Privacy in Cryptocurrencies.” ArXiv abs/1901.02695 (2019): n. pag.
- Bakirtas, Serhat and Elza Erkip. “Database Matching Under Column Deletions.” 2021 IEEE International Symposium on Information Theory (ISIT) (2021): 2720-2725.
- Bakirtas, Serhat and Elza Erkip. “Seeded Database Matching Under Noisy Column Repetitions.” ArXiv abs/2202.01724 (2022): n. pag.
- Bampoulidis, Alexandros and Mihai Lupu. “An Abstract View on the De-anonymization Process.” ArXiv abs/1902.09897 (2019): n. pag.
- Banerjee, Sudipta and A. A. Ross. “Smartphone Camera De-identification while Preserving Biometric Utility.” 2019 IEEE 10th International Conference on Biometrics Theory, Applications and Systems (BTAS) (2019): 1-10.
- Bartolucci, Silvia, Pauline Bernat and Daniel Joseph. “SHARVOT: Secret SHARe-Based VOTing on the Blockchain.” 2018 IEEE/ACM 1st International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB) (2018): 30-34.
- Baumgärtner, Lars, Alexandra Dmitrienko, Bernd Freisleben, Alexander Gruler, Jonas Höchst, Joshua Kühlberg, Mira Mezini, Markus Miettinen, Anel Muhamedagic, Thien Duc Nguyen, Alvar Penning, Dermot Frederik Pustelnik, Filipp Roos, Ahmad-Reza Sadeghi, Michael Schwarz and Christian Uhl. “Mind the GAP: Security & Privacy Risks of Contact Tracing Apps.” 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) (2020): 458-467.
- Beigi, Ghazaleh and Huan Liu. “Privacy in Social Media: Identification, Mitigation and Applications.” ArXiv abs/1808.02191 (2018): n. pag.
- Beigi, Ghazaleh, Kai Shu, Yanchao Zhang and Huan Liu. “Securing Social Media User Data: An Adversarial Approach.” Proceedings of the 29th on Hypertext and Social Media (2018): n. pag.

- Beigi, Ghazaleh. “Social Media and User Privacy.” ArXiv abs/1806.09786 (2018): n. pag.
- Bharadhwaj, Homanga, Dylan Turpin, Animesh Garg and Ashton Anderson. “De-anonymization of authors through arXiv submissions during double-blind review.” ArXiv abs/2007.00177 (2020): n. pag.
- Bradley, Stuart. “Realistic DNA De-anonymization using Phenotypic Prediction.” ArXiv abs/1607.07501 (2016): n. pag.
- Caliskan, Aylin, Fabian Yamaguchi, Edwin Dauber, Richard E. Harang, Konrad Rieck, Rachel Greenstadt and Arvind Narayanan. “When Coding Style Survives Compilation: De-anonymizing Programmers from Executable Binaries.” ArXiv abs/1512.08546 (2018): n. pag.
- Caravita, Ruggero. “PeopleTraffic: a common framework for harmonizing privacy and epidemic risks.” ArXiv abs/2005.10061 (2020): n. pag.
- Chan, Justin, Dean P. Foster, Shyamnath Gollakota, Eric Horvitz, Joseph Jaeger, Sham M. Kakade, Tadayoshi Kohno, John Langford, Jonathan Larson, Sudheesh Singanamalla, Jacob E. Sunshine and Stefano Tessaro. “PACT: Privacy-Sensitive Protocols And Mechanisms for Mobile Contact Tracing.” ArXiv abs/2004.03544 (2020): n. pag.
- Chen, Quanru, Jinguang Han, Jiguo Li, Liquan Chen and Song Li. “A Privacy-Preserving Logistics Information System with Traceability.” CSS (2021).
- Dorri, Ali, Clemence Roulin, Shantanu Pal, Sarah Baalbaki, Raja Jurdak and Salil S. Kanhere. “Device Identification in Blockchain-Based Internet of Things.” ArXiv abs/2202.09603 (2022): n. pag.
- Drakonakis, Kostas, Panagiotis Ilia, Sotiris Ioannidis and Jason Polakis. “Please Forget Where I Was Last Summer: The Privacy Risks of Public Location (Meta)Data.” ArXiv abs/1901.00897 (2019): n. pag.
- Eldosouky, Abdelrahman, Tapadhir Das, Anuraag Kotra and Shamik Sengupta. “Finding the Sweet Spot for Data Anonymization: A Mechanism Design Perspective.” ArXiv abs/2101.12442 (2021): n. pag.
- Espinoza-Cuadros, Fernando M., Juan M. Perero-Codosero, Javier Antón-Martín and Luis Alfonso Hernández Gómez. “Speaker De-identification System using Autoencodersand Adversarial Training.” ArXiv abs/2011.04696 (2020): n. pag.
- Froese, Vincent, Brijnesh J. Jain, Rolf Niedermeier and Malte Renken. “Comparing temporal graphs using dynamic time warping.” Social Network Analysis and Mining 10 (2020): 1-16.
- Fu, Luoyi, Jiapeng Zhang, Shuaiqi Wang, Xinyu Wu, Xinbing Wang and Guihai Chen. “De-Anonymizing Social Networks With Overlapping Community Structure.” IEEE/ACM Transactions on Networking 28 (2020): 360-375.
- Fu, Xinzhe, Zhongzhao Hu, Zhiying Xu, Luoyi Fu and Xinbing Wang. “De-anonymization of Social Networks with Communities: When Quantifications Meet Algorithms.” ArXiv abs/1703.09028 (2017): n. pag.
- Gadotti, Andrea, Florimond Houssiau, Luc Rocher, Benjamin Livshits and Yves-Alexandre de Montjoye. “When the Signal is in the Noise: Exploiting Diffix’s Sticky Noise.” USENIX Security Symposium (2019).
- Ghiasvand, Siavash and Florina M. Ciorba. “Anonymization of System Logs for Privacy and Storage Benefits.” ArXiv abs/1706.04337 (2017): n. pag.

- Gligoric, Kristina, Ryen W. White, Emre Kıcıman, Eric Horvitz, Arnaud Chiolero and Robert West. “Formation of Social Ties Influences Food Choice: A Campus-Wide Longitudinal Study.” ArXivabs/2102.08755 (2021): n. pag.
- Gong, Jiajun, Wuqi Zhang, Charles Zhang and Tao Wang. “WFDefProxy: Modularly Implementing and Empirically Evaluating Website Fingerprinting Defenses.” ArXiv abs/2111.12629 (2021): n. pag.
- Gulyás, Gábor György, Benedek Simon and Sándor Imre. “An Efficient and Robust Social Network De-anonymization Attack.” Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Society (2016): n. pag.
- Han, Jinguang, Liqun Chen, Steve A. Schneider, Helen Treharne and Stephan Wesemeyer. “Anonymous Single-Sign-On for n designated services with traceability.” ArXiv abs/1804.07201 (2018): n. pag.
- Hayhoe, Mikhail, Francisco Barreras, Hamed Hassani and Victor M. Preciado. “SPECTRE: Seedless Network Alignment via Spectral Centralities.” ArXiv abs/1811.01056 (2018): n. pag.
- Hendriksen, Mariya, Ernst Kuiper, Pim Nauts, Sebastian Schelter and M. de Rijke. “Analyzing and Predicting Purchase Intent in E-commerce: Anonymous vs. Identified Customers.” ArXiv abs/2012.08777 (2020): n. pag.
- Horawalavithana, Sameera and Adriana Iamnitchi. “On the Privacy of dK-Random Graphs.” ArXiv abs/1907.01695 (2019): n. pag.
- Jecmen, Steven, Hanrui Zhang, Ryan Liu, Nihar B. Shah, Vincent Conitzer and Fei Fang. “Mitigating Manipulation in Peer Review via Randomized Reviewer Assignments.” ArXiv abs/2006.16437 (2020): n. pag.
- Jeong, Yonghyun, Jooyoung Choi, Sungwon Kim, Youngmin Ro, Tae-Hyun Oh, Doyeon Kim, Heonseok Ha and Sungroh Yoon. “FICGAN: Facial Identity Controllable GAN for De-identification.” ArXiv abs/2110.00740 (2021): n. pag.
- Ji, Shouling, Haiqin Weng, Yiming Wu, Pan Zhou, Qinming He, Raheem A. Beyah and Ting Wang. “FDI: Quantifying Feature-based Data Inferability.” ArXiv abs/1902.00714 (2019): n. pag.
- Ji, Shouling, Qinchen Gu, Haiqin Weng, Qianjun Liu, Pan Zhou, Qinming He, Raheem A. Beyah and Ting Wang. “De-Health: All Your Online Health Information Are Belong to Us.” 2020 IEEE 36th International Conference on Data Engineering (ICDE) (2020): 1609-1620.
- Kappos, George and Ania M. Piotrowska. “Extending the Anonymity of Zcash.” ArXiv abs/1902.07337 (2019): n. pag.
- Karunanayake, Ishan, Nadeem Ahmed, Robert A. Malaney, Rafiqul M. D. Islam and Sanjay Kumar Jha. “De-Anonymisation Attacks on Tor: A Survey.” IEEE Communications Surveys & Tutorials 23 (2021): 2324-2350.
- Khazane, Anish, Julien Hoachuck, Krzysztof J. Gorgolewski and Russell A. Poldrack. “DeepDefacer: Automatic Removal of Facial Features via U-Net Image Segmentation.” ArXiv abs/2205.15536 (2022): n. pag.
- Komarova, Tatiana and Denis Nekipelov. “Identification and Formal Privacy Guarantees.” SSRN Electronic Journal (2020): n. pag.
- Lange, Lukas, Heike Adel and Jannik Strotgen. “Closing the Gap: Joint De-Identification and Concept Extraction in the Clinical Domain.” ACL (2020).
- Lange, Lukas, Heike Adel and Jannik Strotgen. “NLNDE: The Neither-Language-Nor-Domain-Experts’ Way of Spanish Medical Document De-Identification.” IberLEF@SEPLN (2019).

- Lee, Wei-Han, Changchang Liu, Shouling Ji, Prateek Mittal and Ruby B. Lee. “Blind De-anonymization Attacks using Social Networks.” Proceedings of the 2017 on Workshop on Privacy in the Electronic Society (2017): n. pag.
- Lee, Wei-Han, Changchang Liu, Shouling Ji, Prateek Mittal and Ruby B. Lee. “Quantification of De-anonymization Risks in Social Networks.” ICISSP (2017).
- Li, Hangtai, Yingbo Liu and Rui Tan. “Covert Association of Applications on Edge Devices by Processor Workload.” ArXiv abs/2001.01204 (2020): n. pag.
- Ma, Tianxiang, Dongze Li, Wei Wang and Jing Dong. “CFA-Net: Controllable Face Anonymization Network with Identity Representation Manipulation.” (2021).
- Maximov, Maxim, Ismail Elezi and Laura Leal-Taix’e. “CIAGAN: Conditional Identity Anonymization Generative Adversarial Networks.” 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2020): 5446-5455.
- Morales, Aythami, Alejandro Acien, Julian Fierrez, John V. Monaco, Rubén Tolosana, Rubén Vera-Rodríguez and Javier Ortega-Garcia. “Keystroke Biometrics in Response to Fake News Propagation in a Global Pandemic.” 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC) (2020): 1604-1609.
- Morin, Sophie, Jean-Marc Robert And Liane Gabora. “Creativity Training For Future Engineers: Preliminary Results From An Educative Experience.” Arxiv: Physics Education (2015): N. Pag.
- Mozes, Maximilian and Bennett Kleinberg. “No Intruder, no Validity: Evaluation Criteria for Privacy-Preserving Text Anonymization.” ArXiv abs/2103.09263 (2021): n. pag.
- Murray, Jeffrey, Afra Jahanbakhsh Mashhadi, Brent Lagesse and Michael Stiber. “Privacy Preserving Techniques Applied to CPNI Data: Analysis and Recommendations.” ArXivabs/2101.09834 (2021): n. pag.
- Nassar, Huda and David F. Gleich. “Multimodal Network Alignment.” SDM (2017).
- Nguyen, Benjamin and Claude Castelluccia. “Techniques d’anonymisation tabulaire : concepts et mise en oeuvre.” ArXiv abs/2001.02650 (2020): n. pag.
- Nithyanand, Rishab, Rachee Singh, Shinyoung Cho and Phillipa Gill. “Holding all the ASes: Identifying and Circumventing the Pitfalls of AS-aware Tor Client Design.” ArXiv abs/1605.03596 (2016): n. pag.
- Onaran, Efe, Siddharth Garg and Elza Erkip. “Optimal de-anonymization in random graphs with community structure.” 2016 50th Asilomar Conference on Signals, Systems and Computers (2016): 709-713.
- Ong, Jenn-Bing, Wee Keong Ng and C.-C. Jay Kuo. “Convolutional Neural Networks with Transformed Input based on Robust Tensor Network Decomposition.” ArXiv abs/1812.02622 (2018): n. pag.
- Pan, Yi-Lun, Min-Jhih Haung, Kuo-Teng Ding, Ja-Ling Wu and Jyh-Shing Roger Jang. “K-Same-Siamese-GAN: K-Same Algorithm with Generative Adversarial Network for Facial Image De-identification with Hyperparameter Tuning and Mixed Precision Training.” 2019 16th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS) (2019): 1-8.
- Pérez-González, Fernando, Carmela Troncoso and Simon Oya. “A Least Squares Approach to the Static Traffic Analysis of High-Latency Anonymous Communication Systems.” IEEE Transactions on Information Forensics and Security 9 (2014): 1341-1355.
- Pil’an, Ildik’o, Pierre Lison, Lilja Ovrelid, Anthia Papadopoulou, David Sánchez and Montserrat Batet. “The Text Anonymization Benchmark (TAB): A Dedicated Corpus

and Evaluation Framework for Text Anonymization." ArXiv abs/2202.00443 (2022): n. pag.
- Prado, Sandra D., Silvio R. Dahmen, Ana Lúcia Cetertich Bazzan, Pádraig Mac Carron and Ralph Kenna. "Temporal Network Analysis of Literary Texts." Adv. Complex Syst. 19 (2016): 1650005:1-1650005:19.
- Pyrgelis, Apostolos, Nicolas Kourtellis, Ilias Leontiadis, Joan Serrà and Claudio Soriente. "There goes Wally: Anonymously sharing your location gives you away." 2018 IEEE International Conference on Big Data (Big Data) (2018): 1218-1227.
- Qian, Jianwei, Xiangyang Li, Yu Wang, Shaojie Tang, Taeho Jung and Yang Fan. "Social Network De-anonymization: More Adversarial Knowledge, More Users Re-Identified?" arXiv: Social and Information Networks (2017): n. pag.
- Rahalkar, Chaitanya and Anushka Virgaonkar. "Summarizing and Analyzing the Privacy-Preserving Techniques in Bitcoin and other Cryptocurrencies." ArXiv abs/2109.07634 (2021): n. pag.
- Rahman, Mizanur, Nestor Hernandez, Bogdan Carbunar and Duen Horng Chau. "Search Rank Fraud De-Anonymization in Online Systems." Proceedings of the 29th on Hypertext and Social Media (2018): n. pag.
- Ravindra, V. and Ananth Y. Grama. "De-anonymization Attacks on Neuroimaging Datasets." Proceedings of the 2021 International Conference on Management of Data (2021): n. pag.
- Sánchez, David, Sergio Martínez and Josep Domingo-Ferrer. "How to Avoid Reidentification with Proper Anonymization." ArXiv abs/1808.01113 (2018): n. pag.
- Sánchez, David, Sergio Martínez and Josep Domingo-Ferrer. "Supplementary Materials for "How to Avoid Reidentification with Proper Anonymization"." ArXiv abs/1511.05957 (2015): n. pag.
- Shariatnasab, Mahshad, Farhad Shirani, Siddharth Garg and Elza Erkip. "On Graph Matching Using Generalized Seed Side-Information." 2021 IEEE International Symposium on Information Theory (ISIT) (2021): 2726-2731.
- Shen, Jie, Jiajun Zhou, Yunyi Xie, Shanqing Yu and Qi Xuan. "Identity Inference on Blockchain using Graph Neural Network." ArXiv abs/2104.06559 (2021): n. pag.
- Shen, Yun, Yufei Han, Zhikun Zhang, Min Chen, Tingyue Yu, Michael Backes, Yang Zhang and Gianluca Stringhini. "Finding MNEMON: Reviving Memories of Node Embeddings." ArXiv abs/2204.06963 (2022): n. pag.
- Shirani, Farhad, Siddharth Garg and Elza Erkip. "A Concentration of Measure Approach to Database De-anonymization." 2019 IEEE International Symposium on Information Theory (ISIT)(2019): 2748-2752.
- Shirani, Farhad, Siddharth Garg and Elza Erkip. "An information theoretic framework for active de-anonymization in social networks based on group memberships." 2017 55th Annual Allerton Conference on Communication, Control, and Computing (Allerton) (2017): 470-477.
- Shirani, Farhad, Siddharth Garg and Elza Erkip. "Optimal Active social Network De-anonymization Using Information Thresholds." 2018 IEEE International Symposium on Information Theory (ISIT) (2018): 1445-1449.
- Shirani, Farhad, Siddharth Garg and Elza Erkip. "Typicality Matching for Pairs of Correlated Graphs." 2018 IEEE International Symposium on Information Theory (ISIT) (2018): 221-225.

- Soltani, Ramin, Dennis L. Goeckel, Don Towsley and Amir Houmansadr. “Fundamental Limits of Invisible Flow Fingerprinting.” IEEE Transactions on Information Forensics and Security 15 (2020): 345-360.
- Stefanelli, Federica, Enrico Imbimbo, Franco Bagnoli and Andrea Guazzini. “Collective Intelligence Heuristic: An Experimental Evidence.” INSCI (2016).
- Sun, Zhen, R. Schuster and Vitaly Shmatikov. “De-Anonymizing Text by Fingerprinting Language Generation.” ArXiv abs/2006.09615 (2020): n. pag.
- Takbiri, Nazanin, Xiaozhe Shao, Lixin Gao and Hossein Pishro-Nik. “Improving Privacy in Graphs Through Node Addition.” 2019 57th Annual Allerton Conference on Communication, Control, and Computing (Allerton) (2019): 487-494.
- Tavi, Lauri, Tomi H. Kinnunen and Rosa González Hautamäki. “Improving speaker de-identification with functional data analysis of f0 trajectories.” ArXiv abs/2203.16738 (2022): n. pag.
- Valdez, André Calero and Martina Ziefle. “The Users’ Perspective on the Privacy-Utility Trade-offs in Health Recommender Systems.” Int. J. Hum. Comput. Stud. 121 (2019): 108-121.
- Vamosi, Stefan, Michaela D. Platzer and Thomas Reutterer. “AI-based Re-identification of Behavioral Clickstream Data.” ArXiv abs/2201.10351 (2022): n. pag.
- Veiga, Maria Han and Carsten Eickhoff. “A Cross-Platform Collection of Social Network Profiles.” Proceedings of the 39th International ACM SIGIR conference on Research and Development in Information Retrieval (2016): n. pag.
- Veiga, Maria Han and Carsten Eickhoff. “Privacy Leakage through Innocent Content Sharing in Online Social Networks.” ArXiv abs/1607.02714 (2016): n. pag.
- Warren, Michael S. and Samuel W. Skillman. “Mobility Changes in Response to COVID-19.” ArXivabs/2003.14228 (2020): n. pag.
- Wen, Yunqian, Li Song, Bo Liu, Ming Ding and Rong Xie. “IdentityDP: Differential Private Identification Protection for Face Images.” ArXiv abs/2103.01745 (2021): n. pag.
- Yamaç, Mehmet, Mete Ahishali, Nikolaos Passalis, Jenni Raitoharju, Bülent Sankur and M. Gabbouj. “Reversible Privacy Preservation using Multi-level Encryption and Compressive Sensing.” 2019 27th European Signal Processing Conference (EUSIPCO) (2019): 1-5.
- Yousaf, Haaroon, George Kappos and Sarah Meiklejohn. “Tracing Transactions Across Cryptocurrency Ledgers.” USENIX Security Symposium (2019).
- Zhang, Ning, Weina Wang and Lele Wang. “Attributed Graph Alignment.” 2021 IEEE International Symposium on Information Theory (ISIT) (2021): 1829-1834.
- Zhang, Yang, Mathias Humbert, Bartlomiej Surma, Praveen Manoharan, Jilles Vreeken and Michael Backes. “Towards Plausible Graph Anonymization.” Proceedings 2020 Network and Distributed System Security Symposium (2020): n. pag.
- Zhao, Yuchen and Isabel Wagner. “Using Metrics Suites to Improve the Measurement of Privacy in Graphs.” IEEE Transactions on Dependable and Secure Computing 19 (2022): 259-274.
- Zhou, Jiajun, Chenkai Hu, Jianlei Chi, Jiajing Wu, Meng Shen and Qi Xuan. “Behavior-aware Account De-anonymization on Ethereum Interaction Graph.” ArXiv abs/2203.09360 (2022): n. pag.
- Zhu, Haohan, Xianrui Meng and George Kollios. “NED: An Inter-Graph Node Metric Based On Edit Distance.” Proc. VLDB Endow. 10 (2017): 697-708.

Annex II. Re_Identification

- Abdelaziz, T.H.S., Aya Sedky, Bruno Rossi and Mostafa-Sami M. Mostafa. “Identification and Assessment of Software Design Pattern Violations.” ArXiv abs/1906.01419 (2019): n. pag.
- Abdul-Masih, Michael, Andrej Prša, Kyle E. Conroy, Steven Bloemen, Tabetha S. Boyajian, Laurance R. Doyle, Cole Johnston, Veselin B. Kostov, David W. Latham, Gal Matijevič, Avi Shporer and John Southworth. “Kepler Eclipsing Binary Stars. VIII. Identification of False Positive Eclipsing Binaries and Re-extraction of New Light Curves.” arXiv: Solar and Stellar Astrophysics (2016): n. pag.
- Adaimi, George, Sven Kreiss and Alexandre Alahi. “Deep visual Re-identification with confidence.” arXiv: Computer Vision and Pattern Recognition (2019): n. pag.
- Ahmed, Sk. Arif, Debi Prosad Dogra, Hee-seung Choi, Seungho Chae and Ig-Jae Kim. “Person Re-identification in Videos by Analyzing Spatio-temporal Tubes.” Multimedia Tools and Applications(2020): 1-15.
- Ahmed, Sk. Miraj, Aske R. Lejbølle, Rameswar Panda and Amit K. Roy-Chowdhury. “Camera On-Boarding for Person Re-Identification Using Hypothesis Transfer Learning.” 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2020): 12141-12150.
- Aich, Abhishek, Meng Zheng, Srikrishna Karanam, Terrence Chen, Amit K. Roy-Chowdhury and Ziyan Wu. “Spatio-Temporal Representation Factorization for Video-based Person Re-Identification.” 2021 IEEE/CVF International Conference on Computer Vision (ICCV) (2021): 152-162.
- Ainam, Jean-Paul, Ke Qin and Guisong Liu. “Self Attention Grid for Person Re-Identification.” ArXivabs/1809.08556 (2018): n. pag.

- Ainam, Jean-Paul, Ke Qin, Guisong Liu and Guangchun Luo. “Sparse Label Smoothing Regularization for Person Re-Identification.” IEEE Access 7 (2019): 27899-27910.
- Akiyama, Kazunori, Lukasz Stawarz, Yasuyuki T. Tanaka, Hiroshi Nagai, Marcello Giroletti and Mareki Honma. “EVN Observations of HESS J1943+213: Evidence for an Extreme TeV BL Lac Object.” arXiv: High Energy Astrophysical Phenomena (2016): n. pag.
- Alam, Mohammad Arif Ul. “Person Re-identification Attack on Wearable Sensing.” ArXivabs/2106.11900 (2021): n. pag.
- Albers, Casper J., Frank Critchley and John C. Gower. “Explicit minimisation of a convex quadratic under a general quadratic constraint.” (2015).
- Alemu, Leulseged Tesfaye, Mubarak Shah and Marcello Pelillo. “Deep Constrained Dominant Sets for Person Re-Identification.” 2019 IEEE/CVF International Conference on Computer Vision (ICCV)(2019): 9854-9863.
- Alex, Doney, Zishan Sami, Sumandeep Banerjee and Subrat Panda. “Cluster Loss for Person Re-Identification.” Proceedings of the 11th Indian Conference on Computer Vision, Graphics and Image Processing (2018): n. pag.
- Alfasly, Saghir, Yongjian Hu, Tiancai Liang, Xiaofeng Jin, Qingli Zhao and Beibei Liu. “Variational Representation Learning for Vehicle Re-Identification.” 2019 IEEE International Conference on Image Processing (ICIP) (2019): 3118-3122.
- Ali, T. M. Feroz and Subhasis Chaudhuri. “A Semi-Supervised Maximum Margin Metric Learning Approach for Small Scale Person Re-Identification.” 2019 IEEE/CVF International Conference on Computer Vision Workshop (ICCVW) (2019): 1848-1857.
- Ali, T. M. Feroz and Subhasis Chaudhuri. “Cross-view kernel similarity metric learning using pairwise constraints for person re-identification.” Proceedings of the Twelfth Indian Conference on Computer Vision, Graphics and Image Processing (2021): n. pag.
- Ali, T. M. Feroz and Subhasis Chaudhuri. “Maximum Margin Metric Learning Over Discriminative Nullspace for Person Re-identification.” ECCV (2018).
- Ali, T. M. Feroz, Kalpesh K Patel, Rajbabu Velmurugan and Subhasis Chaudhuri. “Multiple Kernel Fisher Discriminant Metric Learning for Person Re-identification.” Proceedings of the 11th Indian Conference on Computer Vision, Graphics and Image Processing (2018): n. pag.
- Ali, Usman, Bayram Bayramli and Hongtao Lu. “Temporal Continuity Based Unsupervised Learning for Person Re-identification.” ArXiv abs/2009.00242 (2019): n. pag.
- Alipour-Fanid, Amir, Monireh Dabaghchian, Ning Wang, Pu Wang, Liang Zhao and Kai Zeng. “Machine Learning-Based Delay-Aware UAV Detection and Operation Mode Identification Over Encrypted Wi-Fi Traffic.” IEEE Transactions on Information Forensics and Security 15 (2020): 2346-2360.
- Almazán, Jon, Bojana Gajic, Naila Murray and Diane Larlus. “Re-ID done right: towards good practices for person re-identification.” ArXiv abs/1801.05339 (2018): n. pag.
- Alqahtani, Hamed, Manolya Kavakli-Thorne and Charles Z. Liu. “An Introduction to Person Re-identification with Generative Adversarial Networks.” ArXiv abs/1904.05992 (2019): n. pag.

- Amati, Lorenzo, P. T. O'Brien, Diego Gotz, Enrico Bozzo and Andrea Santangelo. "The THESEUS space mission: updated design, profile and expected performances." Proceedings of SPIE 11444 (2021): n. pag.
- Amati, Lorenzo, P. T. O'Brien, Diego Götz, Enrico Bozzo, A. Santangelo, Nial R. Tanvir, Filippo Frontera, Sandro Mereghetti, Julian P. Osborne, A. W. Blain, S. Basa, Marica Branchesi, L. Burderi, M. D. Caballero-Garc'ia, Alberto J. Castro-Tirado, L Christensen, Riccardo Ciolfi, Alessandra De Rosa, Victor Doroshenko, Andrea Ferrara, Giancarlo Ghirlanda, L. Hanlon, P. Heddermann, Ian B. Hutchinson, Claudio Labanti, Emeric Le Floch, Hannah N. Lerman, Stéphane Paltani, Víctor Reglero, Luciano Rezzolla, Piero Rosati, Ruben Salvaterra, Giulia Stratta and Chris Tenzer. "The THESEUS space mission: science goals, requirements and mission concept." Experimental Astronomy (2021): n. pag.
- Amin, Mohammad and Marta Molinas. "Non-parametric Impedance based Stability and Controller Bandwidth Extraction from Impedance Measurements of HVDC-connected Wind Farms." ArXivabs/1704.04800 (2017): n. pag.
- Ananthabhotla, Ishwarya and Joseph A. Paradiso. "SoundSignaling: Realtime, Stylistic Modification of a Personal Music Corpus for Information Delivery." ArXiv abs/1811.06859 (2018): n. pag.
- Andreoni, Igor, Michael W. Coughlin, Mouza Almualla, Eric C. Bellm, Federica B. Bianco, Mattia Bulla, A. Cucchiara, Tim Dietrich, Ariel Goobar, Erik C. Kool, Xiaolong Li, Fabio Ragosta, Ana Sagues-Carracedo and Leo P. Singer. "Optimizing Cadences with Realistic Light-curve Filtering for Serendipitous Kilonova Discovery with Vera Rubin Observatory." The Astrophysical Journal Supplement Series 258 (2021): n. pag.
- Andrew, William, Jing Gao, Neill W. Campbell, Andrew W. Dowsey and Tilo Burghardt. "Visual Identification of Individual Holstein Friesian Cattle via Deep Metric Learning." Comput. Electron. Agric. 185 (2021): 106133.
- Ang, Eugene P.W., Lin Shan and Alex Chichung Kot. "DEX: Domain Embedding Expansion for Generalized Person Re-identification." ArXiv abs/2110.11391 (2021): n. pag.
- Ansdell, Megan, Eric Gaidos, Christina Hedges, Marco Tazzari, Adam L. Kraus, Mark C. Wyatt, Grant M. Kennedy, J. P. Williams, Andrew W. Mann, Isabel Angelo, Gaspard Duchêne, Eric E. Mamajek, John M. Carpenter, T. L. Esplin and Aaron C. Rizzuto. "Are inner disc misalignments common? ALMA reveals an isotropic outer disc inclination distribution for young dipper stars." Monthly Notices of the Royal Astronomical Society (2019): n. pag.
- Antonatos, Spyros, Stefano Braghin, Naoise Holohan and Pol Mac Aonghusa. "AnonTokens: tracing re-identification attacks through decoy records." ArXiv abs/1906.09829 (2019): n. pag.
- Antoniou, Anna, Giacomo Dossena, Julia MacMillan, Steven Hamblin, David Clifton and Paula M. Petrone. "Assessing the risk of re-identification arising from an attack on anonymised data." ArXivabs/2203.16921 (2022): n. pag.
- Ardeshir, Shervin, Sandesh Sharma and Ali Broji. "EgoReID: Cross-view Self-Identification and Human Re-identification in Egocentric and Surveillance Videos." ArXiv abs/1612.08153 (2016): n. pag.
- Arhin, Kofi, Ioana Baldini, Dennis Wei, Karthikeyan Natesan Ramamurthy and Moninder Singh. "Ground-Truth, Whose Truth? - Examining the Challenges with Annotating Toxic Text Datasets." ArXiv abs/2112.03529 (2021): n. pag.

- Assari, Shayan Modiri, Haroon Idrees and Mubarak Shah. “Re-identification of Humans in Crowds using Personal, Social and Environmental Constraints.” ArXiv abs/1612.02155 (2016): n. pag.
- Auchère, Frédéric, Clara Froment, K. Bocchialini, Éric Buchlin and Jacques Solomon. “ON THE FOURIER AND WAVELET ANALYSIS OF CORONAL TIME SERIES.” The Astrophysical Journal 825 (2016): 110.
- Ausdemore, Madeline, Jessie H. Hendricks and Cedric Neumann. “Review of several false positive error rate estimates for latent fingerprint examination proposed based on the 2014 Miami Dade Police Department study.” arXiv: Applications (2018): n. pag.
- Avola, Danilo, Marco Cascio, Luigi Cinque and Daniele Pannone. “Wi-Fi Passive Person Re-Identification based on Channel State Information.” ArXiv abs/1911.04900 (2019): n. pag.
- Azari, Samaneh, Bing Xue, Mengjie Zhang and Lifeng Peng. “Improving the Results of De novo Peptide Identification via Tandem Mass Spectrometry Using a Genetic Programming-based Scoring Function for Re-ranking Peptide-Spectrum Matches.” PRICAI (2019).
- Babaee, Maryam, Ali Athar and Gerhard Rigoll. “Multiple People Tracking Using Hierarchical Deep Tracklet Re-identification.” ArXiv abs/1811.04091 (2018): n. pag.
- Baharani, Mohammadreza, Shrey Mohan and Hamed Tabkhi. “Real-Time Person Re-identification at the Edge: A Mixed Precision Approach.” ICIAR (2019).
- Bahrami, Abbas, Alireza Karimian and Hossein Arabi. “Comparison of different deep learning architectures for synthetic CT generation from MR images.” Physica medica : PM : an international journal devoted to the applications of physics to medicine and biology : official journal of the Italian Association of Biomedical Physics 90 (2021): 99-107 .
- Bai, Shuai, Zhedong Zheng, Xiaohan Wang, Junyang Lin, Zhu Zhang, Chang Zhou, Yi Yang and Hongxia Yang. “Connecting Language and Vision for Natural Language-Based Vehicle Retrieval.” 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)(2021): 4029-4038.
- Bai, Song, Xiang Bai and Qi Tian. “Scalable Person Re-identification on Supervised Smoothed Manifold.” 2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (2017): 3356-3365.
- Bai, Song, Yingwei Li, Yuyin Zhou, Qizhu Li and Philip H. S. Torr. “Adversarial Metric Attack and Defense for Person Re-Identification.” IEEE Transactions on Pattern Analysis and Machine Intelligence 43 (2021): 2119-2126.
- Bai, Xiang, Mingkun Yang, Tengteng Huang, Zhiyong Dou, Rui Yu and Yongchao Xu. “Deep-Person: Learning Discriminative Deep Features for Person Re-Identification.” ArXiv abs/1711.10658 (2020): n. pag.
- Bai, Zechen, Zhigang Wang, Jian Wang, Diangang Hu and Errui Ding. “Unsupervised Multi-Source Domain Adaptation for Person Re-Identification.” 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2021): 12909-12918.
- Baig, Wajih Ullah, Adeel Ejaz, Umar Munir and Kashif Sardar. “Partial Fingerprint Detection Using Core Point Location.” ArXiv abs/1902.01400 (2019): n. pag.

- Baisa, Nathanael L.. “Occlusion-robust Online Multi-object Visual Tracking using a GM-PHD Filter with a CNN-based Re-identification.” J. Vis. Commun. Image Represent. 80 (2021): 103279.
- Baisa, Nathanael L.. “Robust Online Multi-target Visual Tracking using a HISP Filter with Discriminative Deep Appearance Learning.” J. Vis. Commun. Image Represent. 77 (2021): 102952.
- Bąk, Sławomir, Peter Carr and Jean-François Lalonde. “Domain Adaptation through Synthesis for Unsupervised Person Re-identification.” ECCV (2018).
- Bakirtas, Serhat and Elza Erkip. “Seeded Database Matching Under Noisy Column Repetitions.” ArXiv abs/2202.01724 (2022): n. pag.
- Bakliwal, Kshitij and S. Chandu Ravela. “The Sloop System for Individual Animal Identification with Deep Learning.” ArXiv abs/2003.00559 (2020): n. pag.
- Balestro, Vitor, Horst Martini and Ralph Teixeira. “Convex analysis in normed spaces and metric projections onto convex bodies.” arXiv: Metric Geometry (2019): n. pag.
- Bansal, Vaibhav, Stuart James and Alessio Del Bue. “re-OBJ: Jointly Learning the Foreground and Background for Object Instance Re-identification.” ArXiv abs/1909.07704 (2019): n. pag.
- Barbosa, Igor Barros, Marco Cristani, Barbara Caputo, Aleksander Rognhaugen and Theoharis Theoharis. “Looking beyond appearances: Synthetic training data for deep CNNs in re-identification.” ArXiv abs/1701.03153 (2018): n. pag.
- Barbui, M., K. Hagel, Jérome Gauthier, Sara Wuenschel, R. Wada, V. Z. Goldberg, R. T. deSouza, S. Hudan, Deqing Fang, X.G. Cao and J.B.Natowitz. “Searching for states analogous to the C12 Hoyle state in heavier nuclei using the thick target inverse kinematics technique.” Physical Review C (2018): n. pag.
- Basaran, Emrah, Muhittin Gokmen and Mustafa Ersel Kamasak. “An Efficient Framework for Visible-Infrared Cross Modality Person Re-Identification.” ArXiv abs/1907.06498 (2020): n. pag.
- Basaran, Emrah, Yonatan Tariku Tesfaye and Mubarak Shah. “EgoReID: Person re-identification in Egocentric Videos Acquired by Mobile Devices with First-Person Point-of-View.” ArXivabs/1812.09570 (2018): n. pag.
- Basu, Sumanta, Karl Kumbier, James B. Brown and Bin Yu. “Iterative Random Forests to detect predictive and stable high-order interactions.” arXiv: Machine Learning (2017): n. pag.
- Beck, Melanie, Claudia Scarlata, Lucy Fortson, Chris J. Lintott, Brooke D Simmons, Melanie A. Galloway, Kyle W. Willett, Hugh J. Dickinson, Karen L. Masters, Philip J. Marshall and Darryl Wright. “Integrating human and machine intelligence in galaxy morphology classification tasks.” Monthly Notices of the Royal Astronomical Society 476 (2018): 5516-5534.
- Bedogni, Luca, Shakila Khan Rumi and Flora D. Salim. “Modelling Memory for Individual Re-identification in Decentralised Mobile Contact Tracing Applications.” Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 5 (2021): 1 - 21.
- Beery, Sara, Arush Agarwal, Elijah Cole and Vighnesh Birodkar. “The iWildCam 2021 Competition Dataset.” ArXiv abs/2105.03494 (2021): n. pag.
- Beidler, M. T., Diego del-Castillo-Negrete, Larry R. Baylor, D. Shiraki and Donald A. Spong. “Spatially dependent modeling and simulation of runaway electron mitigation in DIII-D.” arXiv: Plasma Physics (2020): n. pag.

- Beigi, Ghazaleh, Kai Shu, Ruocheng Guo, Suhang Wang and Huan Liu. “I Am Not What I Write: Privacy Preserving Text Representation Learning.” ArXiv abs/1907.03189 (2019): n. pag.
- Benzine, Abdallah, Mohamed El Amine Seddik and Julien Desmarais. “Deep Miner: A Deep and Multi-branch Network which Mines Rich and Diverse Features for Person Re-identification.” ArXivabs/2102.09321 (2021): n. pag.
- Bergamini, Luca, Angelo Porrello, Andrea Capobianco Dondona, Ercole Del Negro, Mauro Mattioli, Nicola D’Alterio and Simone Calderara. “Multi-views Embedding for Cattle Re-identification.” 2018 14th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS)(2018): 184-191.
- Bergmann, Philipp, Tim Meinhardt and Laura Leal-Taixé. “Tracking Without Bells and Whistles.” 2019 IEEE/CVF International Conference on Computer Vision (ICCV) (2019): 941-951.
- Bernabéu, José, Francisco J. Botella and Miguel Nebot. “Genuine T, CP, CPT asymmetry parameters for the entangled Bd system.” Journal of High Energy Physics 2016 (2016): 1-24.
- Bertocco, Gabriel, Antonio The’ofilo, Fernanda Andal’o and Anderson Rocha. “Reasoning for Complex Data through Ensemble-based Self-Supervised Learning.” ArXiv abs/2202.03126 (2022): n. pag.
- Bertocco, Gabriel, Fernanda A. Andal’o and Anderson Rocha. “Unsupervised and Self-Adaptative Techniques for Cross-Domain Person Re-Identification.” IEEE Transactions on Information Forensics and Security 16 (2021): 4419-4434.
- Beyer, Lucas, Stefan Breuers, Vitaly Kurin and B. Leibe. “Towards a Principled Integration of Multi-camera Re-identification and Tracking Through Optimal Bayes Filters.” 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW) (2017): 1444-1453.
- Beyn, Wolf-Jürgen and Denny Otten. “Fredholm Properties and L^p-Spectra of Localized Rotating Waves in Parabolic Systems.” arXiv: Analysis of PDEs (2016): n. pag.
- Bharadwaj, Sandesh and Kunal Chanda. “Person Re-identification by analyzing Dynamic Variations in Gait Sequences.” ArXiv abs/2006.15109 (2020): n. pag.
- Bhargava, Prajjwal. “Incremental Learning in Person Re-Identification.” ArXiv abs/1808.06281 (2018): n. pag.
- Bikádi, Zsolt, Sapumal Ahangama and Eszter Hazai. “Prediction of Domain Values: High throughput screening of domain names using Support Vector Machines.” ArXiv abs/1707.00906 (2017): n. pag.
- Biswal, Siddharth, Soumya Shubhra Ghosh, Jon D. Duke, Bradley A. Malin, Walter F. Stewart and Jimeng Sun. “EVA: Generating Longitudinal Electronic Health Records Using Conditional Variational Autoencoders.” MLHC (2021).
- Bizzocchi, Luca, Mattia Melosso, Barbara Michela Giuliano, Luca Dore, Filippo Tamassia, Marie-Aline Martin-Drumel, Olivier Pirali, Laurent Margulès and Paola Caselli. “Submillimeter and Far-infrared Spectroscopy of Monodeuterated Amidogen Radical (NHD): Improved Rest Frequencies for Astrophysical Observations.” arXiv: Astrophysics of Galaxies (2020): n. pag.
- Blondel, Gilles, Marta Arias and Ricard Gavaldà. “Identifiability and transportability in dynamic causal networks.” International Journal of Data Science and Analytics 3 (2016): 131-147.

- Bohara, Bharat. “Adaptive Threshold for Online Object Recognition and Re-identification Tasks.” arXiv: Computer Vision and Pattern Recognition (2020): n. pag.
- Boin, Jean-Baptiste, Andre F. de Araújo and Bernd Girod. “Recurrent Neural Networks for Person Re-identification Revisited.” 2019 IEEE Conference on Multimedia Information Processing and Retrieval (MIPR) (2019): 147-152.
- Bonamente, Max, M. S. Mirakhor, Richard Lieu and Sean Walker. “A WHIM origin for the soft excess emission in the Coma cluster.” (2022).
- Borgia, Alessandro, Yang Hua, Elyor Kodirov and Neil Martin Robertson. “GAN-Based Pose-Aware Regulation for Video-Based Person Re-Identification.” 2019 IEEE Winter Conference on Applications of Computer Vision (WACV) (2019): 1175-1184.
- Breckon, T. and Aishah Alsehaim. “Not 3D Re-ID: Simple Single Stream 2D Convolution for Robust Video Re-identification.” 2020 25th International Conference on Pattern Recognition (ICPR)(2021): 5190-5197.
- Brinker, Sascha, Manuel dos Santos Dias and Samir Lounis. “Prospecting chiral multisite interactions in prototypical magnetic systems.” arXiv: Mesoscale and Nanoscale Physics (2020): n. pag.
- Bromley, S. J., B. Neff, S. D. Loch, J. P. Marler, J. Országh, Kumar Venkataramani and Dennis Bodewits. “Atomic Iron and Nickel in the Coma of C/1996 B2 (Hyakutake): Production Rates, Emission Mechanisms, and Possible Parents.” The Planetary Science Journal 2 (2021): n. pag.
- Bromley, S. J., B. Neff, S. D. Loch, J. P. Marler, J. Országh, Kumar Venkataramani and Dennis Bodewits. “Atomic Iron and Nickel in the Coma of C/1996 B2 (Hyakutake): Production Rates, Emission Mechanisms, and Possible Parents.” The Planetary Science Journal 2 (2021): n. pag.
- Brown, J Thomas, Chao Yan, Weiyi Xia, Zhijun Yin, Zhiyu Wan, Aris Gkoulalas-Divanis, Murat Kantarcioglu and Bradley A. Malin. “Dynamically Adjusting Case-Reporting Policy to Maximize Privacy and Utility in the Face of a Pandemic.” ArXiv abs/2106.14649 (2021): n. pag.
- Burgess, Cassandra, Cordelia Neisinger and Rafael Baruch Dinner. “Matching Targets Across Domains with RADON, the Re-Identification Across Domain Network.” ArXiv abs/2105.12056 (2021): n. pag.
- Burman, Erik, Cuiyu He and Mats G. Larson. “Comparison of Shape Derivatives using CutFEM for Ill-posed Bernoulli Free Boundary Problem.” J. Sci. Comput. 88 (2021): 35.
- Cai, Chengtao, Yueyuan Zhou and Yanming Wang. “CHD: Consecutive Horizontal Dropout for Human Gait Feature Extraction.” Proceedings of the 2019 8th International Conference on Computing and Pattern Recognition (2019): n. pag.
- Cai, Honglong, Yuedong Fang, Zhiguan Wang, Tingchun Yeh and Jinxing Cheng. “VMRFANet: View-Specific Multi-Receptive Field Attention Network for Person Re-identification.” ICAART(2020).
- Cai, Honglong, Zhiguan Wang and Jinxing Cheng. “Multi-Scale Body-Part Mask Guided Attention for Person Re-Identification.” 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW) (2019): 1555-1564.

- Cai, Jiarui, Yizhou Wang, Haotian Zhang, Hung-Min Hsu, Chengqian Ma and Jenq-Neng Hwang. “IA-MOT: Instance-Aware Multi-Object Tracking with Motion Consistency.” ArXiv abs/2006.13458 (2020): n. pag.
- Canil, Marco, Jacopo Pegoraro and Michele Rossi. “milliTRACE-IR: Contact Tracing and Temperature Screening via mmWave and Infrared Sensing.” IEEE Journal of Selected Topics in Signal Processing 16 (2022): 208-223.
- Cao, Jiale, Yanwei Pang, Rao Muhammad Anwer, Hisham Cholakkal, J. Xie, Mubarak Shah and Fahad Shahbaz Khan. “PSTR: End-to-End One-Step Person Search With Transformers.” ArXivabs/2204.03340 (2022): n. pag.
- Cao, Jinkun, Xinshuo Weng, Rawal Khirodkar, Jiangmiao Pang and Kris Kitani. “Observation-Centric SORT: Rethinking SORT for Robust Multi-Object Tracking.” ArXiv abs/2203.14360 (2022): n. pag.
- Cao, Ming-Ming, Chen Chen, Hao Dou, Xiyuan Hu, Silong Peng and Arjan Kuijper. “Progressive Bilateral-Context Driven Model for Post-Processing Person Re-Identification.” IEEE Transactions on Multimedia 23 (2021): 1239-1251.
- Cao, Pei and Jiong Tang. “A Reinforcement Learning Hyper-Heuristic in Multi-Objective Single Point Search with Application to Structural Fault Identification.” ArXiv abs/1812.07958 (2018): n. pag.
- Cao, Xuefei, Bor-Chun Chen and Ser-Nam Lim. “Unsupervised Deep Metric Learning via Auxiliary Rotation Loss.” ArXiv abs/1911.07072 (2019): n. pag.
- Cao, Zongjing and Hyo Jong Lee. “Improved Res2Net Model for Person re-Identification.” 2019 IEEE First International Conference on Cognitive Machine Intelligence (CogMI) (2019): 235-240.
- Cardona, Carlos A. and Yu-tin Huang. “S-matrix singularities and CFT correlation functions.” Journal of High Energy Physics 2017 (2017): 1-19.
- Carignano, Stefano, Luca Lepori, Andrea Mammarella, Massimo Mannarelli and G. Pagliaroli. “Scrutinizing the pion condensed phase.” The European Physical Journal A 53 (2016): 1-12.
- Carmona, René A. and Kevin Thomas Webster. “The microstructure of high frequency markets.” arXiv: Trading and Market Microstructure (2017): n. pag.
- Carvalho, Tânia, Nuno Moniz, Pedro Faria and Luís Antunes. “Towards a Data Privacy-Predictive Performance Trade-off.” (2022).
- Casao, Sara, Ana Cristina Murillo and Eduardo Montijano. “Distributed Multi-Target Tracking in Camera Networks.” 2021 IEEE International Conference on Robotics and Automation (ICRA)(2021): 1903-1909.
- Castro-Alvaredo, Olalla A., Benjamin Doyon and Davide Fioravanti. “Conical Twist Fields and Null Polygonal Wilson Loops.” Nuclear Physics 931 (2018): 146-178.
- Chai, Tianrui, Zhiyuan Chen, Annan Li, Jiaxin Chen, Xinyu Mei and Yunhong Wang. “Video Person Re-identification using Attribute-enhanced Features.” ArXiv abs/2108.06946 (2021): n. pag.
- Chang, Xiaobin, Timothy M. Hospedales and Tao Xiang. “Multi-level Factorisation Net for Person Re-identification.” 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition(2018): 2109-2118.
- Chang, Zhigang, Qin Zhou, Mingyang Yu, Shibao Zheng, Hua Yang and Tai-Pang Wu. “Distribution Context Aware Loss for Person Re-identification.” 2019 IEEE Visual Communications and Image Processing (VCIP) (2019): 1-4.

- Chang, Zhigang, Zhao Yang, Yongbiao Chen, Qin Zhou and Shibao Zheng. “Seq-Masks: Bridging the gap between appearance and gait modeling for video-based person re-identification.” 2021 International Conference on Visual Communications and Image Processing (VCIP) (2021): 1-5.
- Chasmai, Mustafa Ebrahim and Tamajit Banerjee. “Person Re-Identification.” ArXivabs/2204.13158 (2022): n. pag.
- Chatain, Audrey, J. E. Wahlund, Oleg Shebanits, Lina Z. Hadid, Michiko W. Morooka, Niklas J. T. Edberg, Olivier Guaitella and N. Carrasco. “Re-Analysis of the Cassini RPWS/LP Data in Titan’s Ionosphere: 2. Statistics on 57 Flybys.” Journal of Geophysical Research: Space Physics 126 (2021): n. pag.
- Chaudhury, Subhajit, Hiroki Ozaki, Daiki Kimura, Phongtharin Vinayavekhin, Asim Munawar, Ryuki Tachibana, Koji Ito, Yuki Inaba, Minoru Matsumoto and Shuji Kidokoro. “Unsupervised Temporal Feature Aggregation for Event Detection in Unstructured Sports Videos.” 2019 IEEE International Symposium on Multimedia (ISM) (2019): 9-97.
- Chelak, Ilja, Ekaterina A. Nepovinnykh, Tuomas Eerola, Heikki Kälviäinen and Igor Belykh. “EDEN: Deep Feature Distribution Pooling for Saimaa Ringed Seals Pattern Matching.” ArXivabs/2105.13979 (2021): n. pag.
- Chen, Binghui, Weihong Deng and Jiani Hu. “Mixed High-Order Attention Network for Person Re-Identification.” 2019 IEEE/CVF International Conference on Computer Vision (ICCV) (2019): 371-381.
- Chen, Chen, Ming-Ming Cao, Xiyuan Hu and Silong Peng. “Key Person Aided Re-identification in Partially Ordered Pedestrian Set.” ArXiv abs/1805.10017 (2017): n. pag.
- Chen, Dapeng, Hongsheng Li, Xihui Liu, Yantao Shen, Zejian Yuan and Xiaogang Wang. “Improving Deep Visual Representation for Person Re-identification by Global and Local Image-language Association.” ECCV (2018).
- Chen, Di, Andreas Doering, Shanshan Zhang, Jian Yang, Juergen Gall and Bernt Schiele. “Keypoint Message Passing for Video-based Person Re-Identification.” ArXiv abs/2111.08279 (2021): n. pag.
- Chen, Di, Shanshan Zhang, Wanli Ouyang, Jian Yang and Ying Tai. “Person Search via A Mask-Guided Two-Stream CNN Model.” ECCV (2018).
- Chen, Feng, Fei Wu, Qi Wu and Zhiguo Wan. “Memory Regulation and Alignment toward Generalizer RGB-Infrared Person.” ArXiv abs/2109.08843 (2021): n. pag.
- Chen, Guangyi, Tianpei Gu, Jiwen Lu, Jin-An Bao and Jie Zhou. “Person Re-Identification via Attention Pyramid.” IEEE Transactions on Image Processing 30 (2021): 7663-7676.
- Chen, Hao, Benoit Lagadec and François Bremond. “Enhancing Diversity in Teacher-Student Networks via Asymmetric branches for Unsupervised Person Re-identification.” 2021 IEEE Winter Conference on Applications of Computer Vision (WACV) (2021): 1-10.
- Chen, Hao, Benoit Lagadec and François Bremond. “ICE: Inter-instance Contrastive Encoding for Unsupervised Person Re-identification.” 2021 IEEE/CVF International Conference on Computer Vision (ICCV) (2021): 14940-14949.
- Chen, Hao, Benoit Lagadec and François Bremond. “Unsupervised Lifelong Person Re-identification via Contrastive Rehearsal.” ArXiv abs/2203.06468 (2022): n. pag.

- Chen, Hao, Yaohui Wang, Benoit Lagadec, Antitza Dantcheva and François Bremond. “Joint Generative and Contrastive Learning for Unsupervised Person Re-identification.” 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2021): 2004-2013.
- Chen, Junru, Shi Feng Geng, Yongluan Yan, Danyang Huang, Hao Liu and Yadong Li. “Vehicle Re-identification Method Based on Vehicle Attribute and Mutual Exclusion Between Cameras.” ArXivabs/2104.14882 (2021): n. pag.
- Chen, Kai, Weihua Chen, Tao He, Rong Du, Fan Wang, Xiuyu Sun, Yuchen Guo and Guiguang Ding. “TAGPerson: A Target-Aware Generation Pipeline for Person Re-identification.” ArXivabs/2112.14239 (2021): n. pag.
- Chen, Lequan, Wei Xie, Zhigang Tu, Yaping Tao and Xinming Wang. “Multi-Attribute Enhancement Network for Person Search.” 2021 International Joint Conference on Neural Networks (IJCNN)(2021): 1-8.
- Chen, Long, Haizhou Ai, Zijie Zhuang and Chong Shang. “Real-Time Multiple People Tracking with Deeply Learned Candidate Selection and Person Re-Identification.” 2018 IEEE International Conference on Multimedia and Expo (ICME) (2018): 1-6.
- Chen, Minghui, Zhiqiang Wang and Feng Zheng. “Benchmarks for Corruption Invariant Person Re-identification.” ArXiv abs/2111.00880 (2021): n. pag.
- Chen, Peixian, Pingyang Dai, Jianzhuang Liu, Feng Zheng, Qi Tian and Rongrong Ji. “Dual Distribution Alignment Network for Generalizable Person Re-Identification.” AAAI (2021).
- Chen, Peixian, Pingyang Dai, Qiong Wu and Yuyu Huang. “Video-based Person Re-identification with Two-stream Convolutional Network and Co-attentive Snippet Embedding.” ArXivabs/1905.11862 (2019): n. pag.
- Chen, Peng, Tong Jia, Pengfei Wu, Jianjun Wu and Dongyue Chen. “Learning Deep Representations by Mutual Information for Person Re-identification.” ArXiv abs/1908.05860 (2019): n. pag.
- Chen, Qiuyu, Wei Zhang and Jianping Fan. “Cluster-level Feature Alignment for Person Re-identification.” ArXiv abs/2008.06810 (2020): n. pag.
- Chen, Shih-Ying, Yueqing Zhuang and Boxun Li. “Learning Context-Aware Embedding for Person Search.” (2021).
- Chen, Shizhe, Chun-Chao Guo and Jianhuang Lai. “Deep Ranking for Person Re-Identification via Joint Representation Learning.” IEEE Transactions on Image Processing 25 (2016): 2353-2367.
- Chen, Sirui, Keenon Werling and C. Karen Liu. “Real-time Model Predictive Control and System Identification Using Differentiable Physics Simulation.” ArXiv abs/2202.09834 (2022): n. pag.
- Chen, Siyu, Dengjie Li, Lishuai Gao, Fan Liang, Wei Zhang and Ling-guo Ma. “Video Temporal Relationship Mining for Data-Efficient Person Re-identification.” ArXiv abs/2110.00549 (2021): n. pag.
- Chen, Tianlong, Shaojin Ding, Jingyi Xie, Ye Yuan, Wuyang Chen, Yang Yang, Zhou Ren and Zhangyang Wang. “ABD-Net: Attentive but Diverse Person Re-Identification.” 2019 IEEE/CVF International Conference on Computer Vision (ICCV) (2019): 8350-8360.
- Chen, Tsai-Shien, Chih-Ting Liu, Chih-Wei Wu and Shao-Yi Chien. “Orientation-aware Vehicle Re-identification with Semantics-guided Part Attention Network.” ECCV (2020).

- Chen, Tsai-Shien, Man-Yu Lee, Chih-Ting Liu and Shao-Yi Chien. “Viewpoint-aware Channel-wise Attentive Network for Vehicle Re-identification.” 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW) (2020): 2448-2455.
- Chen, Weihua, Xiaotang Chen, Jianguo Zhang and Kaiqi Huang. “A Multi-Task Deep Network for Person Re-Identification.” ArXiv abs/1607.05369 (2017): n. pag.
- Chen, Weihua, Xiaotang Chen, Jianguo Zhang and Kaiqi Huang. “Beyond Triplet Loss: A Deep Quadruplet Network for Person Re-identification.” 2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (2017): 1320-1329.
- Chen, Weizhe and Lantao Liu. “Informative Planning in the Presence of Outliers.” ArXivabs/2111.01822 (2021): n. pag.
- Chen, Xianing, Jialang Xu, Jiale Xu and Shenghua Gao. “OH-Former: Omni-Relational High-Order Transformer for Person Re-Identification.” ArXiv abs/2109.11159 (2021): n. pag.
- Chen, Xiaodong, Xinchen Liu, Wu Liu, Xiao-Ping Zhang, Yongdong Zhang and Tao Mei. “Explainable Person Re-Identification with Attribute-guided Metric Distillation.” 2021 IEEE/CVF International Conference on Computer Vision (ICCV) (2021): 11793-11802.
- Chen, Xihui, Ema Këpuska, Sjouke Mauw and Yunior Ramírez-Cruz. “Active Re-identification Attacks on Periodically Released Dynamic Social Graphs.” ArXiv abs/1911.09534 (2020): n. pag.
- Chen, Yanbei, Xiatian Zhu and Shaogang Gong. “Deep Association Learning for Unsupervised Video Person Re-identification.” ArXiv abs/1808.07301 (2018): n. pag.
- Chen, Yehansen, Lin Wan, Zhihang Li, Qianyan Jing and Zongyuan Sun. “Neural Feature Search for RGB-Infrared Person Re-Identification.” 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2021): 587-597.
- Chen, Yifan, Han Wang, Xiaolu Sun, Bin Fan and Chunrui Tang. “Deep Attention Aware Feature Learning for Person Re-Identification.” Pattern Recognit. 126 (2022): 108567.
- Chen, Ying-Cong, Xiatian Zhu, Weishi Zheng and Jianhuang Lai. “Person Re-Identification by Camera Correlation Aware Feature Augmentation.” IEEE Transactions on Pattern Analysis and Machine Intelligence 40 (2018): 392-408.
- Chen, Yongbiao, Shenmin Zhang, Fangxin Liu, Chenggang Wu, Kaicheng Guo and Zhengwei Qi. “DVHN: A Deep Hashing Framework for Large-scale Vehicle Re-identification.” ArXivabs/2112.04937 (2021): n. pag.
- Chen, Yun-Chun, Chao-Te Chou and Y. Wang. “Learning to Learn in a Semi-Supervised Fashion.” ECCV (2020).
- Chen, Yun-Chun, Yu-Jhe Li, Xiaofei Du and Y. Wang. “Learning Resolution-Invariant Deep Representations for Person Re-Identification.” AAAI (2019).
- Chen, Yuntao, Naiyan Wang and Zhaoxiang Zhang. “DarkRank: Accelerating Deep Metric Learning via Cross Sample Similarities Transfer.” AAAI (2018).
- Chen, Zhirui, Jianheng Li and Weishi Zheng. “Weakly Supervised Tracklet Person Re-Identification by Deep Feature-wise Mutual Learning.” ArXiv abs/1910.14333 (2019): n. pag.

- Chen, Zhiyuan, Annan Li, Shilu Jiang and Yunhong Wang. “Attribute-aware Identity-hard Triplet Loss for Video-based Person Re-identification.” ArXiv abs/2006.07597 (2020): n. pag.
- Chena, Bingyang, Xingjie Zeng and Weishan Zhang. “Federated Learning for Cross-block Oil-water Layer Identification.” ArXiv abs/2112.14359 (2021): n. pag.
- Cheng, De, Jingyu Zhou, N. Wang and Xinbo Gao. “Hybrid Dynamic Contrast and Probability Distillation for Unsupervised Person Re-Id.” IEEE Transactions on Image Processing 31 (2022): 3334-3346.
- Cheng, De, Yihong Gong, Zhihui Li, Weiwei Shi, Alexander G. Hauptmann and Nanning Zheng. “Deep Feature Learning via Structured Graph Laplacian Embedding for Person Re-Identification.” Pattern Recognit. 82 (2018): 94-104.
- Chidama, Yusuf Ephraim and Chidi G. Ononiwu. “Empirical Study of Sustaining the Actualized Value Propositions of Implemented E-Government Projects in Sub-Saharan Africa.” ArXivabs/2108.09769 (2021): n. pag.
- Chinta, Vamsi Krishna, Chan-Ye Ohh, Geoffrey R. Spedding and Mitul Luhar. “Regime identification for stratified wakes from limited measurements: A library-based sparse regression formulation.” Physical Review Fluids (2022): n. pag.
- Cho, Yeong-Jun and Kuk-jin Yoon. “Distance-based Camera Network Topology Inference for Person Re-identification.” Pattern Recognit. Lett. 125 (2019): 220-227.
- Cho, Yeong-Jun and Kuk-jin Yoon. “PaMM: Pose-Aware Multi-Shot Matching for Improving Person Re-Identification.” IEEE Transactions on Image Processing 27 (2018): 3739-3752.
- Cho, Yeong-Jun, Jae-Han Park, Su-A. Kim, Kyuewang Lee and Kuk-Jin Yoon. “Unified Framework for Automated Person Re-identification and Camera Network Topology Inference in Camera Networks.” 2017 IEEE International Conference on Computer Vision Workshops (ICCVW) (2017): 2601-2607.
- Cho, Yeong-Jun, Su-A. Kim, Jae-Han Park, Kyuewang Lee and Kuk-jin Yoon. “Joint Person Re-identification and Camera Network Topology Inference in Multiple Cameras.” Comput. Vis. Image Underst. 180 (2019): 34-46.
- Cho, Yoon Hee, Woo Jae Kim, Seunghoon Hong and Sung-eui Yoon. “Part-based Pseudo Label Refinement for Unsupervised Person Re-identification.” ArXiv abs/2203.14675 (2022): n. pag.
- Choi, Sanghyuk, Jeong-in Hwang, Hyungjong Noh and Yeonsoo Lee. “May the Force Be with Your Copy Mechanism: Enhanced Supervised-Copy Method for Natural Language Generation.” ArXivabs/2112.10360 (2021): n. pag.
- Choi, Seokeon, Sumin Lee, Youngeun Kim, Taekyung Kim and Changick Kim. “Hi-CMD: Hierarchical Cross-Modality Disentanglement for Visible-Infrared Person Re-Identification.” 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2020): 10254-10263.
- Choi, Seokeon, Taekyung Kim, Minki Jeong, Hyoungseob Park and Changick Kim. “Meta Batch-Instance Normalization for Generalizable Person Re-Identification.” 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2021): 3424-3434.
- Choi, Yapkan, Yeshwanth Napolean and Jan C. van Gemert. “The Arm-Swing is Discriminative in Video Gait Recognition for Athlete Re-Identification.” 2021 IEEE International Conference on Image Processing (ICIP) (2021): 2309-2313.

- Choudhary, Ankit, Deepak Mishra and Arnab Karmakar. “Domain Adaptive Egocentric Person Re-identification.” CVIP (2020).
- Christlein, Vincent, Lukas Spranger, Mathias Seuret, Anguelos Nicolaou, Pavel Král and Andreas K. Maier. “Deep Generalized Max Pooling.” 2019 International Conference on Document Analysis and Recognition (ICDAR) (2019): 1090-1096.
- Chu, Ruihang, Yifan Sun, Yadong Li, Zheng Ping Liu, Chi Zhang and Yichen Wei. “Vehicle Re-Identification With Viewpoint-Aware Metric Learning.” 2019 IEEE/CVF International Conference on Computer Vision (ICCV) (2019): 8281-8290.
- Chung, Tae-Young, Heansung Lee, MyeongAh Cho, Suhwan Cho and Sangyoun Lee. “Multi-object tracking with self-supervised associating network.” ArXiv abs/2010.13424 (2020): n. pag.
- Comandur, Bharath. “Sports Re-ID: Improving Re-Identification Of Players In Broadcast Videos Of Team Sports.” (2022).
- Corianò, Claudio and Matteo Maria Maglio. “The general 3-graviton vertex (TTT) of conformal field theories in momentum space in $d = 4$.” Nuclear Physics B (2018): n. pag.
- Cortés, Irene, Jorge Beltrán, Arturo de la Escalera and Fernando Turrado García. “siaNMS: Non-Maximum Suppression with Siamese Networks for Multi-Camera 3D Object Detection.” 2020 IEEE Intelligent Vehicles Symposium (IV) (2020): 933-938.
- Culnane, Chris, Benjamin I. P. Rubinstein and Vanessa Teague. “Health Data in an Open World.” ArXiv abs/1712.05627 (2017): n. pag.
- Culnane, Chris, Benjamin I. P. Rubinstein and Vanessa Teague. “Options for encoding names for data linking at the Australian Bureau of Statistics.” ArXiv abs/1802.07975 (2018): n. pag.
- Culnane, Chris, Benjamin I. P. Rubinstein and Vanessa Teague. “Stop the Open Data Bus, We Want to Get Off.” ArXiv abs/1908.05004 (2019): n. pag.
- Cvrček, Václav and Masako Ueda Fidler. “No Keyword is an Island: In search of covert associations.” ArXiv abs/2103.17114 (2021): n. pag.
- Czado, Claudia and Sebastian Scharl. “Analysis of an interventional protein experiment using a vine copula based structural equation model.” (2021).
- Dahan, Eran and Tzvi Diskin. “COFGA: Classification Of Fine-Grained Features In Aerial Images.” ArXiv abs/1808.09001 (2018): n. pag.
- Dai, Ju, Pingping Zhang, D. Wang, Huchuan Lu and Hongyu Wang. “Video Person Re-Identification by Temporal Residual Learning.” IEEE Transactions on Image Processing 28 (2019): 1366-1377.
- Dai, Yongxing, Jun Liu, Yan Bai, Zekun Tong and Ling-yu Duan. “Dual-Refinement: Joint Label and Feature Refinement for Unsupervised Domain Adaptive Person Re-Identification.” IEEE Transactions on Image Processing 30 (2021): 7815-7829.
- Dai, Yongxing, Jun Liu, Yifan Sun, Zekun Tong, Chi Zhang and Ling-yu Duan. “IDM: An Intermediate Domain Module for Domain Adaptive Person Re-ID.” 2021 IEEE/CVF International Conference on Computer Vision (ICCV) (2021): 11844-11854.
- Dai, Yongxing, Xiaotong Li, Jun Liu, Zekun Tong and Ling-yu Duan. “Generalizable Person Re-identification with Relevance-aware Mixture of

Experts.” 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2021): 16140-16149.
- Dai, Yongxing, Yifan Sun, Jun Liu, Zekun Tong, Yi Yang and Ling-yu Duan. “Bridging the Source-to-target Gap for Cross-domain Person Re-Identification with Intermediate Domains.” ArXivabs/2203.01682 (2022): n. pag.
- Dai, Zuozhuo, Guangyuan Wang, Siyu Zhu, Weihao Yuan and Ping Tan. “Cluster Contrast for Unsupervised Person Re-Identification.” ArXiv abs/2103.11568 (2021): n. pag.
- Dai, Zuozhuo, Mingqiang Chen, Xiaodong Gu, Siyu Zhu and Ping Tan. “Batch DropBlock Network for Person Re-Identification and Beyond.” 2019 IEEE/CVF International Conference on Computer Vision (ICCV) (2019): 3690-3700.
- Dall’Asen, Nicola, Yiming Wang, Hao Tang, Luca Zanella and Elisa Ricci. “Graph-based Generative Face Anonymisation with Pose Preservation.” ICIAP (2022).
- Das, Abir, Rameswar Panda and Amit K. Roy-Chowdhury. “Continuous adaptation of multi-camera person identification models through sparse non-redundant representative selection.” Comput. Vis. Image Underst. 156 (2017): 66-78.
- Daubner, Lukas and Raimundas Matulevičius. “Risk-Oriented Design Approach For Forensic-Ready Software Systems.” The 16th International Conference on Availability, Reliability and Security(2021): n. pag.
- Dawson, Glenn, Muhammad Umer and Robi Polikar. “Contributor-Aware Defenses Against Adversarial Backdoor Attacks.” (2022).
- Dawson, Kyle S., Jean-Paul Kneib, et al. “The SDSS-IV extended baryon oscillation spectroscopic survey: Overview and early data.” The Astronomical Journal 151 (2016): 44-44.
- Dehaye, Paul-Olivier and Joel Reardon. “Proximity Tracing in an Ecosystem of Surveillance Capitalism.” Proceedings of the 19th Workshop on Privacy in the Electronic Society (2020): n. pag.
- Dehaye, Paul-Olivier and Joel Reardon. “SwissCovid: a critical analysis of risk assessment by Swiss authorities.” ArXiv abs/2006.10719 (2020): n. pag.
- Delaney, Anne Marie, Eoin Brophy and Tomas E. Ward. “Synthesis of Realistic ECG using Generative Adversarial Networks.” ArXiv abs/1909.09150 (2019): n. pag.
- Delorme, Guillaume, Yihong Xu, Stéphane Lathuilière, Radu Horaud and Xavier Alameda-Pineda. “CANU-ReID: A Conditional Adversarial Network for Unsupervised person Re-IDentification.” 2020 25th International Conference on Pattern Recognition (ICPR) (2021): 4428-4435.
- Deng, Nan, B. R. Noack, Marek Morzy’nski and Luc Pastur. “Cluster-based hierarchical network model of the fluidic pinball – cartographing transient and post-transient, multi-frequency, multi-attractor behaviour.” Journal of Fluid Mechanics 934 (2022): n. pag.
- Deng, Weijian, Liang Zheng, Guoliang Kang, Yezhou Yang, Qixiang Ye and Jianbin Jiao. “Image-Image Domain Adaptation with Preserved Self-Similarity and Domain-Dissimilarity for Person Re-identification.” 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition (2018): 994-1003.
- Deng, Weijian, Liang Zheng, Qixiang Ye, Yi Yang and Jianbin Jiao. “Similarity-preserving Image-image Domain Adaptation for Person Re-identification.” ArXiv abs/1811.10551 (2018): n. pag.

- Desmet, Chance and Diane Joyce Cook. “HydraGAN A Multi-head, Multi-objective Approach to Synthetic Data Generation.” ArXiv abs/2111.07015 (2021): n. pag.
- Dessì, Roberto, Eugene Kharitonov and Marco Baroni. “Interpretable agent communication from scratch(with a generic visual processor emerging on the side).” ArXiv abs/2106.04258 (2021): n. pag.
- D’iaz, Iv’an and Nima S. Hejazi. “Causal mediation analysis for stochastic interventions.” Journal of the Royal Statistical Society: Series B (Statistical Methodology) 82 (2020): n. pag.
- DiazOrdaz, Karla and James R. Carpenter. “Local average treatment effects estimation via substantive model compatible multiple imputation.” Biometrical Journal 61 (2019): 1526 - 1540.
- Dietlmeier, Julia, Feiyan Hu, Frances Ryan, Noel E. O’Connor and Kevin McGuinness. “Improving Person Re-Identification with Temporal Constraints.” 2022 IEEE/CVF Winter Conference on Applications of Computer Vision Workshops (WACVW) (2022): 540-549.
- Dietlmeier, Julia, Joseph Antony, Kevin McGuinness and Noel E. O’Connor. “How important are faces for person re-identification?” 2020 25th International Conference on Pattern Recognition (ICPR) (2021): 6912-6919.
- Ding, Changxing, Kan Wang, Pengfei Wang and Dacheng Tao. “Multi-Task Learning With Coarse Priors for Robust Part-Aware Person Re-Identification.” IEEE Transactions on Pattern Analysis and Machine Intelligence 44 (2022): 1474-1488.
- Ding, Guodong, Salman Hameed Khan, Zhen-min Tang and Fatih Murat Porikli. “Let Features Decide for Themselves: Feature Mask Network for Person Re-identification.” ArXivabs/1711.07155 (2017): n. pag.
- Ding, Guodong, Salman Hameed Khan, Zhen-min Tang, Jian Zhang and Fatih Murat Porikli. “Towards better Validity: Dispersion based Clustering for Unsupervised Person Re-identification.” ArXiv abs/1906.01308 (2019): n. pag.
- Ding, Guodong, Shanshan Zhang, Salman Hameed Khan, Zhen-min Tang, Jian Zhang and Fatih Murat Porikli. “Feature Affinity-Based Pseudo Labeling for Semi-Supervised Person Re-Identification.” IEEE Transactions on Multimedia 21 (2019): 2891-2902.
- Ding, Jian, Enze Xie, Hang Xu, Chenhan Jiang, Zhenguo Li, Ping Luo and Guisong Xia. “Deeply Unsupervised Patch Re-Identification for Pre-training Object Detectors.” IEEE transactions on pattern analysis and machine intelligence PP (2022): n. pag.
- Ding, Jingwen and Xue Zhou. “Learning Feature Fusion for Unsupervised Domain Adaptive Person Re-identification.” ArXiv abs/2205.09495 (2022): n. pag.
- Ding, Wenjie, Xing Wei, Yunfeng Qiu, Rongrong Ji, Xiaopeng Hong and Yihong Gong. “Beyond Universal Person Re-ID Attack.” arXiv: Computer Vision and Pattern Recognition (2020): n. pag.
- Ding, Yuhang, Hehe Fan, Mingliang Xu and Yezhou Yang. “Adaptive Exploration for Unsupervised Person Re-identification.” ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM) 16 (2020): 1 - 19.
- Ding, Zefeng, Changxing Ding, Zhiyin Shao and Dacheng Tao. “Semantically Self-Aligned Network for Text-to-Image Part-aware Person Re-identification.” ArXiv abs/2107.12666 (2021): n. pag.

- Ding, Zixiang, Huihui He, Mengran Zhang and Rui Xia. “From Independent Prediction to Re-ordered Prediction: Integrating Relative Position and Global Label Information to Emotion Cause Identification.” AAAI (2019).
- Disney, Michael John, Roger H. Lang and Juergen Ott. “Clustering and the Search for Dim and Dark Galaxies.” arXiv: Astrophysics of Galaxies (2016): n. pag.
- Doering, Andreas, Di Chen, Shanshan Zhang, Bernt Schiele and Juergen Gall. “PoseTrackReID: Dataset Description.” ArXiv abs/2011.06243 (2020): n. pag.
- Domingo-Ferrer, Josep, Krishnamurty Muralidhar and Maria Bras-Amorós. “General Confidentiality and Utility Metrics for Privacy-Preserving Data Publishing Based on the Permutation Model.” IEEE Transactions on Dependable and Secure Computing 18 (2021): 2506-2517.
- Domps, Baptiste, Julien Marmain and Charles-Antoine Gu’erin. “A Reanalysis of the October 2016 "Meteotsunami" in British Columbia With Help of High-Frequency Radars and Autoregressive Modeling.” IEEE Geosci. Remote. Sens. Lett. 19 (2022): 1-5.
- Drechsler, M., Frederik Lohof and Christopher Gies. “Revisiting the Siegert relation for the partially coherent regime of nanolasers.” Applied Physics Letters (2022): n. pag.
- Dubourvieux, Fabian, Angelique Loesch, Romaric Audigier, Samia Ainouz and Stéphane Canu. “Improving Unsupervised Domain Adaptive Re-Identification Via Source-Guided Selection of Pseudo-Labeling Hyperparameters.” IEEE Access 9 (2021): 149780-149795.
- Dubourvieux, Fabian, Romaric Audigier, Angelique Loesch, Samia Ainouz and Stéphane Canu. “A formal approach to good practices in Pseudo-Labeling for Unsupervised Domain Adaptive Re-Identification.” ArXiv abs/2112.12887 (2021): n. pag.
- Dubourvieux, Fabian, Romaric Audigier, Angelique Loesch, Samia Ainouz and Stéphane Canu. “Unsupervised Domain Adaptation for Person Re-Identification through Source-Guided Pseudo-Labeling.” 2020 25th International Conference on Pattern Recognition (ICPR) (2021): 4957-4964.
- Dwivedi, Raaz, Yan Shuo Tan, Briton Park, Mian Wei, Kevin Horgan, David Madigan and Bin Yu. “Stable Discovery of Interpretable Subgroups via Calibration in Causal Studies.” International Statistical Review 88 (2020): S135 - S178.
- Eberle, Andreas. “Pose-Driven Deep Models for Person Re-Identification.” ArXiv abs/1803.08709 (2018): n. pag.
- Edwards, Victoria, Loy Mcguire and Signe A. Redfield. “Establishing Reliable Robot Behavior using Capability Analysis Tables.” AREA@ECAI (2020).
- Eibl, Günther, Kaibin Bao, Philip-William Grassal, Daniel Bernau and Hartmut Schmeck. “The influence of differential privacy on short term electric load forecasting.” Energy Informatics 1 (2018): 93-113.
- Ekladious, George S. Eskander, Hugo Lemoine, Éric Granger, Kaveh Kamali and Salim Moudache. “Dual-Triplet Metric Learning for Unsupervised Domain Adaptation in Video-Based Face Recognition.” ArXiv abs/2002.04206 (2020): n. pag.
- Elezi, Ismail, Jenny Seidenschwarz, Laurin Wagner, Sebastiano Vascon, Alessandro Torcinovich, Marcello Pelillo and Laura Leal-Taixé. “The Group Loss++: A deeper look into group loss for deep metric learning.” IEEE transactions on pattern analysis and machine intelligence PP (2022): n. pag.

- Elkoumy, Gamal, Alisa Pankova and Marlon Dumas. “Privacy-Preserving Directly-Follows Graphs: Balancing Risk and Utility in Process Mining.” ArXiv abs/2012.01119 (2020): n. pag.
- Eller, P., Nahuel Ferreiro Iachellini, Luca Pattavina and Lolian Shtembari. “Online triggers for supernova and pre-supernova neutrino detection with cryogenic detectors.” (2022).
- Enokiya, Rei and Yasuo Fukui. “A Multiwavelength Study of the Sgr B Region: Contiguous Cloud–Cloud Collisions Triggering Widespread Star Formation Events?” The Astrophysical Journal 931 (2022): n. pag.
- Eom, Chanho and Bumsub Ham. “Learning Disentangled Representation for Robust Person Re-identification.” NeurIPS (2019).
- Eom, Chanho, Geon Lee, Junghyup Lee and Bumsub Ham. “Video-based Person Re-identification with Spatial and Temporal Memory Networks.” 2021 IEEE/CVF International Conference on Computer Vision (ICCV) (2021): 12016-12025.
- Fabbri, Matteo, Guillem Brasó, Gianluca Maugeri, Orcun Cetintas, Riccardo Gasparini, Aljosa Osep, Simone Calderara, Laura Leal-Taixé and Rita Cucchiara. “MOTSynth: How Can Synthetic Data Help Pedestrian Detection and Tracking?” 2021 IEEE/CVF International Conference on Computer Vision (ICCV) (2021): 10829-10839.
- Fabien, Mael, Seyyed Saeed Sarfjoo, Petr Motlícek and Srikanth R. Madikeri. “Improving Speaker Identification using Network Knowledge in Criminal Conversational Data.” ArXiv abs/2006.02093 (2021): n. pag.
- Fan, Hehe, Liang Zheng and Yi Yang. “Unsupervised Person Re-identification: Clustering and Fine-tuning.” arXiv: Computer Vision and Pattern Recognition (2017): n. pag.
- Fan, Lijie, Tianhong Li, Rongyao Fang, Rumen Hristov, Yuan Yuan and Dina Katabi. “Learning Longterm Representations for Person Re-Identification Using Radio Signals.” 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2020): 10696-10706.
- Fan, Xing, Hao Luo, Chi Zhang and Wei Jiang. “Cross-Spectrum Dual-Subspace Pairing for RGB-infrared Cross-Modality Person Re-Identification.” ArXiv abs/2003.00213 (2020): n. pag.
- Fan, Xing, Hao Luo, Xuan Zhang, Lingxiao He, Chi Zhang and Wei Jiang. “SCPNet: Spatial-Channel Parallelism Network for Joint Holistic and Partial Person Re-Identification.” ACCV (2018).
- Fan, Xing, Wei Jiang, Hao Luo and Mengjuan Fei. “SphereReID: Deep Hypersphere Manifold Embedding for Person Re-Identification.” J. Vis. Commun. Image Represent. 60 (2019): 51-58.
- Fang, Pengfei, Pan Ji, Lars Petersson and Mehrtash Tafazzoli Harandi. “Set Augmented Triplet Loss for Video Person Re-Identification.” 2021 IEEE Winter Conference on Applications of Computer Vision (WACV) (2021): 464-473.
- Farooq, Ammarah, Muhammad Awais, Fei Yan, Josef Kittler, Ali Akbari and Syed Safwan Khalid. “A Convolutional Baseline for Person Re-Identification Using Vision and Language Descriptions.” ArXiv abs/2003.00808 (2020): n. pag.
- Farooq, Ammarah, Muhammad Awais, Josef Kittler and Syed Safwan Khalid. “AXM-Net: Cross-Modal Context Sharing Attention Network for Person Re-ID.” ArXiv abs/2101.08238 (2021): n. pag.

- Favato, Danilo, Gabriel Coutinho, Mário S. Alvim and Natasha Fernandes. “A novel reconstruction attack on foreign-trade official statistics, with a Brazilian case study.” (2022).
- Fedorov, Igor, Ritwik Giri, Bhaskar D. Rao and Truong Q. Nguyen. “Relevance Subject Machine: A Novel Person Re-identification Framework.” ArXiv abs/1703.10645 (2017): n. pag.
- Feng, Hao, Minghao Chen, Jinming Hu, Dong Shen, Haifeng Liu and Deng Cai. “Complementary Pseudo Labels for Unsupervised Domain Adaptation On Person Re-Identification.” IEEE Transactions on Image Processing 30 (2021): 2898-2907.
- Feng, Weitao, Zhihao Hu, Wei Wu, Junjie Yan and Wanli Ouyang. “Multi-Object Tracking with Multiple Cues and Switcher-Aware Classification.” ArXiv abs/1901.06129 (2019): n. pag.
- Feng, Yang, Yu Wang and Jiebo Luo. “Video-based Person Re-Identification using Gated Convolutional Recurrent Neural Networks.” ArXiv abs/2003.09717 (2020): n. pag.
- Feng, Yujian, Feng Chen, Jian Yu, Yimu Ji, Fei Wu and Shangdong Liu. “Homogeneous and Heterogeneous Relational Graph for Visible-infrared Person Re-identification.” ArXivabs/2109.08811 (2021): n. pag.
- Feng, Zhanxiang, Jianhuang Lai and Xiaohua Xie. “Learning View-Specific Deep Networks for Person Re-Identification.” IEEE Transactions on Image Processing 27 (2018): 3472-3483.
- Feng, Zhi, Haoyi Xiong, Chuanyuan Song, Sijia Yang, Baoxin Zhao, Licheng Wang, Zeyu Chen, Shengwen Yang, Liping Liu and Jun Huan. “SecureGBM: Secure Multi-Party Gradient Boosting.” 2019 IEEE International Conference on Big Data (Big Data) (2019): 1312-1321.
- Fernando, Tharindu, Simon Denman, Sridha Sridharan and Clinton Fookes. “Tracking by Prediction: A Deep Generative Model for Mutli-person Localisation and Tracking.” 2018 IEEE Winter Conference on Applications of Computer Vision (WACV) (2018): 1122-1132.
- Ferrari, Claudio, Stefano Berretti and A. Bimbo. “Extended YouTube Faces: a Dataset for Heterogeneous Open-Set Face Identification.” 2018 24th International Conference on Pattern Recognition (ICPR) (2018): 3408-3413.
- Forneron, Jean-Jacques. “Detecting Identification Failure in Moment Condition Models.” arXiv: Econometrics (2019): n. pag.
- Francis, Paul L.. “A Note on the Misinterpretation of the US Census Re-identification Attack.” ArXivabs/2202.04872 (2022): n. pag.
- Fu, Chaoyou, Yibo Hu, Xiang Wu, Hailin Shi, Tao Mei and Ran He. “CM-NAS: Cross-Modality Neural Architecture Search for Visible-Infrared Person Re-Identification.” 2021 IEEE/CVF International Conference on Computer Vision (ICCV) (2021): 11803-11812.
- Fu, Dengpan, Bo Xin, Jingdong Wang, Dongdong Chen, Jianmin Bao, Gang Hua and Houqiang Li. “Improving Person Re-Identification With Iterative Impression Aggregation.” IEEE Transactions on Image Processing 29 (2020): 9559-9571.
- Fu, Dengpan, Dongdong Chen, Hao Yang, Jianmin Bao, Lu Yuan, Lei Zhang, Houqiang Li, Fang Wen and Dong Chen. “Large-Scale Pre-training for Person Re-identification with Noisy Labels.” ArXivabs/2203.16533 (2022): n. pag.
- Fu, Dengpan, Dongdong Chen, Jianmin Bao, Hao Yang, Lu Yuan, Lei Zhang, Houqiang Li and Dong Chen. “Unsupervised Pre-training for Person Re-

identification." 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2021): 14745-14754.
- Fu, Luoyi, Jiapeng Zhang, Shuaiqi Wang, Xinyu Wu, Xinbing Wang and Guihai Chen. "De-Anonymizing Social Networks With Overlapping Community Structure." IEEE/ACM Transactions on Networking 28 (2020): 360-375.
- Fu, Xinzhe, Zhongzhao Hu, Zhiying Xu, Luoyi Fu and Xinbing Wang. "De-anonymization of Social Networks with Communities: When Quantifications Meet Algorithms." ArXiv abs/1703.09028 (2017): n. pag.
- Fu, Yang, Xiaoyang Wang, Yunchao Wei and Thomas Huang. "STA: Spatial-Temporal Attention for Large-Scale Video-based Person Re-Identification." ArXiv abs/1811.04129 (2019): n. pag.
- Fu, Yang, Yunchao Wei, Guanshuo Wang, Xi Zhou, Humphrey Shi and Thomas S. Huang. "Self-Similarity Grouping: A Simple Unsupervised Cross Domain Adaptation Approach for Person Re-Identification." 2019 IEEE/CVF International Conference on Computer Vision (ICCV) (2019): 6111-6120.
- Fu, Yang, Yunchao Wei, Yuqian Zhou, Humphrey Shi, Gao Huang, Xinchao Wang, Zhiqiang Yao and Thomas S. Huang. "Horizontal Pyramid Matching for Person Re-identification." ArXivabs/1804.05275 (2019): n. pag.
- Gajic, Bojana, Ariel Amato, Ramón Baldrich and Carlo Gatta. "Bag of Negatives for Siamese Architectures." BMVC (2019).
- Ganin, Yaroslav, E. Ustinova, Hana Ajakan, Pascal Germain, H. Larochelle, François Laviolette, Mario Marchand and Victor S. Lempitsky. "Domain-Adversarial Training of Neural Networks." J. Mach. Learn. Res. (2016).
- Gao, Cunyuan, Y. Hu, Yi Zhang, Rui Yao, Yong Zhou and Jiaqi Zhao. "Vehicle Re-Identification Based on Complementary Features." 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW) (2020): 2520-2526.
- Gao, Guangwei, Hao-Chiang Shao, Yi Yu, Fei Wu and Meng Yang. "Leaning Compact and Representative Features for Cross-Modality Person Re-Identification." ArXiv abs/2103.14210 (2022): n. pag.
- Gao, Shang, Jingya Wang, Huchuan Lu and Zimo Liu. "Pose-Guided Visible Part Matching for Occluded Person ReID." 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2020): 11741-11749.
- Gao, Wen Jun Calvin and Minxian Li. "Unsupervised Clustering Active Learning for Person Re-identification." ArXiv abs/2112.13308 (2021): n. pag.
- Gao, Yajun, Tengfei Liang, Yi Jin, Xiaoyan Gu, Wu Liu, Yidong Li and Congyan Lang. "MSO: Multi-Feature Space Joint Optimization Network for RGB-Infrared Person Re-Identification." Proceedings of the 29th ACM International Conference on Multimedia (2021): n. pag.
- Gao, Zan, Hongwei Wei, Weili Guan, Weizhi Nie, Meng Liu and Meng Wang. "Multigranular Visual-Semantic Embedding for Cloth-Changing Person Re-identification." ArXiv abs/2108.04527 (2021): n. pag.
- Garat, Diego and Dina Wonsever. "Towards De-identification of Legal Texts." ArXivabs/1910.03739 (2019): n. pag.
- Gauld, R., A. Gehrmann-De Ridder, E. W. N. Glover, Alexander Huss and I. Majer. "Associated production of a Higgs boson decaying into bottom quarks and a weak vector boson decaying leptonically at NNLO in QCD." Journal of High Energy Physics (2019): n. pag.

- Gazak, Jonathan Zachary, Ian McQuaid, R. I. Swindle, Matthew G. Phelps and Justin Fletcher. “SpectraNet: Learned Recognition of Artificial Satellites from High Contrast Spectroscopic Imagery.” 2022 IEEE/CVF Winter Conference on Applications of Computer Vision (WACV) (2022): 2403-2411.
- Ge, Wenhang, Chunyan Pan, Ancong Wu, Hongwei Zheng and Weishi Zheng. “Cross-Camera Feature Prediction for Intra-Camera Supervised Person Re-identification across Distant Scenes.” Proceedings of the 29th ACM International Conference on Multimedia (2021): n. pag.
- Ge, Yixiao, Dapeng Chen and Hongsheng Li. “Mutual Mean-Teaching: Pseudo Label Refinery for Unsupervised Domain Adaptation on Person Re-identification.” ArXiv abs/2001.01526 (2020): n. pag.
- Ge, Yixiao, Dapeng Chen, Feng Zhu, Rui Zhao and Hongsheng Li. “Self-paced Contrastive Learning with Hybrid Memory for Domain Adaptive Object Re-ID.” ArXiv abs/2006.02713 (2020): n. pag.
- Ge, Yixiao, Feng Zhu, Rui Zhao and Hongsheng Li. “Structured Domain Adaptation With Online Relation Regularization for Unsupervised Person Re-ID.” IEEE transactions on neural networks and learning systems PP (2022): n. pag.
- Ge, Yixiao, Zhuowan Li, Haiyu Zhao, Guojun Yin, Shuai Yi, Xiaogang Wang and Hongsheng Li. “FD-GAN: Pose-guided Feature Distilling GAN for Robust Person Re-identification.” ArXivabs/1810.02936 (2018): n. pag.
- Ge, Yuying, Ruimao Zhang, Lingyun Wu, Xiaogang Wang, Xiaoou Tang and Ping Luo. “DeepFashion2: A Versatile Benchmark for Detection, Pose Estimation, Segmentation and Re-Identification of Clothing Images.” 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2019): 5332-5340.
- Geng, Mengyue, Yaowei Wang, Tao Xiang and Yonghong Tian. “Deep Transfer Learning for Person Re-Identification.” 2018 IEEE Fourth International Conference on Multimedia Big Data (BigMM)(2018): 1-5.
- Ghosh, Adhir, Kuruparan Shanmugalingam and Wen-Yan Lin. “Relation Preserving Triplet Mining for Stabilizing the Triplet Loss in Vehicle Re-identification.” ArXiv abs/2110.07933 (2021): n. pag.
- Girbau, Andreu, Xavier Gir’o-i-Nieto, Ignasi Rius and F. Miguel Marqu’es. “Multiple Object Tracking with Mixture Density Networks for Trajectory Estimation.” ArXiv abs/2106.10950 (2021): n. pag.
- Goel, Abhinav, Caleb Tung, Xiao Hu, Haobo Wang, James C. Davis, George K. Thiruvathukal and Yung-Hsiang Lu. “Low-Power Multi-Camera Object Re-Identification using Hierarchical Neural Networks.” 2021 IEEE/ACM International Symposium on Low Power Electronics and Design (ISLPED) (2021): 1-6.
- Goldsmith-Pinkham, Paul, Peter Hull and M. Kolesár. “Contamination Bias in Linear Regressions.” (2022).
- Gomez, Tristan, Suiyi Ling, Thomas Fr’eour and Harold Mouchère. “BR-NPA: A Non-Parametric High-Resolution Attention Model to improve the Interpretability of Attention.” (2021).
- G’omez-Silva, Mar’ia J., José María Armingol and Arturo de la Escalera. “Triplet Permutation Method for Deep Learning of Single-Shot Person Re-Identification.” ArXiv abs/2003.08303 (2019): n. pag.

- Gong, Albert, Qiang Qiu and Guillermo Sapiro. “Virtual CNN Branching: Efficient Feature Ensemble for Person Re-Identification.” ArXiv abs/1803.05872 (2018): n. pag.
- Gong, Liqing Huang and Lifei Chen. “Person Re-identification Method Based on Color Attack and Joint Defence.” (2022).
- Gong, Yunpeng and Lifei Chen. “Robust Person Re-identification with Multi-Modal Joint Defence.” ArXiv abs/2111.09571 (2021): n. pag.
- Gong, Yunpeng, Zhiyong Zeng, Liwen Chen, Yi-Xiao Luo, Bin Weng and Feng Ye. “A Person Re-identification Data Augmentation Method with Adversarial Defense Effect.” ArXiv abs/2101.08783 (2021): n. pag.
- Gong, Yunpeng. “A general multi-modal data learning method for Person Re-identification.” (2021).
- Gou, Mengran and Xikang Zhang. “Person Re-id in Appearance Impaired Scenarios.” (2016).
- Granvik, Mikael and Peter Brown. “Identification of meteorite source regions in the Solar System.” Icarus (2018): n. pag.
- Greene, Olivia, Miguel Ricardo Anderson, Mariarosa Marinelli, Kelly Holley-Bockelmann, Lauren E. P. Campbell and Charles T. Liu. “Refining the E + A Galaxy: A Spatially Resolved Spectrophotometric Sample of Nearby Post-starburst Systems in SDSS-IV MaNGA (MPL-5).” The Astrophysical Journal 910 (2021): n. pag.
- Gu, Jianyang, Haowen Luo, Weihua Chen, Yiqi Jiang, Yuqi Zhang, Shuting He, F. Wang, Hao Li and Wei Jiang. “1st Place Solution to VisDA-2020: Bias Elimination for Domain Adaptive Pedestrian Re-identification.” ArXiv abs/2012.13498 (2020): n. pag.
- Gu, Xinqian, Bingpeng Ma, Hong Chang, S. Shan and Xilin Chen. “Temporal Knowledge Propagation for Image-to-Video Person Re-Identification.” 2019 IEEE/CVF International Conference on Computer Vision (ICCV) (2019): 9646-9655.
- Gu, Xinqian, Hong Chang, Bingpeng Ma, Hongkai Zhang and Xilin Chen. “Appearance-Preserving 3D Convolution for Video-based Person Re-identification.” ECCV (2020).
- Gu, Xinqian, Hong Chang, Bingpeng Ma, Shutao Bai, S. Shan and Xilin Chen. “Clothes-Changing Person Re-identification with RGB Modality Only.” ArXiv abs/2204.06890 (2022): n. pag.
- Gualdani, Cristina and Shruti Sinha. “Partial Identification in Matching Models for the Marriage Market.” (2019).
- Gulyás, Gábor György, Benedek Simon and Sándor Imre. “An Efficient and Robust Social Network De-anonymization Attack.” Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Society (2016): n. pag.
- Guo, Jianyuan, Yuhui Yuan, Lang Huang, Chao Zhang, Jin-Ge Yao and Kai Han. “Beyond Human Parts: Dual Part-Aligned Representations for Person Re-Identification.” 2019 IEEE/CVF International Conference on Computer Vision (ICCV) (2019): 3641-3650.
- Guo, Yiluan and Ngai-Man Cheung. “Efficient and Deep Person Re-identification Using Multi-level Similarity.” 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition (2018): 2335-2344.

- Guo, Zijian, Hyunseung Kang, T. Tony Cai and Dylan S. Small. “Confidence intervals for causal effects with invalid instruments by using two-stage hard thresholding with voting.” Journal of the Royal Statistical Society: Series B (Statistical Methodology) 80 (2016): n. pag.
- Guzm’an-Inigo, Juan, Markus Andreas Sodar and George P. Papadakis. “Data-based, reduced-order, dynamic estimator for reconstruction of nonlinear flows exhibiting limit-cycle oscillations.” Physical Review Fluids (2019): n. pag.
- Ha, Mai Lan and Volker Blanz. “Deep Ranking with Adaptive Margin Triplet Loss.” ArXivabs/2107.06187 (2021): n. pag.
- Habibullah, Khan Mohammad and Jennifer Horkoff. “Non-functional Requirements for Machine Learning: Understanding Current Use and Challenges in Industry.” 2021 IEEE 29th International Requirements Engineering Conference (RE) (2021): 13-23.
- Hafner, Frank M., Amran H. Bhuyian, Julian F. P. Kooij and Éric Granger. “Cross-modal distillation for RGB-depth person re-identification.” Comput. Vis. Image Underst. 216 (2022): 103352.
- Hagan, J. Brendan, Élodie Choquet, Rémi Soummer and Arthur Vigan. “ALICE Data Release: A Revaluation of HST-NICMOS Coronagraphic Images.” The Astronomical Journal 155 (2018): 179.
- Han, Byeong-Ju, Kuhyeun Ko and Jae-Young Sim. “Context-Aware Unsupervised Clustering for Person Search.” ArXiv abs/2110.01341 (2021): n. pag.
- Han, Chuchu, Jiacheng Ye, Yunshan Zhong, Xin Tan, Chi Zhang, Changxin Gao and Nong Sang. “Re-ID Driven Localization Refinement for Person Search.” 2019 IEEE/CVF International Conference on Computer Vision (ICCV) (2019): 9813-9822.
- Han, Jian, Yali Li and Shengjin Wang. “Delving into Probabilistic Uncertainty for Unsupervised Domain Adaptive Person Re-Identification.” ArXiv abs/2112.14025 (2021): n. pag.
- Han, Jian. “Learning adaptively from the unknown for few-example video person re-ID.” ArXivabs/1908.09340 (2019): n. pag.
- Han, Kai, Jianyuan Guo, Chao Zhang and Mingjian Zhu. “Attribute-Aware Attention Model for Fine-grained Representation Learning.” Proceedings of the 26th ACM international conference on Multimedia (2018): n. pag.
- Han, Ke, Chenyang Si, Yan Huang, Liangsheng Wang and Tieniu Tan. “Generalizable Person Re-Identification via Self-Supervised Batch Norm Test-Time Adaption.” ArXiv abs/2203.00672 (2022): n. pag.
- Han, Shoudong, Piao Huang, Hongwei Wang, En Yu, Donghaisheng Liu, Xiaofeng Pan and Jun Zhao. “MAT: Motion-Aware Multi-Object Tracking.” ArXiv abs/2009.04794 (2022): n. pag.
- Han, Xiaotian, Quanzeng You, Chunyu Wang, Zhizheng Zhang, Peng Chu, Houdong Hu, Jiang Wang and Zicheng Liu. “MMPTRACK: Large-scale Densely Annotated Multi-camera Multiple People Tracking Benchmark.” ArXiv abs/2111.15157 (2021): n. pag.
- Han, Xumeng, Xuehui Yu, Guorong Li, Jian Zhao, Gang Pan, Qixiang Ye, Jianbin Jiao and Zhenjun Han. “Rethinking Sampling Strategies for Unsupervised Person Re-identification.” (2021).
- Hasan, S. M. Kamrul and Cristian A. Linte. “U-NetPlus: A Modified Encoder-Decoder U-Net Architecture for Semantic and Instance Segmentation of Surgical

Instruments from Laparoscopic Images." 2019 41st Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC) (2019): 7205-7211.
- He, Lingxiao, Jian Liang, Haiqing Li and Zhenan Sun. "Deep Spatial Feature Reconstruction for Partial Person Re-identification: Alignment-free Approach." 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition (2018): 7073-7082.
- He, Lingxiao, Wu Liu, Jian Liang, Kecheng Zheng, Xingyu Liao, Peng Cheng and Tao Mei. "Semi-Supervised Domain Generalizable Person Re-Identification." ArXiv abs/2108.05045 (2021): n. pag.
- He, Lingxiao, Xingyu Liao, Wu Liu, Xinchen Liu, Peng Cheng and Tao Mei. "FastReID: A Pytorch Toolbox for General Instance Re-identification." ArXiv abs/2006.02631 (2020): n. pag.
- He, Lingxiao, Yinggang Wang, Wu Liu, Xingyu Liao, He Zhao, Zhenan Sun and Jiashi Feng. "Foreground-Aware Pyramid Reconstruction for Alignment-Free Occluded Person Re-Identification." 2019 IEEE/CVF International Conference on Computer Vision (ICCV) (2019): 8449-8458.
- He, Lingxiao, Zhenan Sun, Yuhao Zhu and Yunbo Wang. "Recognizing Partial Biometric Patterns." ArXiv abs/1810.07399 (2018): n. pag.
- He, Shuting, Hao Luo, Weihua Chen, Miao Zhang, Yuqi Zhang, F. Wang, Hao Li and Wei Jiang. "Multi-Domain Learning and Identity Mining for Vehicle Re-Identification." 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW) (2020): 2485-2493.
- He, Shuting, Haowen Luo, Pichao Wang, F. Wang, Hao Li and Wei Jiang. "TransReID: Transformer-based Object Re-Identification." 2021 IEEE/CVF International Conference on Computer Vision (ICCV) (2021): 14993-15002.
- He, Tianyu, Xin Jin, Xu Shen, Jianqiang Huang, Zhibo Chen and Xiansheng Hua. "Dense Interaction Learning for Video-based Person Re-identification." 2021 IEEE/CVF International Conference on Computer Vision (ICCV) (2021): 1470-1481.
- He, Xuanyu, Wei Zhang, Ran Song and Xiangyuan Lan. "Take More Positives: A Contrastive Learning Framework for Unsupervised Person Re-Identification." ArXiv abs/2101.04340 (2021): n. pag.
- He, Zhenwei, Lei Zhang and Wei Jia. "End-to-End Detection and Re-identification Integrated Net for Person Search." ACCV (2018).
- He, Zhi-Fen, Hongbo Zhao and Wenquan Feng. "PGGANet: Pose Guided Graph Attention Network for Person Re-identification." (2021).
- Henkel, Christof. "Efficient large-scale image retrieval with deep feature orthogonality and Hybrid-Swin-Transformers." ArXiv abs/2110.03786 (2021): n. pag.
- Hermans, Alexander, Lucas Beyer and B. Leibe. "In Defense of the Triplet Loss for Person Re-Identification." ArXiv abs/1703.07737 (2017): n. pag.
- Herzog, Fabian, Xunbo Ji, Torben Teepe, Stefan Hörmann, Johannes Gilg and Gerhard Rigoll. "Lightweight Multi-Branch Network For Person Re-Identification." 2021 IEEE International Conference on Image Processing (ICIP) (2021): 1129-1133.
- Hilton, Michael L., Mark T. Yamane and Leah M. Knezevich. "An Image Processing Pipeline for Camera Trap Time-Lapse Recordings." (2022).

- Hirsch, Andreas and Frank Hauke. “Post-Graphene 2D Chemistry: The Emerging Field of Molybdenum Disulfide and Black Phosphorus Functionalization.” Angewandte Chemie (International Ed. in English) 57 (2018): 4338 - 4354.
- Hlad, Nicolas, Abdelhak-Djamel Seriai and Christophe Dony. “IsiSPL: Toward an Automated Reactive Approach to build Software Product Lines.” ArXiv abs/2107.00552 (2021): n. pag.
- Hoffmann, Susanne M. and Nikolaus Vogt. “A search for the modern counterparts of the Far Eastern guest stars 369 CE, 386 CE and 393 CE.” Monthly Notices of the Royal Astronomical Society 497 (2020): 1419-1433.
- Hoffmann, Susanne M. and Nikolaus Vogt. “Counterparts of Far Eastern Guest Stars: Novae, supernovae, or something else?” Monthly Notices of the Royal Astronomical Society 496 (2020): 4488-4506.
- Hoffmann, Susanne M.. “What information can we derive from historical Far Eastern guest stars for modern research on novae and cataclysmic variables?” Monthly Notices of the Royal Astronomical Society (2019): n. pag.
- Hofmann, Ralf. “SU(2) Yang-Mills thermodynamics: A priori estimate and radiative corrections.” (2018).
- Hong, Guanglei, Fan Yang and Xu Qin. “Post-Treatment Confounding in Causal Mediation Studies: A Cutting-Edge Problem and A Novel Solution via Sensitivity Analysis.” (2021).
- Hooft, Gerard ‘t. “The Black Hole Firewall Transformation and Realism in Quantum Mechanics.” Universe (2021): n. pag.
- Horawalavithana, Sameera, Clayton Gandy, Juan Arroyo Flores, John Skvoretz and Adriana Iamnitchi. “Diversity, Homophily and the Risk of Node Re-identification in Labeled Social Graphs.” COMPLEX NETWORKS (2018).
- Hou, Haopeng. “Unsupervised Domain Adaptive Person Re-id with Local-enhance and Prototype Dictionary Learning.” ArXiv abs/2201.03803 (2022): n. pag.
- Hou, Rui, Bingpeng Ma, Hong Chang, Xinqian Gu, S. Shan and Xilin Chen. “Feature Completion for Occluded Person Re-Identification.” IEEE transactions on pattern analysis and machine intelligence PP (2021): n. pag.
- Hou, Rui, Bingpeng Ma, Hong Chang, Xinqian Gu, S. Shan and Xilin Chen. “IAUnet: Global Context-Aware Feature Learning for Person Reidentification.” IEEE Transactions on Neural Networks and Learning Systems 32 (2021): 4460-4474.
- Hou, Rui, Bingpeng Ma, Hong Chang, Xinqian Gu, S. Shan and Xilin Chen. “Interaction-And-Aggregation Network for Person Re-Identification.” 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2019): 9309-9318.
- Hou, Rui, Bingpeng Ma, Hong Chang, Xinqian Gu, S. Shan and Xilin Chen. “VRSTC: Occlusion-Free Video Person Re-Identification.” 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2019): 7176-7185.
- Hou, Rui, Hong Chang, Bingpeng Ma, Rui Huang and S. Shan. “BiCnet-TKS: Learning Efficient Spatial-Temporal Representation for Video Person Re-Identification.” 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2021): 2014-2023.

- Hou, Rui, Hong Chang, Bingpeng Ma, S. Shan and Xilin Chen. “Temporal Complementary Learning for Video Person Re-Identification.” ECCV (2020).
- Hou, Yunzhong, Liang Zheng, Zhongdao Wang and Shengjin Wang. “Locality Aware Appearance Metric for Multi-Target Multi-Camera Tracking.” ArXiv abs/1911.12037 (2019): n. pag.
- Hou, Yunzhong, Zhongdao Wang, Shengjin Wang and Liang Zheng. “Adaptive Affinity for Associations in Multi-Target Multi-Camera Tracking.” IEEE Transactions on Image Processing 31 (2022): 612-622.
- Hsu, Huan-Cheng, Ching-Hang Chen, Hsiao-Rong Tyan and Hong-Yuan Mark Liao. “Hierarchical Cross Network for Person Re-identification.” ArXiv abs/1712.06820 (2017): n. pag.
- Hsu, Hung-Min, Jiarui Cai, Yizhou Wang, Jenq-Neng Hwang and Kwang-Ju Kim. “Multi-Target Multi-Camera Tracking of Vehicles Using Metadata-Aided Re-ID and Trajectory-Based Camera Link Model.” IEEE Transactions on Image Processing 30 (2021): 5198-5210.
- Hsu, Hung-Min, Yizhou Wang and Jenq-Neng Hwang. “Traffic-Aware Multi-Camera Tracking of Vehicles Based on ReID and Camera Link Model.” Proceedings of the 28th ACM International Conference on Multimedia (2020): n. pag.
- Hu, Hou-Ning, Qi-Zhi Cai, Dequan Wang, Ji Lin, Min Sun, Philipp Krähenbühl, Trevor Darrell and Fisher Yu. “Joint Monocular 3D Vehicle Detection and Tracking.” 2019 IEEE/CVF International Conference on Computer Vision (ICCV) (2019): 5389-5398.
- Hu, Hou-Ning, Yung-Hsu Yang, Tobias Fischer, Trevor Darrell, Fisher Yu and Min Sun. “Monocular Quasi-Dense 3D Object Tracking.” IEEE transactions on pattern analysis and machine intelligencePP (2022): n. pag.
- Hu, Jingchen, Terrance D. Savitsky and Matthew R. Williams. “Risk-Efficient Bayesian Data Synthesis for Privacy Protection.” Journal of Survey Statistics and Methodology (2019): n. pag.
- Hu, Panwen, Jiazhen Liu and Rui Huang. “Concentrated Multi-Grained Multi-Attention Network for Video Based Person Re-Identification.” ArXiv abs/2009.13019 (2020): n. pag.
- Hu, Ting-yao and Alexander Hauptmann. “Multi-shot Person Re-identification through Set Distance with Visual Distributional Representation.” Proceedings of the 2019 on International Conference on Multimedia Retrieval (2019): n. pag.
- Hu, Wenyi, Yuchen Jin, Xuqing Wu and Jiefu Chen. “Progressive transfer learning for low frequency data prediction in full waveform inversion.” ArXiv abs/1912.09944 (2021): n. pag.
- Hu, Zheng, Chuang Zhu and Gang He. “Hard-sample Guided Hybrid Contrast Learning for Unsupervised Person Re-Identification.” 2021 7th IEEE International Conference on Network Intelligence and Digital Content (IC-NIDC) (2021): 91-95.
- Hu, Zhijun, Yong Xu, Jie Wen, Lilei Sun and P RajaS. “Vehicle Re-identification Based on Dual Distance Center Loss.” ArXiv abs/2012.12519 (2020): n. pag.
- Hu, Zhijun, Yong Xu, Jie Wen, Xianjing Cheng, Zaijun Zhang, Lilei Sun and Yaowei Wang. “Global-Supervised Contrastive Loss and View-Aware-Based Post-Processing for Vehicle Re-Identification.” ArXiv abs/2204.07943 (2022): n. pag.
- Huang, Chu-Hsiang, Mingjie Shao, Wing-Kin Ma and Anthony Man-Cho So. “SISAL Revisited.” SIAM Journal on Imaging Sciences (2022): n. pag.

- Huang, Houjing, Wenjie Yang, Xiaotang Chen, Xin Zhao, Kaiqi Huang, Jinbin Lin, Guan Huang and Dalong Du. “EANet: Enhancing Alignment for Cross-Domain Person Re-identification.” ArXivabs/1812.11369 (2018): n. pag.
- Huang, Nianchang, Jianan Liu, Qiang Zhang and Jungong Han. “Exploring Modality-shared Appearance Features and Modality-invariant Relation Features for Cross-modality Person Re-Identification.” ArXiv abs/2104.11539 (2021): n. pag.
- Huang, Qingqiu, Wentao Liu and Dahua Lin. “Person Search in Videos with One Portrait Through Visual and Temporal Links.” ArXiv abs/1807.10510 (2018): n. pag.
- Huang, Weiquan, Yan Bai, Qiuyu Ren, Xinbo Zhao, Ming Feng and Yin Wang. “Large-Scale Unsupervised Person Re-Identification with Contrastive Learning.” ArXiv abs/2105.07914 (2021): n. pag.
- Huang, Yan, Jingsong Xu, Qiang Wu, Zhedong Zheng, Zhaoxiang Zhang and Jian Zhang. “Multi-Pseudo Regularized Label for Generated Data in Person Re-Identification.” IEEE Transactions on Image Processing 28 (2019): 1391-1403.
- Huang, Yan, Qiang Wu, Jingsong Xu and Yi Zhong. “SBSGAN: Suppression of Inter-Domain Background Shift for Person Re-Identification.” 2019 IEEE/CVF International Conference on Computer Vision (ICCV) (2019): 9526-9535.
- Huang, Yangru, Peixi Peng, Yi Jin, Junliang Xing, Congyan Lang and Songhe Feng. “Domain Adaptive Attention Model for Unsupervised Cross-Domain Person Re-Identification.” ArXivabs/1905.10529 (2019): n. pag.
- Huang, Yukun, Zhengjun Zha, Xueyang Fu, Richang Hong and Liang Li. “Real-World Person Re-Identification via Degradation Invariance Learning.” 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2020): 14072-14082.
- Huang, Zhipeng, Jiawei Liu, Liang Li, Kecheng Zheng and Zhengjun Zha. “Modality-Adaptive Mixup and Invariant Decomposition for RGB-Infrared Person Re-Identification.” ArXiv abs/2203.01735 (2022): n. pag.
- Huang, Zhipeng, Zhizheng Zhang, Cuiling Lan, Wenjun Zeng, Peng Chu, Quanzeng You, Jiang Wang, Zicheng Liu and Zhengjun Zha. “Lifelong Unsupervised Domain Adaptive Person Re-identification with Coordinated Anti-forgetting and Adaptation.” ArXiv abs/2112.06632 (2021): n. pag.
- Huang, Ziling, Zongge Wang, Chung-Chi Tsai, Shin’ichi Satoh and Chia-Wen Lin. “DotSCN: Group Re-Identification via Domain-Transferred Single and Couple Representation Learning.” IEEE Transactions on Circuits and Systems for Video Technology 31 (2021): 2739-2750.
- Hufnagel, Lorenz, Jacopo Canton, Ramis Örlü, Oana Marin, Elia Merzari and Philipp Schlatter. “The three-dimensional structure of swirl-switching in bent pipe flow.” Journal of Fluid Mechanics 835 (2017): 86 - 101.
- Huynh, Su V., Nam-Hoang Nguyen, Ngoc-Thanh Nguyen, Vinh Nguyen, Chau Huynh and Chuong H. Nguyen. “A Strong Baseline for Vehicle Re-Identification.” 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW) (2021): 4142-4149.
- Hyun, Jeongseok, Myunggu Kang, Dongyoon Wee and Dit-Yan Yeung. “Detection Recovery in Online Multi-Object Tracking with Sparse Graph Tracker.” ArXiv abs/2205.00968 (2022): n. pag.

- Ibrahim, Shibal, Natalia Ponomareva and Rahul Mazumder. “Newer is not always better: Rethinking transferability metrics, their peculiarities, stability and performance.” ArXivabs/2110.06893 (2021): n. pag.
- Iida, Kenta and Hitoshi Kiya. “An Image Identification Scheme Of Encrypted Jpeg Images For Privacy-Preserving Photo Sharing Services.” 2019 IEEE International Conference on Image Processing (ICIP) (2019): 4564-4568.
- Iida, Kenta and Hitoshi Kiya. “Robust Image Identification for Double-Compressed and Resized JPEG Images.” 2018 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC) (2018): 1968-1974.
- Iida, Kenta and Hitoshi Kiya. “Robust Image Identification for Double-Compressed JPEG Images.” 2018 International Conference on Communications (COMM) (2018): 143-146.
- Ina, Takuro, Atsushi Hashimoto, Masaaki Iiyama, Hidekazu Kasahara, Mikihiko Mori and Michihiko Minoh. “Outlier Cluster Formation in Spectral Clustering.” ArXiv abs/1703.01028 (2017): n. pag.
- Iodice, Sara and Krystian Mikolajczyk. “Partial Person Re-identification with Alignment and Hallucination.” ArXiv abs/1807.09162 (2018): n. pag.
- Iodice, Sara and Krystian Mikolajczyk. “Person Re-identification with Bias-controlled Adversarial Training.” ArXiv abs/1904.00244 (2019): n. pag.
- Iranmanesh, Seyed Mehdi, Ali Dabouei and Nasser M. Nasrabadi. “Attribute Adaptive Margin Softmax Loss using Privileged Information.” ArXiv abs/2009.01972 (2020): n. pag.
- Islam, Md. Jahidul, Jiawei Mo and Junaed Sattar. “Robot-to-Robot Relative Pose Estimation using Humans as Markers.” Auton. Robots 45 (2021): 579-593.
- Isobe, Takashi, Dong Li, Lu Tian, Weihua Chen, Yi Shan and Shengjin Wang. “Towards Discriminative Representation Learning for Unsupervised Person Re-identification.” 2021 IEEE/CVF International Conference on Computer Vision (ICCV) (2021): 8506-8516.
- Isobe, Takashi, Jian Han, Fang Zhu, Yali Li and Shengjin Wang. “Intra-Clip Aggregation For Video Person Re-Identification.” 2020 IEEE International Conference on Image Processing (ICIP) (2020): 2336-2340.
- Izutov, Evgeny. “Fast and Accurate Person Re-Identification with RMNet.” ArXiv abs/1812.02465 (2018): n. pag.
- Jacques, Julio Cezar Silveira, Xavier Baró and Sergio Escalera. “Exploiting feature representations through similarity learning, post-ranking and ranking aggregation for person re-identification.” ArXiv abs/1804.04419 (2018): n. pag.
- Jaech, Aaron, Shobhit Hathi and Mari Ostendorf. “Community Member Retrieval on Social Media Using Textual Information.” NAACL (2018).
- Jankowski, Mikolaj, Deniz Gündüz and Krystian Mikolajczyk. “Wireless Image Retrieval at the Edge.” IEEE Journal on Selected Areas in Communications 39 (2021): 89-100.
- Jha, Nikhil, Thomas Favale, Luca Vassio, Martino Trevisan and Marco Mellia. “z-anonymity: Zero-Delay Anonymization for Data Streams.” 2020 IEEE International Conference on Big Data (Big Data) (2020): 3996-4005.
- Ji, Deyi, Haoran Wang, Han Hu, Weihao Gan, Wei Wu and Junjie Yan. “Context-Aware Graph Convolution Network for Target Re-identification.” AAAI (2021).
- Ji, Zilong, Xiaolong Zou, Tiejun Huang and Si Wu. “Unsupervised Few-shot Learning via Self-supervised Training.” ArXiv abs/1912.12178 (2019): n. pag.

- Jia, Chengyou, Minnan Luo, Caixia Yan, Xiao Chang and Qinghua Zheng. “CGUA: Context-Guided and Unpaired-Assisted Weakly Supervised Person Search.” ArXiv abs/2203.14307 (2022): n. pag.
- Jia, Jieru, Qiuqi Ruan and Timothy M. Hospedales. “Frustratingly Easy Person Re-Identification: Generalizing Person Re-ID in Practice.” BMVC (2019).
- Jia, Lianjie, Chenyang Yu, Xiehao Ye, Tianyu Yan, Yinjie Lei and Pingping Zhang. “Mind Your Clever Neighbours: Unsupervised Person Re-identification via Adaptive Clustering Relationship Modeling.” ArXiv abs/2112.01839 (2021): n. pag.
- Jia, Mengxi, Xinhua Cheng, Shijian Lu and Jian Zhang. “Learning Disentangled Representation Implicitly via Transformer for Occluded Person Re-Identification.” ArXiv abs/2107.02380 (2022): n. pag.
- Jia, Mengxi, Yunpeng Zhai, Shijian Lu, Siwei Ma and Jian Zhang. “A Similarity Inference Metric for RGB-Infrared Cross-Modality Person Re-identification.” IJCAI (2020).
- Jiang, Bo, Sheng Wang, Xiao Wang and Aihua Zheng. “STADB: A Self-Thresholding Attention Guided ADB Network for Person Re-identification.” (2020).
- Jiang, Bo, Xixi Wang and Bin Luo. “PH-GCN: Person Re-identification with Part-based Hierarchical Graph Convolutional Network.” ArXiv abs/1907.08822 (2019): n. pag.
- Jiang, Bo, Xixi Wang and Jin Tang. “AttKGCN: Attribute Knowledge Graph Convolutional Network for Person Re-identification.” ArXiv abs/1911.10544 (2019): n. pag.
- Jiang, Xiang, Shikui Wei, Ruizhen Zhao, Yao Zhao and Xindong Wu. “Camera Fingerprint: A New Perspective for Identifying User’s Identity.” ArXiv abs/1610.07728 (2016): n. pag.
- Jiang, Xinyang, Yifei Gong, Xiao-Wei Guo, Q. Yang, Feiyue Huang, Weishi Zheng, Feng Zheng and Xing Sun. “Rethinking Temporal Fusion for Video-based Person Re-identification on Semantic and Time Aspect.” AAAI (2020).
- Jiang, Yiqi, Weihua Chen, Xiuyu Sun, Xiaoyu Shi, Fan Wang and Hao Li. “Exploring the Quality of GAN Generated Images for Person Re-Identification.” Proceedings of the 29th ACM International Conference on Multimedia (2021): n. pag.
- Jiao, Bingliang, Xin Tan, Jinghao Zhou, Lu Yang, Yunlong Wang and Peng Wang. “Instance and Pair-Aware Dynamic Networks for Re-Identification.” ArXiv abs/2103.05395 (2021): n. pag.
- Jiao, Wenxiang, Xing Wang, Shilin He, Irwin King, Michael R. Lyu and Zhaopeng Tu. “Data Rejuvenation: Exploiting Inactive Training Examples for Neural Machine Translation.” EMNLP(2020).
- Jin, Dapeng and Minxian Li. “Towards Fewer Labels: Support Pair Active Learning for Person Re-identification.” ArXiv abs/2204.10008 (2022): n. pag.
- Jin, Haibo, Xiaobo Wang, Shengcai Liao and S. Li. “Deep person re-identification with improved embedding and efficient training.” 2017 IEEE International Joint Conference on Biometrics (IJCB)(2017): 261-267.
- Jin, Junyang, Ye Yuan, Wei Pan, Duong L. T. Pham, Claire J. Tomlin, Alex Webb and Jorge M. Gonçalves. “On Identification of Sparse Multivariable ARX Model: A Sparse Bayesian Learning Approach.” ArXiv abs/1609.09660 (2016): n. pag.

- Jin, Xin, Cuiling Lan, Wenjun Zeng and Zhibo Chen. “Global Distance-distributions Separation for Unsupervised Person Re-identification.” ECCV (2020).
- Jin, Xin, Cuiling Lan, Wenjun Zeng and Zhibo Chen. “Uncertainty-Aware Multi-Shot Knowledge Distillation for Image-Based Object Re-Identification.” AAAI (2020).
- Jin, Xin, Cuiling Lan, Wenjun Zeng, Guoqiang Wei and Zhibo Chen. “Semantics-Aligned Representation Learning for Person Re-identification.” ArXiv abs/1905.13143 (2020): n. pag.
- Jin, Xin, Cuiling Lan, Wenjun Zeng, Zhibo Chen and Li Zhang. “Style Normalization and Restitution for Generalizable Person Re-Identification.” 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2020): 3140-3149.
- Jin, Xin, Tianyu He, Kecheng Zheng, Zhiheng Yin, Xu Shen, Zhen Huang, Ruoyu Feng, Jianqiang Huang, Xiansheng Hua and Zhibo Chen. “Cloth-Changing Person Re-identification from A Single Image with Gait Prediction and Regularization.” ArXiv abs/2103.15537 (2021): n. pag.
- Jin, Xin, Tianyu He, Zhiheng Yin, Xu Shen, Tongliang Liu, Xinchao Wang, Jianqiang Huang, Xiansheng Hua and Zhibo Chen. “Meta Clustering Learning for Large-scale Unsupervised Person Re-identification.” ArXiv abs/2111.10032 (2021): n. pag.
- Jin, Zhiping, Kenta Hotokezaka, Xiang Li, Masaomi Tanaka, Paolo D’Avanzo, Yi-Zhong Fan, Stefano Covino, Daming Wei and Tsvi Piran. “The Macronova in GRB 050709 and the GRB-macronova connection.” Nature Communications 7 (2016): n. pag.
- Johnson, Jubin, Shunsuke Yasugi, Yoichiro Sugino, Sugiri Pranata and Shengmei Shen. “Person re-identification with fusion of hand-crafted and deep pose-based body region features.” ArXivabs/1803.10630 (2018): n. pag.
- Johnston, Hunter, Carl Leake, Marcelino M. de Almeida and Daniele Mortari. “Recursive Star-Identification Algorithm Using an Adaptive Singular-Value-Decomposition-Based Angular-Velocity Estimator.” Journal of Spacecraft and Rockets (2021): n. pag.
- Jordan, Simon, Mathias Seuret, Pavel Kr’al, Ladislav Lenc, Jivr’i Mart’inek, Barbara Wiermann, Tobias Schwinger, Andreas K. Maier and Vincent Christlein. “Re-ranking for Writer Identification and Writer Retrieval.” ArXiv abs/2007.07101 (2020): n. pag.
- Jordon, James, Daniel Jarrett, Jinsung Yoon, Tavian Barnes, Paul W. G. Elbers, Patrick J. Thoral, Ari Ercole, Cui-cui Zhang, Danielle Belgrave and Mihaela van der Schaar. “Hide-and-Seek Privacy Challenge.” ArXiv abs/2007.12087 (2020): n. pag.
- Jose, Cijo and François Fleuret. “Scalable Metric Learning via Weighted Approximate Rank Component Analysis.” ECCV (2016).
- Joung, Sunghun, Seungryong Kim, Minsu Kim, Ig-Jae Kim and Kwanghoon Sohn. “Learning Canonical 3D Object Representation for Fine-Grained Recognition.” 2021 IEEE/CVF International Conference on Computer Vision (ICCV) (2021): 1015-1025.
- Jung, Jipmin, Phillip Park, Jaedong Lee, Hyein Lee, Geon-Ju Lee and Hyosoung Cha. “A Determination Scheme for Quasi-Identifiers Using Uniqueness and

Influence for De-Identification of Clinical Data." J. Medical Imaging Health Informatics 10 (2020): 295-303.
- Kalayeh, Mahdi M., Emrah Basaran, Muhittin Gokmen, Mustafa Ersel Kamasak and Mubarak Shah. "Human Semantic Parsing for Person Re-identification." 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition (2018): 1062-1071.
- Kalmukov, Y.. "Using word clouds for fast identification of papers' subject domain and reviewers' competences." ArXiv abs/2112.14861 (2021): n. pag.
- Kanaci, Aytaç, Xiatian Zhu and Shaogang Gong. "Vehicle Re-Identification in Context." GCPR(2018).
- Kang, Hao, Jianming Zhang, Haoxiang Li, Zhe L. Lin, Tj Rhodes and Bedrich Benes. "LeRoP: A Learning-Based Modular Robot Photography Framework." ArXiv abs/1911.12470 (2019): n. pag.
- Karanam, Srikrishna, Eric Lam and Richard J. Radke. "Rank Persistence: Assessing the Temporal Performance of Real-World Person Re-Identification." Proceedings of the 11th International Conference on Distributed Smart Cameras (2017): n. pag.
- Karanam, Srikrishna, Mengran Gou, Ziyan Wu, Angels Rates-Borras, Octavia I. Camps and Richard J. Radke. "A Systematic Evaluation and Benchmark for Person Re-Identification: Features, Metrics, and Datasets." IEEE Transactions on Pattern Analysis and Machine Intelligence 41 (2019): 523-536.
- Karianakis, Nikolaos, Zicheng Liu, Yinpeng Chen and Stefano Soatto. "Reinforced Temporal Attention and Split-Rate Transfer for Depth-Based Person Re-identification." ECCV (2018).
- Karmakar, Arnab and Deepak Mishra. "Pose Invariant Person Re-Identification using Robust Pose-transformation GAN." ArXiv abs/2105.00930 (2021): n. pag.
- Karras, Christos, Aristeidis Karras and Spyros Sioutas. "Pattern Recognition and Event Detection on IoT Data-streams." ArXiv abs/2203.01114 (2022): n. pag.
- Karthik, Shyamgopal, Ameya Prabhu and Vineet Gandhi. "Simple Unsupervised Multi-Object Tracking." ArXiv abs/2006.02609 (2020): n. pag.
- Kassani, Peyman Hosseinzadeh, Alexej Gossmann and Yu-ping Wang. "Multimodal Sparse Classifier for Adolescent Brain Age Prediction." IEEE Journal of Biomedical and Health Informatics 24 (2020): 336-344.
- Katnagallu, Shyam, Leigh T. Stephenson, Isabelle Mouton, Christoph Freysoldt, Aparna P. A. Subramanyam, J. Jenke, A. N. Ladines, Steffen Neumeier, Thomas Hammerschmidt, Ralf Drautz, Jörg Neugebauer, Franccois Vurpillot, Dierk Raabe and Baptiste Gault. "Imaging individual solute atoms at crystalline imperfections in metals." New Journal of Physics (2019): n. pag.
- Keetha, Nikhil Varma, Chen Wang, Yuheng Qiu, Kuan Xu and Sebastian A. Scherer. "AirObject: A Temporally Evolving Graph Embedding for Object Identification." (2021).
- Keskin, Gokce, Tyler Lee, Cory Stephenson and Oguz H. Elibol. "Many-to-Many Voice Conversion with Out-of-Dataset Speaker Support." ArXiv abs/1905.02525 (2019): n. pag.
- Khalife, Sammy and Michalis Vazirgiannis. "Scalable graph-based individual named entity identification." ArXiv abs/1811.10547 (2018): n. pag.
- Khan, Furqan Muhammad and François Bremond. "Person Re-identification for Real-world Surveillance Systems." ArXiv abs/1607.05975 (2016): n. pag.

- Khan, Sultan Daud and Habib Ullah. “A survey of advances in vision-based vehicle re-identification.” Comput. Vis. Image Underst. 182 (2019): 50-63.
- Khatun, Amena, Simon Denman, Sridha Sridharan and Clinton Fookes. “A Deep Four-Stream Siamese Convolutional Neural Network with Joint Verification and Identification Loss for Person Re-Detection.” 2018 IEEE Winter Conference on Applications of Computer Vision (WACV) (2018): 1292-1301.
- Khatun, Amena, Simon Denman, Sridha Sridharan and Clinton Fookes. “End-to-End Domain Adaptive Attention Network for Cross-Domain Person Re-Identification.” IEEE Transactions on Information Forensics and Security 16 (2021): 3803-3813.
- Khatun, Amena, Simon Denman, Sridha Sridharan and Clinton Fookes. “Pose-driven Attention-guided Image Generation for Person Re-Identification.” ArXiv abs/2104.13773 (2021): n. pag.
- Khatun, Amena, Simon Denman, Sridha Sridharan and Clinton Fookes. “Semantic Consistency and Identity Mapping Multi-Component Generative Adversarial Network for Person Re-Identification.” 2020 IEEE Winter Conference on Applications of Computer Vision (WACV) (2020): 2256-2265.
- Khazeiynasab, Seyyed Rashid and Junjian Qi. “Resilience Analysis and Cascading FailureModeling of Power Systems under Extreme Temperatures.” ArXiv abs/2009.14155 (2020): n. pag.
- Khochare, Aakash, Aravindhan K. Krishnan and Yogesh L. Simmhan. “A Scalable Platform for Distributed Object Tracking Across a Many-Camera Network.” IEEE Transactions on Parallel and Distributed Systems 32 (2021): 1479-1493.
- Khorramshahi, Pirazh, Amit Kumar, Neehar Peri, Sai Saketh Rambhatla, Jun-Cheng Chen and Rama Chellappa. “A Dual-Path Model With Adaptive Attention for Vehicle Re-Identification.” 2019 IEEE/CVF International Conference on Computer Vision (ICCV) (2019): 6131-6140.
- Khorramshahi, Pirazh, Neehar Peri, Jun-Cheng Chen and Rama Chellappa. “The Devil is in the Details: Self-Supervised Attention for Vehicle Re-Identification.” ArXiv abs/2004.06271 (2020): n. pag.
- Khorramshahi, Pirazh, Vineet Shenoy and Rama Chellappa. “Scalable Vehicle Re-Identification via Self-Supervision.” ArXiv abs/2205.07613 (2022): n. pag.
- Khorramshahi, Pirazh, Vineet Shenoy, Michael L. Pack and Rama Chellappa. “Scalable and Real-time Multi-Camera Vehicle Detection, Re-Identification, and Tracking.” ArXiv abs/2204.07442 (2022): n. pag.
- KHov’ari, Zs., A. Kunstler, Klaus G. Strassmeier, Thorsten A. Carroll, M. Weber, L. Kriskovics, Katalin Ol’ah, Krisztián Vida and Thomas Granzer. “Time-series Doppler images and surface differential rotation of the effectively-single rapidly-rotating K-giant KU Pegasi.” arXiv: Solar and Stellar Astrophysics (2016): n. pag.
- Khraimeche, Yacine, Guillaume-Alexandre Bilodeau, David Steele and Harshad Mahadik. “Unsupervised Disentanglement GAN for Domain Adaptive Person Re-Identification.” ArXivabs/2007.15560 (2020): n. pag.
- Kim, Joshua, Tongliang Liu and Kalina Yacef. “Transfer Learning in Conversational Analysis through Reusing Preprocessing Data as Supervisors.” ArXiv abs/2112.03032 (2021): n. pag.
- Kim, Youngeun, Seokeon Choi, Taeksun Kim, Sumin Lee and Changick Kim. “Learning to Align Multi-Camera Domains using Part-Aware Clustering for

Unsupervised Video Person Re-Identification." arXiv: Computer Vision and Pattern Recognition (2019): n. pag.
- Kimura, Hiroshi. "High Radiation Pressure on Interstellar Dust Computed by Light-Scattering Simulation on Fluffy Agglomerates of Magnesium-silicate Grains with Metallic-iron Inclusions." arXiv: Astrophysics of Galaxies (2017): n. pag.
- Kiran, M., Amran Bhuiyan, Louis-Antoine Blais-Morin, Mehrsan Javan, Ismail Ben Ayed and Éric Granger. "A Flow-Guided Mutual Attention Network for Video-Based Person Re-Identification." arXiv: Computer Vision and Pattern Recognition (2020): n. pag.
- Kiran, M., R Gnana Praveen, Le Thanh Nguyen-Meidine, Soufiane Belharbi, Louis-Antoine Blais-Morin and Eric Granger. "Holistic Guidance for Occluded Person Re-Identification." ArXivabs/2104.06524 (2021): n. pag.
- Klagyivik, P'eter, Hans J. Deeg, Szilárd Csizmadia, Juan Cabrera and Grzegorz Nowak. "Orbital Period Refinement of CoRoT Planets with TESS Observations." Frontiers in Astronomy and Space Sciences (2021): n. pag.
- Kochmar, Ekaterina, Sian Gooding and Matthew Shardlow. "Detecting Multiword Expression Type Helps Lexical Complexity Assessment." LREC (2020).
- Koebe, Till and Alejandra Arias-Salazar. "Releasing survey microdata with exact cluster locations and additional privacy safeguards." ArXiv abs/2205.12260 (2022): n. pag.
- Kong, Jiangtao, Yu Cheng, K. Li and Junliang Xing. "DSAM: A Distance Shrinking with Angular Marginalizing Loss for High Performance Vehicle Re-identificatio." ArXiv abs/2011.06228 (2020): n. pag.
- Kossen, Tabea, Pooja Subramaniam, Vince Istvan Madai, Anja Hennemuth, Kristian Hildebrand, Adam Hilbert, Jan Sobesky, Michelle Livne, Ivana Galinovic, Ahmed A. Khalil, Jochen B. Fiebach and Dietmar Frey. "Anonymization of labeled TOF-MRA images for brain vessel segmentation using generative adversarial networks." ArXiv abs/2009.04227 (2020): n. pag.
- Kulits, Peter, Jake Wall, Anka Bedetti, Michelle Deborah Henley and Sara Beery. "ElephantBook: A Semi-Automated Human-in-the-Loop System for Elephant Re-Identification." ACM SIGCAS Conference on Computing and Sustainable Societies (2021): n. pag.
- Kumar, Abhinav, Shantanu Sen Gupta, Vladimir Kozitsky and Sriganesh Madhvanath. "Neural Signatures for Licence Plate Re-identification." ArXiv abs/1712.00282 (2017): n. pag.
- Kumar, Devinder, Parthipan Siva, Paul Marchwica and Alexander Wong. "Fairest of Them All: Establishing a Strong Baseline for Cross-Domain Person ReID." ArXiv abs/1907.12016 (2019): n. pag.
- Kumar, Devinder, Parthipan Siva, Paul Marchwica and Alexander Wong. "Unsupervised Domain Adaptation in Person re-ID via k-Reciprocal Clustering and Large-Scale Heterogeneous Environment Synthesis." 2020 IEEE Winter Conference on Applications of Computer Vision (WACV) (2020): 2634-2643.
- Kumar, Ratnesh, Edwin Weill, Farzin Aghdasi and Parthasarathy Sriram. "Vehicle Re-identification: an Efficient Baseline Using Triplet Embedding." 2019 International Joint Conference on Neural Networks (IJCNN) (2019): 1-9.
- Kumar, S. V. Aruna, Ehsan Yaghoubi and Hugo Proença. "A Symbolic Temporal Pooling method for Video-based Person Re-Identification." ArXiv abs/2006.11416 (2020): n. pag.

- Kumar, S. V. Aruna, Ehsan Yaghoubi, Abhijit Das, B. S. Harish and Hugo Proença. "The P-DESTRE: A Fully Annotated Dataset for Pedestrian Detection, Tracking, Re-Identification and Search from Aerial Devices." ArXiv abs/2004.02782 (2020): n. pag.
- kushwaha, pradeep, Jai Sukhatme and Ravi S. Nanjundiah. "Classification of Middle Tropospheric Systems over the Arabian Sea and Western India." (2022).
- Lale, Sahin, Kamyar Azizzadenesheli, Babak Hassibi and Anima Anandkumar. "Logarithmic Regret Bound in Partially Observable Linear Dynamical Systems." ArXiv abs/2003.11227 (2020): n. pag.
- Lan, Long, Xiao Teng, Haoang Chi and Xiang Zhang. "Multi-scale Knowledge Distillation for Unsupervised Person Re-Identification." ArXiv abs/2204.09931 (2022): n. pag.
- Lan, Xu, Hangxiao Wang, Shaogang Gong and Xiatian Zhu. "Deep Reinforcement Learning Attention Selection For Person Re-Identification." arXiv: Computer Vision and Pattern Recognition(2017): n. pag.
- Lan, Xu, Xiatian Zhu and Shaogang Gong. "Universal Person Re-Identification." ArXivabs/1907.09511 (2019): n. pag.
- Lan, Yushi, Yuan Liu, Maoqing Tian, Xinchi Zhou, Xuesen Zhang, Shuai Yi and Hongsheng Li. "MagnifierNet: Towards Semantic Adversary and Fusion for Person Re-identification." arXiv: Computer Vision and Pattern Recognition (2020): n. pag.
- Langis, Karin de and Junaed Sattar. "Real-Time Multi-Diver Tracking and Re-identification for Underwater Human-Robot Collaboration." ArXiv abs/1910.09636 (2019): n. pag.
- LaRock, Timothy, Mengqiao Xu and Tina Eliassi-Rad. "A path-based approach to analyzing the global liner shipping network." EPJ Data Science 11 (2022): 1-32.
- Lavi, Bahram, Ihsan Ullah, Mehdi Fatan and Anderson Rocha. "Survey on Reliable Deep Learning-Based Person Re-Identification Models: Are We There Yet?" ArXiv abs/2005.00355 (2020): n. pag.
- Lavi, Bahram, Mehdi Fatan Serj and Ihsan Ullah. "Survey on Deep Learning Techniques for Person Re-Identification Task." ArXiv abs/1807.05284 (2018): n. pag.
- Lawen, Hussam, Avi Ben-Cohen, Matan Protter, Itamar Friedman and Lihi Zelnik-Manor. "Compact Network Training for Person ReID." Proceedings of the 2020 International Conference on Multimedia Retrieval (2020): n. pag.
- Le, Trung-Nghia, Tam V. Nguyen and Minh-Triet Tran. "Contextual Guided Segmentation Framework for Semi-supervised Video Instance Segmentation." Mach. Vis. Appl. 33 (2022): 24.
- Lee, Donghoon, Tomas Pfister and Ming-Hsuan Yang. "Inserting Videos Into Videos." 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2019): 10053-10062.
- Lee, Jinhee and Inseok Song. "Bayesian assessment of moving group membership: importance of models and prior knowledge." Monthly Notices of the Royal Astronomical Society 475 (2018): 2955-2970.
- Lee, Sangrock, Rahul, James Lukan, Tatiana Boyko, Kateryna Zelenova, Basiel Makled, Conner Parsey, Jack Norfleet and Suvranu De. "A deep learning model for burn depth classification using ultrasound imaging." Journal of the mechanical behavior of biomedical materials 125 (2021): 104930 .

- Lee, Sangrok, Eunsoo Park, Hongsuk Yi and Sang Hun Lee. “StRDAN: Synthetic-to-Real Domain Adaptation Network for Vehicle Re-Identification.” 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW) (2020): 2590-2597.
- Lee, Sangrok, Taekang Woo and Sang Hun Lee. “Multi-Attention-Based Soft Partition Network for Vehicle Re-Identification.” ArXiv abs/2104.10401 (2021): n. pag.
- Lei, Jianjun, Lijie Niu, H. Fu, Bo Peng, Qingming Huang and Chunping Hou. “Person Re-Identification by Semantic Region Representation and Topology Constraint.” IEEE Transactions on Circuits and Systems for Video Technology 29 (2019): 2453-2466.
- Leiser, David, Stefan Loehle, Stefanos Fasoulas High Enthalpy Flow Diagnostics Group, Institute of Electronic Systems, University of Stuttgart and H Germany. “Spectral Features for Re-entry Break-up Event Identification.” (2022).
- Lestyan, Szilvia, Gergely Ács, G. Biczók and Zsolt Szalay. “Extracting Vehicle Sensor Signals from CAN Logs for Driver Re-identification.” ICISSP (2019).
- Li, Da and Zhang Zhang. “Large-Scale Pedestrian Retrieval Competition.” ArXiv abs/1903.02137 (2019): n. pag.
- Li, Dangwei, Xiaotang Chen, Z. Zhang and Kaiqi Huang. “Learning Deep Context-Aware Features over Body and Latent Parts for Person Re-identification.” 2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (2017): 7398-7407.
- Li, Dangwei, Z. Zhang, Xiaotang Chen, Haibin Ling and Kaiqi Huang. “A Richly Annotated Dataset for Pedestrian Attribute Recognition.” ArXiv abs/1603.07054 (2016): n. pag.
- Li, Duo, Aojun Zhou and Anbang Yao. “HBONet: Harmonious Bottleneck on Two Orthogonal Dimensions.” 2019 IEEE/CVF International Conference on Computer Vision (ICCV) (2019): 3315-3324.
- Li, Guo Wei, Shahbaz Rezaei and Xin Liu. “User-Level Membership Inference Attack against Metric Embedding Learning.” ArXiv abs/2203.02077 (2022): n. pag.
- Li, Hanjun, Gaojie Wu and Weishi Zheng. “Combined Depth Space based Architecture Search For Person Re-identification.” 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2021): 6725-6734.
- Li, Haoran, Yang Weng, Yizheng Liao, Brian Keel and Kenneth E. Brown. “Robust Hidden Topology Identification in Distribution Systems.” ArXiv abs/1902.01365 (2019): n. pag.
- Li, Haotang, Sheng Jun Guo, Kailin Lyu, Xiao Yang, Tianchen Chen, Jianqing Zhu and Huanqiang Zeng. “A Challenging Benchmark of Anime Style Recognition.” ArXiv abs/2204.14034 (2022): n. pag.
- Li, Huadong, Yuefeng Wang, Ying Wei, Lin Wang and Lingchi Ge. “Discriminative-Region Attention and Orthogonal-View Generation Model for Vehicle Re-Identification.” ArXiv abs/2204.13323 (2022): n. pag.
- Li, Huafeng, Kaixiong Xu, Jinxing Li, Guangming Lu, Yong Xu, Zhengtao Yu and David Zhang. “Dual-Stream Reciprocal Disentanglement Learning for Domain Adaption Person Re-Identification.” ArXiv abs/2106.13929 (2021): n. pag.

- Li, Hui, Jimin Xiao, Mingjie Sun, Eng Gee Lim and Yao Zhao. “Progressive Sample Mining and Representation Learning for One-Shot Person Re-identification with Adversarial Samples.” Pattern Recognit. 110 (2021): 107614.
- Li, Hui, Meng Yang, Zhihui Lai, Weishi Zheng and Zitong Yu. “Pedestrian re-Identification Based on Tree Branch Network with Local and Global Learning.” 2019 IEEE International Conference on Multimedia and Expo (ICME) (2019): 694-699.
- Li, Jianing and Shiliang Zhang. “Joint Visual and Temporal Consistency for Unsupervised Domain Adaptive Person Re-Identification.” ECCV (2020).
- Li, Jianing, Jingdong Wang, Qi Tian, Wen Gao and Shiliang Zhang. “Global-Local Temporal Representations for Video Person Re-Identification.” 2019 IEEE/CVF International Conference on Computer Vision (ICCV) (2019): 3957-3966.
- Li, Jianing, Shiliang Zhang and Tiejun Huang. “Multi-scale 3D Convolution Network for Video Based Person Re-Identification.” AAAI (2019).
- Li, Jianing, Shiliang Zhang, Jingdong Wang, Wen Gao and Qi Tian. “LVreID: Person Re-Identification with Long Sequence Videos.” ArXiv abs/1712.07286 (2017): n. pag.
- Li, Kai, Zhengming Ding, Kunpeng Li, Yulun Zhang and Yun Raymond Fu. “Support Neighbor Loss for Person Re-Identification.” Proceedings of the 26th ACM international conference on Multimedia (2018): n. pag.
- Li, Kun, Jinsong Zhang, Yebin Liu, Yu-Kun Lai and Qionghai Dai. “PoNA: Pose-Guided Non-Local Attention for Human Pose Transfer.” IEEE Transactions on Image Processing 29 (2020): 9584-9599.
- Li, Ming, Xinming Huang and Ziming Zhang. “Self-supervised Geometric Features Discovery via Interpretable Attention for Vehicle Re-Identification and Beyond.” 2021 IEEE/CVF International Conference on Computer Vision (ICCV) (2021): 194-204.
- Li, Minghan, Tanli Zuo, Ruicheng Li, Martha White and Weishi Zheng. “Accelerating Large Scale Knowledge Distillation via Dynamic Importance Sampling.” ArXiv abs/1812.00914 (2018): n. pag.
- Li, Mingkun, Chun-Guang Li and Jun Guo. “Cluster-Guided Asymmetric Contrastive Learning for Unsupervised Person Re-Identification.” IEEE Transactions on Image Processing 31 (2022): 3606-3617.
- Li, Mingkun, Peng Xu, Xiatian Zhu and Jun Guo. “Unsupervised Long-Term Person Re-Identification with Clothes Change.” ArXiv abs/2202.03087 (2022): n. pag.
- Li, Ming-Wei, Qing-Yuan Jiang and Wu-Jun Li. “Deep Multi-Index Hashing for Person Re-Identification.” ArXiv abs/1905.10980 (2019): n. pag.
- Li, Minxian, Xiatian Zhu and Shaogang Gong. “Unsupervised Noisy Tracklet Person Re-identification.” ArXiv abs/2101.06391 (2021): n. pag.
- Li, Minxian, Xiatian Zhu and Shaogang Gong. “Unsupervised Person Re-identification by Deep Learning Tracklet Association.” ECCV (2018).
- Li, Minxian, Xiatian Zhu and Shaogang Gong. “Unsupervised Tracklet Person Re-Identification.” IEEE Transactions on Pattern Analysis and Machine Intelligence 42 (2020): 1770-1782.
- Li, Pei, Loreto Prieto, Domingo Mery and Patrick J. Flynn. “On Low-Resolution Face Recognition in the Wild: Comparisons and New Techniques.” IEEE Transactions on Information Forensics and Security 14 (2019): 2000-2012.

- Li, Peng, Jiabin Zhang, Zheng Zhu, Yanwei Li, Luyue Jiang and Guan Huang. “State-Aware Re-Identification Feature for Multi-Target Multi-Camera Tracking.” 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW) (2019): 1506-1516.
- Li, Qilei, Jiabo Huang and Shaogang Gong. “Local-Global Associative Frame Assemble in Video Re-ID.” ArXiv abs/2110.12018 (2021): n. pag.
- Li, Qilei, Jiabo Huang, Jian Hu and Shaogang Gong. “Feature-Distribution Perturbation and Calibration for Generalized Person ReID.” ArXiv abs/2205.11197 (2022): n. pag.
- Li, Qing, Xiaojiang Peng, Yu Qiao and Qi Hao. “Unsupervised Person Re-Identification with Multi-Label Learning Guided Self-Paced Clustering.” Pattern Recognit. 125 (2022): 108521.
- Li, Shuang, Sławomir Bąk, Peter Carr and Xiaogang Wang. “Diversity Regularized Spatiotemporal Attention for Video-Based Person Re-identification.” 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition (2018): 369-378.
- Li, Shuyuan, Jianguo Li, Hanlin Tang, Rui Qian and Weiyao Lin. “ATRW: A Benchmark for Amur Tiger Re-identification in the Wild.” Proceedings of the 28th ACM International Conference on Multimedia (2020): n. pag.
- Li, Shuzhao, Huimin Yu, Wei Huang and Jing Zhang. “Attributes-aided Part Detection and Refinement for Person Re-identification.” Pattern Recognit. 97 (2020): n. pag.
- Li, Tao and Chris Clifton. “Differentially Private Imaging via Latent Space Manipulation.” ArXivabs/2103.05472 (2021): n. pag.
- Li, Tao and Minsoo Choi. “DeepBlur: A Simple and Effective Method for Natural Image Obfuscation.” ArXiv abs/2104.02655 (2021): n. pag.
- Li, Tianjiao, Jun Liu, Wei Zhang, Yun Ni, Wenqian Wang and Zhiheng Li. “UAV-Human: A Large Benchmark for Human Behavior Understanding with Unmanned Aerial Vehicles.” 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2021): 16261-16270.
- Li, Toby Jia-Jun, Jingya Chen, Brandon Canfield and Brad A. Myers. “Privacy-Preserving Script Sharing in GUI-based Programming-by-Demonstration Systems.” Proceedings of the ACM on Human-Computer Interaction 4 (2020): 1 - 23.
- Li, Wei, Xiatian Zhu and Shaogang Gong. “Harmonious Attention Network for Person Re-identification.” 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition (2018): 2285-2294.
- Li, Wei, Xiatian Zhu and Shaogang Gong. “Person Re-Identification by Deep Joint Learning of Multi-Loss Classification.” ArXiv abs/1705.04724 (2017): n. pag.
- Li, Wei-Hong, Zhuowei Zhong and Weishi Zheng. “One-pass Person Re-identification by Sketch Online Discriminant Analysis.” Pattern Recognit. 93 (2019): 237-250.
- Li, Wenkang, Ke Qi, Wenbin Chen and Yicong Zhou. “Unified Batch All Triplet Loss for Visible-Infrared Person Re-identification.” 2021 International Joint Conference on Neural Networks (IJCNN) (2021): 1-8.
- Li, Wenkang, Qi Ke, Wenbin Chen and Yicong Zhou. “Bridging the Distribution Gap of Visible-Infrared Person Re-identification with Modality Batch

Normalization.” 2021 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA) (2021): 23-28.
- Li, Wenpeng, Yongli Sun, Jinjun Wang, Han Xu, Xiangru Yang and Long Cui. “Collaborative Attention Network for Person Re-identification.” Journal of Physics: Conference Series 1848 (2019): n. pag.
- Li, Wenqi, Furong Xu, Jianan Zhao, Ruobing Zheng, Cheng Zou, Meng Wang and Yuan Cheng. “HBReID: Harder Batch for Re-identification.” ArXiv abs/2112.04761 (2021): n. pag.
- Li, Xiang, Ancong Wu and Weishi Zheng. “Adversarial Open-World Person Re-Identification.” ECCV(2018).
- Li, Xiang, Chen Lin, Chuming Li, Ming Sun, Wei Wu, Junjie Yan and Wanli Ouyang. “Improving One-Shot NAS by Suppressing the Posterior Fading.” 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2020): 13833-13842.
- Li, Xiaoxiao and Chen Change Loy. “Video Object Segmentation with Joint Re-identification and Attention-Aware Mask Propagation.” ECCV (2018).
- Li, Xiaoxiao, Yuankai Qi, Zhe Wang, Kai Chen, Ziwei Liu, Jianping Shi, Ping Luo, Xiaoou Tang and Chen Change Loy. “Video Object Segmentation with Re-identification.” ArXiv abs/1708.00197 (2017): n. pag.
- Li, Xuekai, Tengfei Liang, Yi Jin, Tao Wang and Yidong Li. “Camera-aware Style Separation and Contrastive Learning for Unsupervised Person Re-identification.” ArXiv abs/2112.10089 (2021): n. pag.
- Li, Ye-jian, Guangqiang Yin, Chunhui Liu, Xiaoyu Yang and Zhiguo Wang. “Triplet Online Instance Matching Loss for Person Re-identification.” Neurocomputing 433 (2021): 10-18.
- Li, Yitian, Ruini Xue, Mengmeng Zhu, Jing Xu and Zenglin Xu. “Angular Triplet Loss-based Camera Network for ReID.” 2021 International Joint Conference on Neural Networks (IJCNN) (2021): 1-7.
- Li, Yu-Jhe, Ci-Siang Lin, Yan-Bo Lin and Y. Wang. “Cross-Dataset Person Re-Identification via Unsupervised Pose Disentanglement and Adaptation.” 2019 IEEE/CVF International Conference on Computer Vision (ICCV) (2019): 7918-7928.
- Li, Yu-Jhe, Fu-En Yang, Yen-Cheng Liu, Yu-Ying Yeh, Xiaofei Du and Y. Wang. “Adaptation and Re-identification Network: An Unsupervised Deep Transfer Learning Approach to Person Re-identification.” 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW) (2018): 285-2856.
- Li, Yu-Jhe, Yun-Chun Chen, Yen-Yu Lin and Y. Wang. “Cross-Resolution Adversarial Dual Network for Person Re-Identification and Beyond.” ArXiv abs/2002.09274 (2020): n. pag.
- Li, Yu-Jhe, Yun-Chun Chen, Yen-Yu Lin, Xiaofei Du and Y. Wang. “Recover and Identify: A Generative Dual Model for Cross-Resolution Person Re-Identification.” 2019 IEEE/CVF International Conference on Computer Vision (ICCV) (2019): 8089-8098.
- Li, Yu-Jhe, Zhengyi Luo, Xinshuo Weng and Kris M. Kitani. “Learning Shape Representations for Clothing Variations in Person Re-Identification.” ArXiv abs/2003.07340 (2020): n. pag.

- Li, Yulin, Jianfeng He, Tianzhu Zhang, Xiang Liu, Yongdong Zhang and Feng Wu. “Diverse Part Discovery: Occluded Person Re-identification with Part-Aware Transformer.” 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2021): 2897-2906.
- Li, Zhengjia and Duoqian Miao. “Sequential End-to-end Network for Efficient Person Search.” AAAI(2021).
- Li, Zhuguo, Han Shao, Nian Xue, Liang Niu and Liangliang Cao. “Progressive Learning Algorithm for Efficient Person Re- Identification.” 2020 25th International Conference on Pattern Recognition (ICPR) (2021): 16-23.
- Liang, Chang-Hui, Wanlei Zhao and Run-Qing Chen. “Dynamic Sampling for Deep Metric Learning.” Pattern Recognit. Lett. 150 (2021): 49-56.
- Liang, Chao, Zhipeng Zhang, Yi Lu, Xue Zhou, Bing Li, Xiyong Ye and Jianxiao Zou. “Rethinking the Competition Between Detection and ReID in Multiobject Tracking.” IEEE Transactions on Image Processing 31 (2022): 3182-3196.
- Liang, Jian, Yuren Cao, Chenbin Zhang, Shiyu Chang, Kun Bai and Zenglin Xu. “Additive Adversarial Learning for Unbiased Authentication.” 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2019): 11420-11429.
- Liang, Jian, Yuren Cao, Shuang Li, Bing Bai, Hao Li, Fei Wang and Kun Bai. “Domain Agnostic Learning for Unbiased Authentication.” ArXiv abs/2010.05250 (2020): n. pag.
- Liang, Tengfei, Yi Jin, Yajun Gao, Wu Liu, Songhe Feng, Tao Wang and Yidong Li. “CMTR: Cross-modality Transformer for Visible-infrared Person Re-identification.” ArXiv abs/2110.08994 (2021): n. pag.
- Liang, Wenqi, Guangcong Wang, Jianhuang Lai and Jun-Yong Zhu. “M2M-GAN: Many-to-Many Generative Adversarial Transfer Learning for Person Re-Identification.” ArXiv abs/1811.03768 (2018): n. pag.
- Liao, Shengcai and Ling Shao. “Graph Sampling Based Deep Metric Learning for Generalizable Person Re-Identification.” ArXiv abs/2104.01546 (2021): n. pag.
- Liao, Shengcai and Ling Shao. “Interpretable and Generalizable Person Re-identification with Query-Adaptive Convolution and Temporal Lifting.” ECCV (2020).
- Liao, Shengcai and Ling Shao. “TransMatcher: Deep Image Matching Through Transformers for Generalizable Person Re-identification.” NeurIPS (2021).
- Liao, Wentong, Michael Ying Yang, Ni Zhan and Bodo Rosenhahn. “Triplet-Based Deep Similarity Learning for Person Re-Identification.” 2017 IEEE International Conference on Computer Vision Workshops (ICCVW) (2017): 385-393.
- Liao, Xingyu, Lingxiao He and Zhouwang Yang. “Video-based Person Re-identification via 3D Convolutional Networks and Non-local Attention.” ACCV (2018).
- Lima, João Paulo Eufrazio de, Rafael Alves Roberto, Lucas Silva Figueiredo, Francisco Simões and Veronica Teichrieb. “Generalizable Multi-Camera 3D Pedestrian Detection.” 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW) (2021): 1232-1240.
- Lin, Ci-Siang, Yuan-Chia Cheng and Y. Wang. “Domain Generalized Person Re-Identification via Cross-Domain Episodic Learning.” 2020 25th International Conference on Pattern Recognition (ICPR) (2021): 6758-6763.

- Lin, Jianping and Hao Li. “HPILN: A feature learning framework for cross-modality person re-identification.” IET Image Process. 13 (2019): 2897-2904.
- Lin, Kewei, Juan Rojas and Yisheng Guan. “A vision-based scheme for kinematic model construction of re-configurable modular robots.” 2017 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS) (2017): 2751-2757.
- Lin, Liang, Guangrun Wang, Wangmeng Zuo, Xiangchu Feng and Lei Zhang. “Cross-Domain Visual Matching via Generalized Similarity Measure and Feature Learning.” IEEE Transactions on Pattern Analysis and Machine Intelligence 39 (2017): 1089-1102.
- Lin, Liang, Keze Wang, Deyu Meng, Wangmeng Zuo and Lei Zhang. “Active Self-Paced Learning for Cost-Effective and Progressive Face Identification.” IEEE Transactions on Pattern Analysis and Machine Intelligence 40 (2018): 7-19.
- Lin, Shan, Chang-Tsun Li and Alex Chichung Kot. “Multi-Domain Adversarial Feature Generalization for Person Re-Identification.” IEEE Transactions on Image Processing 30 (2021): 1596-1607.
- Lin, Shan, Haoliang Li, Chang-Tsun Li and Alex Chichung Kot. “Multi-task Mid-level Feature Alignment Network for Unsupervised Cross-Dataset Person Re-Identification.” ArXivabs/1807.01440 (2018): n. pag.
- Lin, Weiyao, Yang Shen, Junchi Yan, Mingliang Xu, Jianxin Wu, Jingdong Wang and Ke Lu. “Learning Correspondence Structures for Person Re-Identification.” IEEE Transactions on Image Processing 26 (2017): 2438-2453.
- Lin, Xiangtan, Pengzhen Ren, Chung-Hsing Yeh, L. Yao, A. Song and Xiaojun Chang. “Unsupervised Person Re-Identification: A Systematic Survey of Challenges and Solutions.” ArXivabs/2109.06057 (2021): n. pag.
- Lin, Yutian, Liang Zheng, Zhedong Zheng, Yu Wu and Yi Yang. “Improving Person Re-identification by Attribute and Identity Learning.” Pattern Recognit. 95 (2019): 151-161.
- Lin, Yutian, Lingxi Xie, Yu Wu, Chenggang Clarence Yan and Qi Tian. “Unsupervised Person Re-Identification via Softened Similarity Learning.” 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2020): 3387-3396.
- Ling, Yongguo, Zhun Zhong, Donglin Cao, Zhiming Luo, Yaojin Lin, Shaozi Li and N. Sebe. “Cross-Modality Earth Mover’s Distance for Visible Thermal Person Re-Identification.” ArXivabs/2203.01675 (2022): n. pag.
- Lisanti, Giuseppe, Niki Martinel, A. Bimbo and Gian Luca Foresti. “Group Re-identification via Unsupervised Transfer of Sparse Features Encoding.” 2017 IEEE International Conference on Computer Vision (ICCV) (2017): 2468-2477.
- Lisanti, Giuseppe. “0 Multi Channel-Kernel Canonical Correlation Analysis for Cross-View Person Re-Identification.” (2017).
- Liu, C., Xiaojun Chang and Yi-Dong Shen. “Unity Style Transfer for Person Re-Identification.” 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2020): 6886-6895.
- Liu, Cen, Yunbo Peng and Yue Lin. “A Technical Report for ICCV 2021 VIPriors Re-identification Challenge.” ArXiv abs/2109.15164 (2021): n. pag.
- Liu, Chih-Ting, Chih-Wei Wu, Y. Wang and Shao-Yi Chien. “Spatially and Temporally Efficient Non-local Attention Network for Video-based Person Re-Identification.” ArXiv abs/1908.01683 (2019): n. pag.

- Liu, Chih-Ting, Jun-Cheng Chen, Chu-Song Chen and Shao-Yi Chien. “Video-based Person Re-identification without Bells and Whistles.” 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW) (2021): 1491-1500.
- Liu, Chih-Ting, Man-Yu Lee, Tsai-Shien Chen and Shao-Yi Chien. “Hard Samples Rectification for Unsupervised Cross-Domain Person Re-Identification.” 2021 IEEE International Conference on Image Processing (ICIP) (2021): 429-433.
- Liu, Chih-Ting, Yu-Jhe Li, Shao-Yi Chien and Y. Wang. “Semantics-Guided Clustering with Deep Progressive Learning for Semi-Supervised Person Re-identification.” ArXiv abs/2010.01148 (2020): n. pag.
- Liu, Chong, Yuqi Zhang, Haowen Luo, Jiasheng Tang, Weihua Chen, Xianzhe Xu, F. Wang, Hao Li and Yiyan Shen. “City-Scale Multi-Camera Vehicle Tracking Guided by Crossroad Zones.” 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW) (2021): 4124-4132.
- Liu, Chuang, Han Yang, Qin Zhou and Shibao Zheng. “Subtask-dominated Transfer Learning for Long-tail Person Search.” ArXiv abs/2112.00527 (2021): n. pag.
- Liu, Chuang, Hua Yang, Qin Zhou and Shibao Zheng. “Making Person Search Enjoy the Merits of Person Re-identification.” Pattern Recognit. 127 (2022): 108654.
- Liu, Chunlei, Wenrui Ding, Yuan Hu, Baochang Zhang, Jianzhuang Liu and Guodong Guo. “GBCNs: Genetic Binary Convolutional Networks for Enhancing the Performance of 1-bit DCNNs.” ArXivabs/1911.11634 (2019): n. pag.
- Liu, Donghaisheng, Shoudong Han, Yang Chen, Chenfei Xia and Jun Zhao. “FTN: Foreground-Guided Texture-Focused Person Re-Identification.” ArXiv abs/2009.11425 (2020): n. pag.
- Liu, Fangrui and Zheng Liu. “Shuffle and Learn: Minimizing Mutual Information for Unsupervised Hashing.” ArXiv abs/2011.10239 (2020): n. pag.
- Liu, Fang-Yi and Lei Zhang. “View Confusion Feature Learning for Person Re-Identification.” 2019 IEEE/CVF International Conference on Computer Vision (ICCV) (2019): 6638-6647.
- Liu, Haijun and Jian Cheng. “Enhancing the Discriminative Feature Learning for Visible-Thermal Cross-Modality Person Re-Identification.” ArXiv abs/1907.09659 (2020): n. pag.
- Liu, Haijun and Xiaoheng Tan. “Parameter Sharing Exploration and Hetero-Center Triplet Loss for Visible-Thermal Person Re-Identification.” IEEE Transactions on Multimedia 23 (2021): 4414-4425.
- Liu, Haijun, Jian Cheng, Shiguang Wang and Wen Wang. “Attention: A Big Surprise for Cross-Domain Person Re-Identification.” ArXiv abs/1905.12830 (2019): n. pag.
- Liu, Haijun, Yanxia Chai, Xiaoheng Tan, Dong Li and Xichuan Zhou. “Strong but Simple Baseline With Dual-Granularity Triplet Loss for Visible-Thermal Person Re-Identification.” IEEE Signal Processing Letters 28 (2021): 653-657.
- Liu, Hao, Jiashi Feng, Meibin Qi, Jianguo Jiang and Shuicheng Yan. “End-to-End Comparative Attention Networks for Person Re-Identification.” IEEE Transactions on Image Processing 26 (2017): 3492-3506.

- Liu, Hao, Jingjing Wu, Jianguo Jiang, Meibin Qi and Bo Ren. “Sequence-based Person Attribute Recognition with Joint CTC-Attention Model.” ArXiv abs/1811.08115 (2018): n. pag.
- Liu, Hao, Zequn Jie, Karlekar Jayashree, Meibin Qi, Jianguo Jiang, Shuicheng Yan and Jiashi Feng. “Video-Based Person Re-Identification With Accumulative Motion Context.” IEEE Transactions on Circuits and Systems for Video Technology 28 (2018): 2788-2802.
- Liu, Haojie, Daoxun Xia, Wei Jiang and Chao Xu. “Towards Homogeneous Modality Learning and Multi-Granularity Information Exploration for Visible-Infrared Person Re-Identification.” ArXivabs/2204.04842 (2022): n. pag.
- Liu, Haojie, Shun Ma, Daoxun Xia and Shaozi Li. “SFANet: A Spectrum-aware Feature Augmentation Network for Visible-Infrared Person Re-Identification.” IEEE transactions on neural networks and learning systems PP (2021): n. pag.
- Liu, Jialun, Wenhui Li, Hongbin Pei, Ying Wang, Feng Qu, You-shan Qu and Yuhao Chen. “Identity Preserving Generative Adversarial Network for Cross-Domain Person Re-Identification.” IEEE Access 7 (2019): 114021-114032.
- Liu, Jialun, Yifan Sun, Chuchu Han, Zhaopeng Dou and Wenhui Li. “Deep Representation Learning on Long-Tailed Data: A Learnable Embedding Augmentation Perspective.” 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2020): 2967-2976.
- Liu, Jiawei, Xierong Zhu and Zhengjun Zha. “Temporal Attribute-Appearance Learning Network for Video-based Person Re-Identification.” ArXiv abs/2009.04181 (2020): n. pag.
- Liu, Jiawei, Xierong Zhu, Zhengjun Zha and Na Jiang. “Co-Saliency Spatio-Temporal Interaction Network for Person Re-Identification in Videos.” IJCAI (2020).
- Liu, Jiawei, Zhengjun Zha, Hongtao Xie, Zhiwei Xiong and Yongdong Zhang. “CA3Net: Contextual-Attentional Attribute-Appearance Network for Person Re-Identification.” Proceedings of the 26th ACM international conference on Multimedia (2018): n. pag.
- Liu, Jiawei, Zhengjun Zha, Wei Wu, Kecheng Zheng and Qibin Sun. “Spatial-Temporal Correlation and Topology Learning for Person Re-Identification in Videos.” 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2021): 4368-4377.
- Liu, Jiawei, Zhipeng Huang, Kecheng Zheng, Dong Liu, Xiaoyan Sun and Zhengjun Zha. “Adaptive Domain-Specific Normalization for Generalizable Person Re-Identification.” ArXiv abs/2105.03042 (2021): n. pag.
- Liu, Jiawei, Zhipeng Huang, Liang Li, Kecheng Zheng and Zhengjun Zha. “Debiased Batch Normalization via Gaussian Process for Generalizable Person Re-Identification.” ArXivabs/2203.01723 (2022): n. pag.
- Liu, Jie, Cheng Sun, Xiang Xu, Baomin Xu and Shuangyuan Yu. “A spatial and temporal features mixture model with body parts for video-based person re-identification.” Applied Intelligence(2019): 1-11.
- Liu, Meichen, Ke-jun Wang, Juihang Ji and Shuzhi Sam Ge. “Person image generation with semantic attention network for person re-identification.” ArXiv abs/2008.07884 (2020): n. pag.

- Liu, Qiankun, Dongdong Chen, Qi Chu, Lu Yuan, B. Liu, Lei Zhang and Nenghai Yu. “Online Multi-Object Tracking with Unsupervised Re-Identification Learning and Occlusion Estimation.” Neurocomputing 483 (2022): 333-347.
- Liu, Shiran, Zhaoqiang Guo, Yanhui Li, Chuanqi Wang, Lin Chen, Zhongbin Sun and Yuming Zhou. “An extensive empirical study of inconsistent labels in multi-version-project defect data sets.” ArXiv abs/2101.11749 (2021): n. pag.
- Liu, Tianyang, Yutian Lin and Bo Du. “Unsupervised Person Re-identification with Stochastic Training Strategy.” ArXiv abs/2108.06938 (2021): n. pag.
- Liu, Xiaobin, Shiliang Zhang, Qingming Huang and Wen Gao. “RAM: A Region-Aware Deep Model for Vehicle Re-Identification.” 2018 IEEE International Conference on Multimedia and Expo (ICME)(2018): 1-6.
- Liu, Xiaobing and Shiliang Zhang. “Domain Adaptive Person Re-Identification via Coupling Optimization.” Proceedings of the 28th ACM International Conference on Multimedia (2020): n. pag.
- Liu, Xiaobing and Shiliang Zhang. “Graph Consistency Based Mean-Teaching for Unsupervised Domain Adaptive Person Re-Identification.” IJCAI (2021).
- Liu, Xiaofeng, Zhenhua Guo, Site Li, Lingsheng Kong, Ping Jia, Jane Jia You and B. V. K. Vijaya Kumar. “Permutation-Invariant Feature Restructuring for Correlation-Aware Image Set-Based Recognition.” 2019 IEEE/CVF International Conference on Computer Vision (ICCV) (2019): 4985-4995.
- Liu, Xihui, Haiyu Zhao, Maoqing Tian, Lu Sheng, Jing Shao, Shuai Yi, Junjie Yan and Xiaogang Wang. “HydraPlus-Net: Attentive Deep Features for Pedestrian Analysis.” 2017 IEEE International Conference on Computer Vision (ICCV) (2017): 350-359.
- Liu, Xuehu, Pingping Zhang, Chenyang Yu, Huchuan Lu and Xiaoyun Yang. “Watching You: Global-guided Reciprocal Learning for Video-based Person Re-identification.” 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2021): 13329-13338.
- Liu, Xuehu, Pingping Zhang, Chenyang Yu, Huchuan Lu, Xuesheng Qian and Xiaoyun Yang. “A Video Is Worth Three Views: Trigeminal Transformers for Video-based Person Re-identification.” ArXiv abs/2104.01745 (2021): n. pag.
- Liu, Yiheng, Wen-gang Zhou, Jianzhuang Liu, Guo-Jun Qi, Qi Tian and Houqiang Li. “An End-to-End Foreground-Aware Network for Person Re-Identification.” IEEE Transactions on Image Processing30 (2021): 2060-2071.
- Liu, Yiheng, Wen-gang Zhou, Mao Xi, Sanjing Shen and Houqiang Li. “Vision Meets Wireless Positioning: Effective Person Re-identification with Recurrent Context Propagation.” Proceedings of the 28th ACM International Conference on Multimedia (2020): n. pag.
- Liu, Yiheng, Wen-gang Zhou, Qiaokang Xie and Houqiang Li. “Unsupervised Person Re-Identification with Wireless Positioning under Weak Scene Labeling.” ArXiv abs/2110.15610 (2021): n. pag.
- Liu, Yiheng, Zhenxun Yuan, Wen-gang Zhou and Houqiang Li. “Spatial and Temporal Mutual Promotion for Video-based Person Re-identification.” ArXiv abs/1812.10305 (2019): n. pag.
- Liu, Yong, Lin Shang and A. Song. “Adaptive Re-ranking of Deep Feature for Person Re-identification.” ArXiv abs/1811.08561 (2018): n. pag.

- Liu, Yongxin. “Study on Key Technologies of Transit Passengers Travel Pattern Mining and Applications based on Multiple Sources of Data.” ArXiv abs/2006.02526 (2020): n. pag.
- Liu, Yu, Junjie Yan and Wanli Ouyang. “Quality Aware Network for Set to Set Recognition.” 2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (2017): 4694-4703.
- Liu, Yuanliu, Peipei Shi, Bo Peng, He Yan, Yong Zhou, Bing Han, Yi Zheng, Chao Lin, Jianbin Jiang, Yin Fan, Tingwei Gao, Ganwen Wang, Jian Liu, Xiangju Lu and Danming Xie. “iQIYI-VID: A Large Dataset for Multi-modal Person Identification.” ArXiv abs/1811.07548 (2018): n. pag.
- Liu, Zheng, Jie Qin, Annan Li, Yunhong Wang and Luc Van Gool. “Adversarial Binary Coding for Efficient Person Re-Identification.” 2019 IEEE International Conference on Multimedia and Expo (ICME) (2019): 700-705.
- Liu, Zhipu, Lei Zhang and Yang Yang. “Hierarchical Bi-Directional Feature Perception Network for Person Re-Identification.” Proceedings of the 28th ACM International Conference on Multimedia(2020): n. pag.
- Liu, Zhizhe, Xingxing Zhang, Zhenfeng Zhu, Shuai Zheng, Yao Zhao and Jian Cheng. “Taking Modality-free Human Identification as Zero-shot Learning.” ArXiv abs/2010.00975 (2020): n. pag.
- Liu, Zimo, Jingya Wang, Shaogang Gong, Dacheng Tao and Huchuan Lu. “Deep Reinforcement Active Learning for Human-in-the-Loop Person Re-Identification.” 2019 IEEE/CVF International Conference on Computer Vision (ICCV) (2019): 6121-6130.
- Loesch, Angelique, Jaonary Rabarisoa and Romaric Audigier. “End-To-End Person Search Sequentially Trained On Aggregated Dataset.” 2019 IEEE International Conference on Image Processing (ICIP) (2019): 4574-4578.
- Lu, Chen and Balaji Jayaraman. “Interplay of Sensor Quantity, Placement and System Dimensionality on Energy Sparse Reconstruction of Fluid Flows.” (2018).
- Lu, Yan, Yue Wu, B. Liu, Tianzhu Zhang, Baopu Li, Q. Chu and Nenghai Yu. “Cross-Modality Person Re-Identification With Shared-Specific Feature Transfer.” 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2020): 13376-13386.
- Luo, Chuanchen, Yuntao Chen, Naiyan Wang and Zhaoxiang Zhang. “Spectral Feature Transformation for Person Re-Identification.” 2019 IEEE/CVF International Conference on Computer Vision (ICCV) (2019): 4975-4984.
- Luo, Hao, Wei Jiang, Youzhi Gu, Fuxu Liu, Xingyu Liao, Shenqi Lai and Jianyang Gu. “A Strong Baseline and Batch Normalization Neck for Deep Person Re-Identification.” IEEE Transactions on Multimedia 22 (2020): 2597-2609.
- Luo, Hao, Xing Fan, Chi Zhang and Wei Jiang. “STNReID: Deep Convolutional Networks With Pairwise Spatial Transformer Networks for Partial Person Re-Identification.” IEEE Transactions on Multimedia 22 (2020): 2905-2913.
- Luo, Hao, Youzhi Gu, Xingyu Liao, Shenqi Lai and Wei Jiang. “Bag of Tricks and a Strong Baseline for Deep Person Re-Identification.” 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW) (2019): 1487-1495.
- Luo, Haowen, Pichao Wang, Yi Xu, Feng Ding, Yanxin Zhou, Fan Wang, Hao Li and Rong Jin. “Self-Supervised Pre-Training for Transformer-Based Person Re-Identification.” ArXiv abs/2111.12084 (2021): n. pag.

- Luo, Haowen, Weihua Chen, Xianzhe Xu, Jianyang Gu, Yuqi Zhang, Chong Liu, Yiqi Jiang, Shuting He, F. Wang and Hao Li. “An Empirical Study of Vehicle Re-Identification on the AI City Challenge.” 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)(2021): 4090-4097.
- Luo, Shengda, Alex Po Leung, Chung Yue Hui and K. L. Li. “An investigation on the factors affecting machine learning classifications in gamma-ray astronomy.” Monthly Notices of the Royal Astronomical Society (2020): n. pag.
- Lv, Jianming and Xintong Wang. “Cross-dataset Person Re-Identification Using Similarity Preserved Generative Adversarial Networks.” KSEM (2018).
- Lv, Jianming, Weihang Chen, Qing Li and Can Yang. “Unsupervised Cross-Dataset Person Re-identification by Transfer Learning of Spatial-Temporal Patterns.” 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition (2018): 7948-7956.
- Ma, Jun, Zilong Cheng, Haiyue Zhu, Xiaocong Li, Masayoshi Tomizuka and Tong-heng Lee. “Convex Parameterization and Optimization for Robust Tracking of a Magnetically Levitated Planar Positioning System.” IEEE Transactions on Industrial Electronics 69 (2022): 3798-3809.
- Ma, Liqian, Hong Liu, Liang Hu, Can Wang and Qianru Sun. “Orientation Driven Bag of Appearances for Person Re-identification.” ArXiv abs/1605.02464 (2016): n. pag.
- Ma, Liqian, Qianru Sun, Stamatios Georgoulis, Luc Van Gool, Bernt Schiele and Mario Fritz. “Disentangled Person Image Generation.” 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition (2018): 99-108.
- Ma, Liqian, Xu Jia, Qianru Sun, Bernt Schiele, Tinne Tuytelaars and Luc Van Gool. “Pose Guided Person Image Generation.” NIPS (2017).
- Ma, Tinghuai, Mingming Yang, Huan Rong, Yurong Qian, Yuan Tian and Najla Abdulrahman Al-Nabhan. “Dual-path CNN with Max Gated block for Text-Based Person Re-identification.” Image Vis. Comput. 111 (2021): 104168.
- Ma, Xiaolong, Xiatian Zhu, Shaogang Gong, Xudong Xie, Jianming Hu, Kin-Man Lam and Yisheng Zhong. “Person Re-Identification by Unsupervised Video Matching.” Pattern Recognit. 65 (2017): 197-210.
- Ma, Zhongxing, Yifan Zhao and Jia Li. “Pose-guided Inter- and Intra-part Relational Transformer for Occluded Person Re-Identification.” Proceedings of the 29th ACM International Conference on Multimedia (2021): n. pag.
- Maddu, Suryanarayana, Bevan L. Cheeseman, Ivo F. Sbalzarini and Christian L. Müller. “Stability selection enables robust learning of partial differential equations from limited noisy data.” ArXivabs/1907.07810 (2019): n. pag.
- Maitra, Promita, Souvick Ghosh and Dipankar Das. “Authorship Verification: An Approach based on Random Forest: Notebook for PAN at CLEF 2015.” ArXiv abs/1607.08885 (2015): n. pag.
- Mak, Terrence W.K., Ferdinando Fioretto and Pascal Van Hentenryck. “Privacy-Preserving Obfuscation for Distributed Power Systems.” ArXiv abs/1910.04250 (2019): n. pag.
- Malekzadeh, M., Richard G. Clegg, Andrea Cavallaro and Hamed Haddadi. “Mobile sensor data anonymization.” Proceedings of the International Conference on Internet of Things Design and Implementation (2019): n. pag.

- Malekzadeh, M., Richard G. Clegg, Andrea Cavallaro and Hamed Haddadi. “Privacy and Utility Preserving Sensor-Data Transformations.” ArXiv abs/1911.05996 (2020): n. pag.
- Mangi, Sanam Nisar. “Multi-target tracking for video surveillance using deep affinity network: a brief review.” ArXiv abs/2110.15674 (2021): n. pag.
- Mania, Horia, Michael I. Jordan and Benjamin Recht. “Active Learning for Nonlinear System Identification with Guarantees.” J. Mach. Learn. Res. 23 (2022): 32:1-32:30.
- Mao, Chaojie, Yingming Li, Yaqing Zhang, Zhongfei Zhang and Xi Li. “Multi-Channel Pyramid Person Matching Network for Person Re-Identification.” ArXiv abs/1803.02558 (2018): n. pag.
- Mao, Chaojie, Yingming Li, Zhongfei Zhang, Yaqing Zhang and Xi Li. “Pyramid Person Matching Network for Person Re-identification.” ArXiv abs/1803.02547 (2017): n. pag.
- Mao, Shunan, Shiliang Zhang and Ming Yang. “Resolution-invariant Person Re-Identification.” ArXiv abs/1906.09748 (2019): n. pag.
- Mao, Xiao, Jiahao Cao, Dongfang Li, Xiaogang Jia and Qingfang Zheng. “Integrating Coarse Granularity Part-level Features with Supervised Global-level Features for Person Re-identification.” ArXiv abs/2010.07675 (2020): n. pag.
- Marchwica, Paul, Michael Jamieson and Parthipan Siva. “An Evaluation of Deep CNN Baselines for Scene-Independent Person Re-identification.” 2018 15th Conference on Computer and Robot Vision (CRV) (2018): 297-304.
- Margapuri, Venkat and Michael L. Neilsen. “Classification of Seeds using Domain Randomization on Self-Supervised Learning Frameworks.” 2021 IEEE Symposium Series on Computational Intelligence (SSCI) (2021): 01-08.
- Marín-Reyes, Pedro A., Javier Lorenzo-Navarro and Modesto Castrillón Santana. “Comparative study of histogram distance measures for re-identification.” ArXiv abs/1611.08134 (2016): n. pag.
- Martinel, Niki, Abir Das, Christian Micheloni and Amit K. Roy-Chowdhury. “Temporal Model Adaptation for Person Re-identification.” ECCV (2016).
- Mart’inez-Iriarte, Juli’an and Pietro Emilio Spini. “MTE with Misspecification.” (2022).
- Masood, Rahat, Wing Yan Cheng, Dinusha Vatsalan, Deepak Mishra, Hassan Jameel Asghar and Mohamed Ali Kâafar. “Privacy Preserving Release of Mobile Sensor Data.” ArXiv abs/2205.06641 (2022): n. pag.
- Masson, Hugo, Md Amran Hossen Bhuiyan, Le Thanh Nguyen-Meidine, Mehrsan Javan, Parthipan Siva, Ismail Ben Ayed and Éric Granger. “Exploiting Prunability for Person Re-identification.” (2020).
- Matiyali, Neeraj and Gaurav Sharma. “Video Person Re-Identification using Learned Clip Similarity Aggregation.” 2020 IEEE Winter Conference on Applications of Computer Vision (WACV) (2020): 2644-2653.
- Matsukawa, Tetsu, Takahiro Okabe, Einoshin Suzuki and Yoichi Sato. “Hierarchical Gaussian Descriptors with Application to Person Re-Identification.” IEEE Transactions on Pattern Analysis and Machine Intelligence 42 (2020): 2179-2194.
- Mauw, Sjouke, Yunior Ram’irez-Cruz and Rolando Trujillo-Rasua. “Preventing active re-identification attacks on social graphs via sybil subgraph obfuscation.” Knowl. Inf. Syst. 64 (2022): 1077-1100.

- Mazel, Alexander E., Izabella Stuhl and Yuri M. Suhov. “High-density hard-core model on triangular and hexagonal lattices.” arXiv: Probability (2018): n. pag.
- Mehta, Ronak R., Sourav Pal, Vikas Singh and Sathya Ravi. “Deep Unlearning via Randomized Conditionally Independent Hessians.” ArXiv abs/2204.07655 (2022): n. pag.
- Mekhazni, Djebril, Amran Bhuiyan, George S. Eskander Ekladious and Éric Granger. “Unsupervised Domain Adaptation in the Dissimilarity Space for Person Re-identification.” ECCV (2020).
- Mendelevitch, Ofer and Michael D. Lesh. “Fidelity and Privacy of Synthetic Medical Data.” ArXivabs/2101.08658 (2021): n. pag.
- Meng, Dechao, Liang Li, Xuejing Liu, Yadong Li, Shijie Yang, Zhengjun Zha, Xingyu Gao, Shuhui Wang and Qingming Huang. “Parsing-Based View-Aware Embedding Network for Vehicle Re-Identification.” 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)(2020): 7101-7110.
- Meng, Jingke, Sheng Wu and Weishi Zheng. “Weakly Supervised Person Re-Identification.” 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2019): 760-769.
- Meng, Qiang, Xinqian Gu, Xiaqing Xu and Feng Zhou. “Basket-based Softmax.” ArXivabs/2201.09308 (2022): n. pag.
- Meshky, Nima Mohammadi, Sara Iodice and Krystian Mikolajczyk. “Domain Adversarial Training for Infrared-colour Person Re-Identification.” ICDP (2019).
- Messoussi, Oumayma, Felipe G. Magalhaes, Francois Lamarre, Francis Perreault, Ibrahima Sogoba, Guillaume-Alexandre Bilodeau and Gabriela Nicolescu. “Vehicle Detection and Tracking From Surveillance Cameras in Urban Scenes.” ISVC (2021).
- Metzger, Philip T., Mark V. Sykes, Alan Stern and Kirby D. Runyon. “The reclassification of asteroids from planets to non-planets.” Icarus (2019): n. pag.
- Miah, Mehdi, Justine Pepin, Nicolas Saunier and Guillaume-Alexandre Bilodeau. “An Empirical Analysis of Visual Features for Multiple Object Tracking in Urban Scenes.” 2020 25th International Conference on Pattern Recognition (ICPR) (2021): 5595-5602.
- Miao, Yunqi, Nianchang Huang, Xiao Ma, Qiang Zhang and Jungong Han. “On Exploring Pose Estimation as an Auxiliary Learning Task for Visible-Infrared Person Re-identification.” ArXivabs/2201.03859 (2022): n. pag.
- Milgram, Michael. “Exploring Riemann’s functional equation.” Cogent Mathematics 3 (2015): n. pag.
- Ming, Zhang, Min Zhu, Xiaoyong Wei, Xiangkun Wang, Jiamin Zhu, Junlong Cheng and Yong Yang. “Deep learning-based person re-identification methods: A survey and outlook of recent works.” Image Vis. Comput. 119 (2022): 104394.
- Ming, Zhang, Yong Yang, Xiaoyong Wei, Jianrong Yan, Xiangkun Wang, Fengjie Wang and Min Zhu. “Global-Local Dynamic Feature Alignment Network for Person Re-Identification.” ArXivabs/2109.05759 (2021): n. pag.
- Minniti, Maria Vittoria, Ruben Grandia, Kevin Fäh, Farbod Farshidian and Marco Hutter. “Model Predictive Robot-Environment Interaction Control for Mobile Manipulation Tasks.” ArXivabs/2106.04202 (2021): n. pag.
- Mohana, Mohamed, Prasanalakshmi Balaji, Salem Alelyani and Mohammed Alsaqer. “Fused Deep Neural Network based Transfer Learning in Occluded Face Classification and Person re-Identification.” ArXiv abs/2205.07203 (2022): n. pag.

- Mohtaj, Salar, Fatemeh Tavakkoli and Habibollah Asghari. “PerPaDa: A Persian Paraphrase Dataset based on Implicit Crowdsourcing Data Collection.” ArXiv abs/2201.06573 (2022): n. pag.
- Mokhtar, Sonia Ben, Antoine Boutet, Pascal Felber, Marcelo Pasin, Rafael Pires and Valerio Schiavoni. “X-search: revisiting private web search using intel SGX.” Proceedings of the 18th ACM/IFIP/USENIX Middleware Conference (2017): n. pag.
- Moon, Saemi, Myeonghyeon Kim, Zhenyue Qin, Yang Liu and Dongwoo Kim. “Anonymization for Skeleton Action Recognition.” (2021).
- Moseley, Edward T., Joy T. Wu, Jonathan Welt, John Foote, Patrick D. Tyler, David W. Grant, Eric T. Carlson, Sebastian Gehrmann, Franck Dernoncourt and Leo Anthony Celi. “A Corpus for Detecting High-Context Medical Conditions in Intensive Care Patient Notes Focusing on Frequently Readmitted Patients.” LREC (2020).
- Moskvyak, Olga, Frédéric Maire, Asia O. Armstrong, Feras Dayoub and Mahsa Baktash. “Robust Re-identification of Manta Rays from Natural Markings by Learning Pose Invariant Embeddings.” 2021 Digital Image Computing: Techniques and Applications (DICTA) (2021): 1-8.
- Moskvyak, Olga, Frédéric Maire, Feras Dayoub and Mahsa Baktash. “Learning Landmark Guided Embeddings for Animal Re-identification.” 2020 IEEE Winter Applications of Computer Vision Workshops (WACVW) (2020): 12-19.
- Moskvyak, Olga, Frédéric Maire, Feras Dayoub and Mahsa Baktashmotlagh. “Going Deeper into Semi-supervised Person Re-identification.” ArXiv abs/2107.11566 (2021): n. pag.
- Moskvyak, Olga, Frédéric Maire, Feras Dayoub and Mahsa Baktashmotlagh. “Keypoint-Aligned Embeddings for Image Retrieval and Re-identification.” 2021 IEEE Winter Conference on Applications of Computer Vision (WACV) (2021): 676-685.
- Mouawad, Issa and Francesca Odone. “FasterVideo: Efficient Online Joint Object Detection And Tracking.” ICIAP (2022).
- Mozafari, Marzieh, Reza Farahbakhsh and Noël Crespi. “Hate speech detection and racial bias mitigation in social media based on BERT model.” PLoS ONE 15 (2020): n. pag.
- Munir, Asad, Chengjin Lyu, Bart Goossens, Wilfried Philips and Christian Micheloni. “Resolution based Feature Distillation for Cross Resolution Person Re-Identification.” 2021 IEEE/CVF International Conference on Computer Vision Workshops (ICCVW) (2021): 281-289.
- Munjal, Bharti, Abdul Rafey Aftab, S. Amin, Meltem Brandlmaier, Federico Tombari and Fabio Galasso. “Joint Detection and Tracking in Videos with Identification Features.” ArXivabs/2005.10905 (2020): n. pag.
- Munjal, Bharti, Fabio Galasso and S. Amin. “Knowledge Distillation for End-to-End Person Search.” ArXiv abs/1909.01058 (2019): n. pag.
- Munjal, Bharti, S. Amin and Fabio Galasso. “Class Interference Regularization.” ArXivabs/2009.02396 (2020): n. pag.
- Munjal, Bharti, S. Amin, Federico Tombari and Fabio Galasso. “Query-Guided End-To-End Person Search.” 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2019): 811-820.

- Murakami, Takao and Kenta Takahashi. “Toward Evaluating Re-identification Risks in the Local Privacy Model.” Trans. Data Priv. 14 (2021): 79-116.
- Murakami, Takao, Hiromi Arai, Koki Hamada, Takuma Hatano, Makoto Iguchi, Hiroaki Kikuchi, Atsushi Kuromasa, Hiroshi Nakagawa, Yuichi Nakamura, Kenshiro Nishiyama, Ryo Nojima, Hidenobu Oguri, Chiemi Watanabe, Akira Yamada, Takayasu Yamaguchi and Yuji Yamaoka. “Designing a Location Trace Anonymization Contest.” ArXiv abs/2107.10407 (2021): n. pag.
- Murray, Jeffrey, Afra Jahanbakhsh Mashhadi, Brent Lagesse and Michael Stiber. “Privacy Preserving Techniques Applied to CPNI Data: Analysis and Recommendations.” ArXivabs/2101.09834 (2021): n. pag.
- Nafzi, Mohamed, Michael Brauckmann and Tobias Glasmachers. “Data Augmentation and Clustering for Vehicle Make/Model Classification.” ArXiv abs/2009.06679 (2020): n. pag.
- Nafzi, Mohamed, Michael Brauckmann and Tobias Glasmachers. “Methods of the Vehicle Re-identification.” IntelliSys (2020).
- Nafzi, Mohamed, Michael Brauckmann and Tobias Glasmachers. “Vehicle Shape and Color Classification Using Convolutional Neural Network.” ArXiv abs/1905.08612 (2019): n. pag.
- Naphade, Milind R., Shuo Wang, D. Anastasiu, Zheng Tang, Ming-Ching Chang, Xiaodong Yang, Liang Zheng, Anuj Sharma, Rama Chellappa and Pranamesh Chakraborty. “The 4th AI City Challenge.” 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW) (2020): 2665-2674.
- Naphade, Milind R., Shuo Wang, D. Anastasiu, Zheng Tang, Ming-Ching Chang, Xiaodong Yang, Yue Yao, Liang Zheng, Pranamesh Chakraborty, Christian E. López, Anuj Sharma, Qi Feng, Vitaly Ablavsky and Stan Sclaroff. “The 5th AI City Challenge.” 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW) (2021): 4258-4268.
- Napolean, Yeshwanth, Priadi Teguh Wibowo and Jan C. van Gemert. “Running Event Visualization using Videos from Multiple Cameras.” ArXiv abs/1909.02835 (2019): n. pag.
- Narayan, Neeti, Nishant Sankaran, Srirangaraj Setlur and Venu Govindaraju. “CAN: Composite Appearance Network for Person Tracking and How to Model Errors in a Tracking System.” arXiv: Computer Vision and Pattern Recognition (2018): n. pag.
- Nassar, Ahmed Samy, Sébastien Lefèvre and Jan Dirk Wegner. “Simultaneous Multi-View Instance Detection With Learned Geometric Soft-Constraints.” 2019 IEEE/CVF International Conference on Computer Vision (ICCV) (2019): 6558-6567.
- Nasseri, Mohammad Hossein, Hadi Moradi, Reshad Hosseini and Mohammadreza Babaee. “Simple online and real-time tracking with occlusion handling.” ArXiv abs/2103.04147 (2021): n. pag.
- Navaneet, K. L., Ravi Kiran Sarvadevabhatla, Shashank Shekhar, R. Venkatesh Babu and Anirban Chakraborty. “Operator-in-the-Loop Deep Sequential Multi-Camera Feature Fusion for Person Re-Identification.” IEEE Transactions on Information Forensics and Security 15 (2020): 2375-2385.
- Neff, Christopher, Mat’ias Mendieta, Shrey Mohan, Mohammadreza Baharani, Samuel Rogers and Hamed Tabkhi. “REVAMP2T: Real-Time Edge Video

Analytics for Multicamera Privacy-Aware Pedestrian Tracking." IEEE Internet of Things Journal 7 (2020): 2591-2602.
- Neogi, Anupam and Nilanjan Mitra. "Body-centered phase of shock loaded Cu." arXiv: Materials Science (2016): n. pag.
- Nepovinnykh, Ekaterina A., Ilia Chelak, Tuomas Eerola and Heikki A. Kalviainen. "NORPPA: NOvel Ringed seal re-identification by Pelage Pattern Aggregation." (2022).
- Nepovinnykh, Ekaterina A., Tuomas Eerola, Vincent Biard, Piia Mutka, Marja Niemi, Heikki A. Kalviainen and Mervi Kunnasranta. "SealID: Saimaa ringed seal re-identification dataset." (2022).
- Nesterenko, D.A., Anu Kankainen, Joel Kostensalo, Chantal R. Nobs, Alison Bruce, O. Beliuskina, L. Canete, T. Eronen, E. R. Gamba, S. Geldhof, Ruben De Groote, A. Jokinen, J. Kurpeta, I. D. Moore, L. N. Morrison, Zs. Podoly'ak, Ilkka Pohjalainen, S. Rinta-Antila, A. de Roubin, M. Rudigier, Jouni Suhonen, M. Vil'en, Ville J Virtanen and Juha Heikki Aysto. "Novel Penning-trap techniques reveal isomeric states in ^{128}In and ^{130}In for the first time." arXiv: Nuclear Experiment (2020): n. pag.
- Nguyen, Binh X., Binh Nguyen, Tuong KL. Do, Erman Tjiputra, Quang D. Tran and Anh Gia-Tuan Nguyen. "Graph-based Person Signature for Person Re-Identifications." 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW) (2021): 3487-3496.
- Nguyen, Duong and Ronan Fablet. "TrAISformer-A generative transformer for AIS trajectory prediction." ArXiv abs/2109.03958 (2021): n. pag.
- Nguyen, Pha, Kha Gia Quach, Chi Nhan Duong, Ngan T. H. Le, Xuan-Bac Nguyen and Khoa Luu. "Multi-Camera Multiple 3D Object Tracking on the Move for Autonomous Vehicles." ArXivabs/2204.09151 (2022): n. pag.
- Nguyen, Thanh Tan, Ali Shameli, Yasin Abbasi-Yadkori, Anup B. Rao and Branislav Kveton. "Sample Efficient Graph-Based Optimization with Noisy Observations." AISTATS (2019).
- Nguyen-Meidine, Le Thanh, Atif Belal, M. Kiran, José Dolz, Louis-Antoine Blais-Morin and Éric Granger. "Knowledge Distillation Methods for Efficient Unsupervised Adaptation Across Multiple Domains." Image Vis. Comput. 108 (2021): 104096.
- Nguyen-Meidine, Le Thanh, Éric Granger, M. Kiran, José Dolz and Louis-Antoine Blais-Morin. "Joint Progressive Knowledge Distillation and Unsupervised Domain Adaptation." 2020 International Joint Conference on Neural Networks (IJCNN) (2020): 1-8.
- Ni, Xingyang and Esa Rahtu. "FlipReID: Closing the Gap Between Training and Inference in Person Re-Identification." 2021 9th European Workshop on Visual Information Processing (EUVIP)(2021): 1-6.
- Ni, Xingyang, Heikki Huttunen and Esa Rahtu. "On the Importance of Encrypting Deep Features." 2021 IEEE/CVF International Conference on Computer Vision Workshops (ICCVW) (2021): 4125-4132.
- Ni, Xingyang, Liang Fang and Heikki Huttunen. "Adaptive L2 Regularization in Person Re-Identification." 2020 25th International Conference on Pattern Recognition (ICPR) (2021): 9601-9607.
- Nicholson, Hamish. "Psychophysical Evaluation of Deep Re-Identification Models." ArXivabs/2005.02136 (2020): n. pag.

- Nikhal, Kshitij and Benjamin S. Riggan. “Unsupervised Attention Based Instance Discriminative Learning for Person Re-Identification.” 2021 IEEE Winter Conference on Applications of Computer Vision (WACV) (2021): 2421-2430.
- Niu, Kai, Yan Huang, Wanli Ouyang and Liang Wang. “Improving Description-Based Person Re-Identification by Multi-Granularity Image-Text Alignments.” IEEE Transactions on Image Processing 29 (2020): 5542-5556.
- Nouri, Alireza, Alireza Soroudi and Andrew Keane. “Resilient Decentralized Control of Inverter-interfaced Distributed Energy Sources in Low-voltage Distribution Grids.” ArXiv abs/1911.11420 (2019): n. pag.
- Nye, Benjamin E., Jay DeYoung, Eric P. Lehman, Ani Nenkova, Iain James Marshall and Byron C. Wallace. “Understanding Clinical Trial Reports: Extracting Medical Entities and Their Relations.” ArXiv abs/2010.03550 (2020): n. pag.
- Oh, Seong Joon, Rodrigo Benenson, Mario Fritz and Bernt Schiele. “Person Recognition in Personal Photo Collections.” IEEE Transactions on Pattern Analysis and Machine Intelligence 42 (2020): 203-220.
- Okay, Arda Efe, Manal Al Ghamdi, Robert Westendorp and Mohamed Abdel-Mottaleb. “Multi-Resolution Overlapping Stripes Network for Person Re-Identification.” ICASSP 2020 - 2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (2020): 3652-3656.
- Oliveira, Icaro Oliveira de, Keiko Verônica Ono Fonseca and Rodrigo Minetto. “A Two-Stream Siamese Neural Network for Vehicle Re-Identification by Using Non-Overlapping Cameras.” 2019 IEEE International Conference on Image Processing (ICIP) (2019): 669-673.
- Ooi, Hui-Lee, Guillaume-Alexandre Bilodeau and Nicolas Saunier. “Supervised and Unsupervised Detections for Multiple Object Tracking in Traffic Scenes: A Comparative Study.” ArXivabs/2003.13644 (2020): n. pag.
- Organisciak, Daniel, Brian K. S. Isaac-Medina, Matt Poyser, Shanfeng Hu, T. Breckon and Hubert P. H. Shum. “UAV-ReID: A Benchmark on Unmanned Aerial Vehicle Re-identification.” VISIGRAPP(2022).
- Ororbia, Alexander, Fridolin Linder and Joshua Snoke. “Using Neural Generative Models to Release Synthetic Twitter Corpora with Reduced Stylometric Identifiability of Users.” arXiv: Computation and Language (2016): n. pag.
- Ospici, Matthieu and Antoine Cecchi. “Person re-identification across different datasets with multi-task learning.” ArXiv abs/1807.09666 (2018): n. pag.
- Packhäuser, Kai, Sebastian Gündel, Nicolas Münster, Christopher Syben, Vincent Christlein and Andreas K. Maier. “Is Medical Chest X-ray Data Anonymous?” ArXiv abs/2103.08562 (2021): n. pag.
- Paik, Chong-Dae and Hyunwoo J. Kim. “Improving Object Detection, Multi-object Tracking, and Re-Identification for Disaster Response Drones.” ArXiv abs/2201.01494 (2022): n. pag.
- Paisitkriangkrai, Sakrapee, Lin Wu, Chunhua Shen and Anton van den Hengel. “Structured learning of metric ensembles with application to person re-identification.” Comput. Vis. Image Underst.156 (2017): 51-65.
- Pan, Chuanyu, Yanchao Yang, Kaichun Mo, Yueqi Duan and Leonidas J. Guibas. “Object Pursuit: Building a Space of Objects via Discriminative Weight Generation.” ArXiv abs/2112.07954 (2021): n. pag.

- Panda, Pranoy and Martin Barczyk. “Blending of Learning-based Tracking and Object Detection for Monocular Camera-based Target Following.” ArXiv abs/2008.09644 (2020): n. pag.
- Panda, Rameswar, Amran Bhuiyan, Vittorio Murino and Amit K. Roy-Chowdhury. “Unsupervised Adaptive Re-identification in Open World Dynamic Camera Networks.” 2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (2017): 1377-1386.
- Pang, Bo, Deming Zhai, Junjun Jiang and Xianming Liu. “Fully Unsupervised Person Re-Identification via Selective Contrastive Learning.” ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM) 18 (2022): 1 - 15.
- Pang, Jian, Dacheng Zhang, Huafeng Li, Weifeng Liu and Zhengtao Yu. “Hazy Re-ID: An Interference Suppression Model for Domain Adaptation Person Re-Identification Under Inclement Weather Condition.” 2021 IEEE International Conference on Multimedia and Expo (ICME) (2021): 1-6.
- Pappalardo, Luca, Filippo Simini, Gianni Barlacchi and Roberto Pellungrini. “scikit-mobility: a Python library for the analysis, generation and risk assessment of mobility data.” arXiv: Physics and Society (2019): n. pag.
- Parameshwarappa, Pooja, Zhiyuan Chen and Günes Koru. “A Multi-level Clustering Approach for Anonymizing Large-Scale Physical Activity Data.” ArXiv abs/1908.07976 (2019): n. pag.
- Park, Hyunjong and Bumsub Ham. “Relation Network for Person Re-identification.” AAAI (2020).
- Park, Hyunjong, Sanghoon Lee, Junghyup Lee and Bumsub Ham. “Learning by Aligning: Visible-Infrared Person Re-identification using Cross-Modal Correspondences.” 2021 IEEE/CVF International Conference on Computer Vision (ICCV) (2021): 12026-12035.
- Pathak, P.. “Fine-Grained Re-Identification.” ArXiv abs/2011.13475 (2020): n. pag.
- Patro, Jasabanta, Bidisha Samanta, Saurabh Singh, Aparna Basu, Prithwish Mukherjee, Monojit Choudhury and Animesh Mukherjee. “All that is English may be Hindi: Enhancing language identification through automatic ranking of the likeliness of word borrowing in social media.” EMNLP (2017).
- Peng, Haoran, He Huang, Li Xu, Tianjiao Li, J. Liu, Hossein Rahmani, Qiuhong Ke, Zhicheng Guo, Cong Wu, Rongchang Li, Mang Ye, Jiahao Wang, Jiaxu Zhang, Yuanzhong Liu, Tao He, Fuwei Zhang, Xianbin Liu and Tao Lin. “The Multi-Modal Video Reasoning and Analyzing Competition.” 2021 IEEE/CVF International Conference on Computer Vision Workshops (ICCVW) (2021): 806-813.
- Peng, Jinjia, Guangqi Jiang, Dongyan Chen, Tongtong Zhao, Huibing Wang and Xianping Fu. “Eliminating cross-camera bias for vehicle re-identification.” ArXiv abs/1912.10193 (2019): n. pag.
- Peng, Jinjia, Huibing Wang and Xianping Fu. “Cross Domain Knowledge Learning with Dual-branch Adversarial Network for Vehicle Re-identification.” ArXiv abs/1905.00006 (2020): n. pag.
- Peng, Jinjia, Huibing Wang, Tongtong Zhao and Xianping Fu. “Cross Domain Knowledge Transfer for Unsupervised Vehicle Re-Identification.” 2019 IEEE

International Conference on Multimedia & Expo Workshops (ICMEW) (2019): 453-458.
- Peng, Jinjia, Yang Wang, Huibing Wang, Zhao Zhang, Xianping Fu and Meng Wang. “Unsupervised Vehicle Re-identification with Progressive Adaptation.” ArXiv abs/2006.11486 (2020): n. pag.
- Peng, Xiongfeng, Zhihua Liu, Qiang Wang, Yun Tae Kim and Myungjae Jeon. “Accurate Visual-Inertial SLAM by Feature Re-identification.” 2021 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS) (2021): 9168-9175.
- Peng, Yang, Ping Liu, Yawei Luo, Pan Zhou, Zichuan Xu and Jingen Liu. “Unsupervised Domain Adaptive Person Re-Identification via Human Learning Imitation.” ArXiv abs/2111.14014 (2021): n. pag.
- Pereira, Rodolfo Miranda, Diego Bertolini, Lucas O. Teixeira, Carlos Nascimento Silla and Yandre M. G. Costa. “COVID-19 identification in chest X-ray images on flat and hierarchical classification scenarios.” Computer Methods and Programs in Biomedicine 194 (2020): 105532 - 105532.
- Pereira, Tiago de C. G. and Teófilo Emídio de Campos. “Domain Adaptation for Person Re-identification on New Unlabeled Data.” ArXiv abs/2106.15693 (2020): n. pag.
- Pereira, Tiago de C. G. and Teófilo Emídio de Campos. “Learn by Guessing: Multi-Step Pseudo-Label Refinement for Person Re-Identification.” VISIGRAPP (2022).
- Petrova, Elena, Tatiana Podladchikova, Astrid M. Veronig, Stijn Lemmens, Benjamin Bastida Virgili and Tim Flohrer. “Medium-term Predictions of F10.7 and F30 cm Solar Radio Flux with the Adaptive Kalman Filter.” The Astrophysical Journal Supplement Series 254 (2021): n. pag.
- Pfeiffer, Kilian Y., Alexander Hermans, I. Sárándi, Mark Weber and B. Leibe. “Visual Person Understanding through Multi-Task and Multi-Dataset Learning.” ArXiv abs/1906.03019 (2019): n. pag.
- Phan, Hai T. and Anh M Nguyen. “DeepFace-EMD: Re-ranking Using Patch-wise Earth Mover’s Distance Improves Out-Of-Distribution Face Identification.” ArXiv abs/2112.04016 (2021): n. pag.
- Pichara, Karim, Pavlos Protopapas and Daniel Le’on. “Meta-classification for Variable Stars.” The Astrophysical Journal 819 (2016): 18.
- Pillai, Sudeep and John J. Leonard. “Self-Supervised Visual Place Recognition Learning in Mobile Robots.” ArXiv abs/1905.04453 (2019): n. pag.
- Pires, Rafael, David Goltzsche, Sonia Ben Mokhtar, Sara Bouchenak, Antoine Boutet, Pascal Felber, Rüdiger Kapitza, Marcelo Pasin and Valerio Schiavoni. “CYCLOSA: Decentralizing Private Web Search through SGX-Based Browser Extensions.” 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS) (2018): 467-477.
- Pires, Rafael. “Distributed systems and trusted execution environments: Trade-offs and challenges.” ArXiv abs/2001.09670 (2020): n. pag.
- Ponce-López, Víctor, Tilo Burghardt, Sion L. Hannuna, Dima Damen, Alessandro Masullo and Majid Mirmehdi. “Semantically Selective Augmentation for Deep Compact Person Re-Identification.” ArXiv abs/1806.04074 (2018): n. pag.
- Poncyljusz, Bo.zena, Tomasz Bulik, Niraj Dhital, Oleksandr Sushchov, Sławomir Stuglik, Piotr Homola, David E. Alvarez-Castillo, Marcin Piekarczyk, Tadeusz Wibig, Jaroslaw Stasielak, P’eter Kov’acs, Katarzyna Smelcerz, Maria Rodriguez

Frias, Michal Nied'zwiecki, Justyna Miszczyk, Tomasz So'snicki, Lukasz Bibrzycki, Arman Tursunov, Luis del Peral and Krzysztof Rzecki. "Simulation of the isotropic ultra-high energy photons flux in the solar magnetic field." (2022).

- Porrello, Angelo, Luca Bergamini and Simone Calderara. "Robust Re-Identification by Multiple Views Knowledge Distillation." ArXiv abs/2007.04174 (2020): n. pag.
- Porter, Troy A., Gavin Rowell, G Jóhannesson and Igor V. Moskalenko. "Galactic PeVatrons and helping to find them: Effects of galactic absorption on the observed spectra of very high energy γ-ray sources." Physical review. D. 98 4 (2018): n. pag.
- Potapov, Alexey, Sergey Rodionov, Hugo Latapie and Enzo Fenoglio. "Metric Embedding Autoencoders for Unsupervised Cross-Dataset Transfer Learning." ICANN (2018).
- Prasad, Saurabh, Tanu Priya, Minshan Cui and S. Shah. "Person Re-identification with Hyperspectral Multi-Camera Systems --- A Pilot Study." arXiv: Computer Vision and Pattern Recognition (2016): n. pag.
- Prates, Raphael C. and William Robson Schwartz. "Kernel Cross-View Collaborative Representation based Classification for Person Re-Identification." J. Vis. Commun. Image Represent. 58 (2019): 304-315.
- Psarros, Georgios N., Pantelis A. Dratsas and Stavros A. Papathanassiou. "A comparison between central- and self-dispatch storage management principles in island systems." ArXivabs/2105.13458 (2021): n. pag.
- Pu, Nan, Wei Chen, Yu Liu, Erwin M. Bakker and Michael S. Lew. "Dual Gaussian-based Variational Subspace Disentanglement for Visible-Infrared Person Re-Identification." Proceedings of the 28th ACM International Conference on Multimedia (2020): n. pag.
- Pu, Nan, Wei Chen, Yu Liu, Erwin M. Bakker and Michael S. Lew. "Lifelong Person Re-Identification via Adaptive Knowledge Accumulation." 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2021): 7897-7906.
- Pullen, Anthony R., Christopher M. Hirata, Olivier Doré and Alvise Raccanelli. "Interloper bias in future large-scale structure surveys." arXiv: Cosmology and Nongalactic Astrophysics (2015): n. pag.
- Qi, Fengliang, Bo Yan, Leilei Cao and Hongbin Wang. "Stronger Baseline for Person Re-Identification." ArXiv abs/2112.01059 (2021): n. pag.
- Qi, Lei, Jiayi Shen, Jiaqi Liu, Yinghuan Shi and Xin Geng. "Label Distribution Learning for Generalizable Multi-source Person Re-identification." ArXiv abs/2204.05903 (2022): n. pag.
- Qi, Lei, Jing Huo, Lei Wang, Yinghuan Shi and Yang Gao. "MaskReID: A Mask Based Deep Ranking Neural Network for Person Re-identification." ArXiv abs/1804.03864 (2018): n. pag.
- Qi, Lei, Lei Wang, Jing Huo, Luping Zhou, Yinghuan Shi and Yang Gao. "A Novel Unsupervised Camera-Aware Domain Adaptation Framework for Person Re-Identification." 2019 IEEE/CVF International Conference on Computer Vision (ICCV) (2019): 8079-8088.
- Qi, Lei, Lei Wang, Jing Huo, Yinghuan Shi and Yang Gao. "Adversarial Camera Alignment Network for Unsupervised Cross-Camera Person Re-Identification." IEEE Transactions on Circuits and Systems for Video Technology 32 (2022): 2921-2936.

- Qi, Lei, Lei Wang, Jing Huo, Yinghuan Shi and Yang Gao. “GreyReID: A Two-stream Deep Framework with RGB-grey Information for Person Re-identification.” ArXiv abs/1908.05142 (2019): n. pag.
- Qi, Lei, Lei Wang, Jing Huo, Yinghuan Shi and Yang Gao. “Progressive Cross-Camera Soft-Label Learning for Semi-Supervised Person Re-Identification.” IEEE Transactions on Circuits and Systems for Video Technology 30 (2020): 2815-2829.
- Qi, Lei, Lei Wang, Yinghuan Shi and Xing-xiao Geng. “A Novel Mix-normalization Method for Generalizable Multi-source Person Re-identification.” ArXiv abs/2201.09846 (2022): n. pag.
- Qi, Lei, Lei Wang, Yinghuan Shi and Xing-xiao Geng. “Unsupervised Domain Generalization for Person Re-identification: A Domain-specific Adaptive Framework.” ArXiv abs/2111.15077 (2021): n. pag.
- Qian, Jingjing, Wei Jiang, Hao Luo and Hongyan Yu. “Stripe-based and Attribute-aware Network: A Two-Branch Deep Model for Vehicle Re-identification.” ArXiv abs/1910.05549 (2019): n. pag.
- Qian, Xuelin, Wenxuan Wang, Li Zhang, Fangrui Zhu, Yanwei Fu, Tao Xiang, Yu-Gang Jiang and X. Xue. “Long-Term Cloth-Changing Person Re-identification.” ArXiv abs/2005.12633 (2020): n. pag.
- Qian, Xuelin, Yanwei Fu, Tao Xiang, Wenxuan Wang, Jie Qiu, Yang Wu, Yu-Gang Jiang and X. Xue. “Pose-Normalized Image Generation for Person Re-identification.” ECCV (2018).
- Qian, Xuelin, Yanwei Fu, Yu-Gang Jiang, Tao Xiang and X. Xue. “Multi-scale Deep Learning Architectures for Person Re-identification.” 2017 IEEE International Conference on Computer Vision (ICCV) (2017): 5409-5418.
- Qian, Yaguan and Anlin Sun. “Person Re-identification based on Robust Features in Open-world.” ArXiv abs/2102.10798 (2021): n. pag.
- Qiu, Tairu, Guanxian Chen, Zhongang Qi, Bin Li, Ying Shan and X. Xue. “A Generic Object Re-identification System for Short Videos.” ArXiv abs/2102.05275 (2021): n. pag.
- Quade, Markus, Markus Abel, J. Nathan Kutz and Steven L. Brunton. “Sparse identification of nonlinear dynamics for rapid model recovery.” Chaos 28 6 (2018): 063116 .
- Quan, Ruijie, Xuanyi Dong, Yuehua Wu, Linchao Zhu and Yi Yang. “Auto-ReID: Searching for a Part-Aware ConvNet for Person Re-Identification.” 2019 IEEE/CVF International Conference on Computer Vision (ICCV) (2019): 3749-3758.
- Quispe, Rodolfo and Hélio Pedrini. “Improved Person Re-Identification Based on Saliency and Semantic Parsing with Deep Neural Network Models.” ArXiv abs/1807.05618 (2019): n. pag.
- Quispe, Rodolfo and Hélio Pedrini. “Top-DB-Net: Top DropBlock for Activation Enhancement in Person Re-Identification.” 2020 25th International Conference on Pattern Recognition (ICPR)(2021): 2980-2987.
- Quispe, Rodolfo, Cuiling Lan, Wenjun Zeng and Hélio Pedrini. “AttributeNet: Attribute Enhanced Vehicle Re-Identification.” Neurocomputing 465 (2021): 84-92.
- Rafael-Palou, Xavier, Anton Aubanell, Ilaria Bonavita, Mario Ceresa, Gemma Piella, Vicent J. Ribas and Miguel Ángel González Ballester. “Re-Identification and

Growth Detection of Pulmonary Nodules without Image Registration Using 3D Siamese Neural Networks." Medical image analysis67 (2021): 101823 .
- Rahimpour, Alireza and Hairong Qi. "Attention-based Few-Shot Person Re-identification Using Meta Learning." ArXiv abs/1806.09613 (2018): n. pag.
- Rahimpour, Alireza, L. Liu, Ali Taalimi, Yang Song and Hairong Qi. "Person re-identification using visual attention." 2017 IEEE International Conference on Image Processing (ICIP) (2017): 4242-4246.
- Rahman, Tanzila, Mrigank Rochan and Yang Wang. "Convolutional Temporal Attention Model for Video-Based Person Re-Identification." 2019 IEEE International Conference on Multimedia and Expo (ICME) (2019): 1102-1107.
- Rahul, Rohit, Shubham Paliwal, Monika Sharma and Lovekesh Vig. "Automatic Information Extraction from Piping and Instrumentation Diagrams." ICPRAM (2019).
- Rajput, Pranjal Singh, Yeshwanth Napolean and Jan C. van Gemert. "Heuristics2Annotate: Efficient Annotation of Large-Scale Marathon Dataset For Bounding Box Regression." ArXivabs/2104.02749 (2021): n. pag.
- Rami, Hamza, Matthieu Ospici and Stéphane Lathuilière. "Online Unsupervised Domain Adaptation for Person Re-identification." ArXiv abs/2205.04383 (2022): n. pag.
- Ramirez, Wilmer Ariza, Zhi Quan Leong, Hung Duc Nguyen and Shantha Gamini Jayasinghe. "Exploration of the Applicability of Probabilistic Inference for Learning Control in Underactuated Autonomous Underwater Vehicles." ArXiv abs/1912.11584 (2020): n. pag.
- Rangnekar, Aneesh, Nilay Mokashi, Emmett Ientilucci, Christopher Kanan and Matthew J. Hoffman. "AeroRIT: A New Scene for Hyperspectral Image Analysis." IEEE Transactions on Geoscience and Remote Sensing 58 (2020): 8116-8124.
- Rao, Haocong and Chunyan Miao. "SimMC: Simple Masked Contrastive Learning of Skeleton Representations for Unsupervised Person Re-Identification." ArXiv abs/2204.09826 (2022): n. pag.
- Rao, Haocong, Shihao Xu, Xiping Hu, Jun Cheng and B. Hu. "Multi-Level Graph Encoding with Structural-Collaborative Relation Learning for Skeleton-Based Person Re-Identification." ArXivabs/2106.03069 (2021): n. pag.
- Rao, Haocong, Siqi Wang, Xiping Hu, Mingkui Tan, Huang Da, Jun Cheng and Bin Hu. "Self-Supervised Gait Encoding with Locality-Aware Attention for Person Re-Identification." ArXivabs/2008.09435 (2020): n. pag.
- Rao, Haocong, Siqi Wang, Xiping Hu, Mingkui Tan, Yi Guo, Jun Cheng, Bin Hu and Xinwang Liu. "A Self-Supervised Gait Encoding Approach with Locality-Awareness for 3D Skeleton Based Person Re-Identification." IEEE transactions on pattern analysis and machine intelligence PP (2021): n. pag.
- Rao, Haocong, Xiping Hu, Jun Cheng and Bin Hu. "SM-SGE: A Self-Supervised Multi-Scale Skeleton Graph Encoding Framework for Person Re-Identification." Proceedings of the 29th ACM International Conference on Multimedia (2021): n. pag.
- Rao, Shivansh, Tanzila Rahman, Mrigank Rochan and Yang Wang. "Video-based Person Re-identification Using Spatial-Temporal Attention Networks." ArXiv abs/1810.11261 (2018): n. pag.

- Rao, Yongming, Guangyi Chen, Jiwen Lu and Jie Zhou. “Counterfactual Attention Learning for Fine-Grained Visual Categorization and Re-identification.” 2021 IEEE/CVF International Conference on Computer Vision (ICCV) (2021): 1005-1014.
- Rapko, Kenneth, Wanlin Xie and Andrew Walsh. “MONCE Tracking Metrics: a comprehensive quantitative performance evaluation methodology for object tracking.” ArXiv abs/2204.05280 (2022): n. pag.
- Rasoulzadeh, Shervin and Bagher BabaAli. “Writer Identification and Writer Retrieval Based on NetVLAD with Re-ranking.” IET Biom. 11 (2022): 10-22.
- Raychaudhuri, Dripta S. and Amit K. Roy-Chowdhury. “Exploiting Temporal Coherence for Self-Supervised One-shot Video Re-identification.” ECCV (2020).
- Reggiani, Lino and Eleonora Alfinito. “Fluctuation Dissipation Theorem and Electrical Noise Revisited.” Fluctuation and Noise Letters (2019): n. pag.
- Remeli, Mina, Szilvia Lestyan, Gergely Ács and G. Biczók. “Automatic Driver Identification from In-Vehicle Network Logs.” 2019 IEEE Intelligent Transportation Systems Conference (ITSC) (2019): 1150-1157.
- Remigereau, F’elix, Djebril Mekhazni, Sajjad Abdoli, Le Thanh Nguyen-Meidine, Rafael M. O. Cruz and Éric Granger. “Knowledge Distillation for Multi-Target Domain Adaptation in Real-Time Person Re-Identification.” ArXiv abs/2205.06237 (2022): n. pag.
- Ren, Chuan-Xian, Bo-Hua Liang and Zhen Lei. “Domain Adaptive Person Re-Identification via Camera Style Generation and Label Propagation.” IEEE Transactions on Information Forensics and Security 15 (2020): 1290-1302.
- Ren, Hanchi, Jingjing Deng and Xianghua Xie. “GRNN: Generative Regression Neural Network - A Data Leakage Attack for Federated Learning.” ACM Transactions on Intelligent Systems and Technology (TIST) (2022): n. pag.
- Ren, Jiawei, Xiao Ma, Chen Xu, Haiyu Zhao and Shuai Yi. “HAVANA: Hierarchical and Variation-Normalized Autoencoder for Person Re-identification.” ArXiv abs/2101.02568 (2021): n. pag.
- Ren, Min, Lingxiao He, Xingyu Liao, Wu Liu, Yunlong Wang and Tieniu Tan. “Learning Instance-level Spatial-Temporal Patterns for Person Re-identification.” 2021 IEEE/CVF International Conference on Computer Vision (ICCV) (2021): 14910-14919.
- Ren, Pengyuan and Jianmin Li. “Factorized Distillation: Training Holistic Person Re-identification Model by Distilling an Ensemble of Partial ReID Models.” ArXiv abs/1811.08073 (2018): n. pag.
- Riseley, Christopher J, A. M. M. Scaife, Michael W. Wise and Alex O. Clarke. “Diffuse radio emission in MACS J0025.4$-$1222: the effect of a major merger on bulk separation of ICM components.” arXiv: Cosmology and Nongalactic Astrophysics (2016): n. pag.
- Ristani, Ergys and Carlo Tomasi. “Features for Multi-target Multi-camera Tracking and Re-identification.” 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition (2018): 6036-6046.
- Ro, Youngmin, Jongwon Choi, Dae Ung Jo, Byeongho Heo, Jongin Lim and Jin Young Choi. “Backbone Can Not be Trained at Once: Rolling Back to Pre-trained Network for Person Re-Identification.” AAAI (2019).

- Robert, Martine, Patrick Dallaire and Philippe Giguère. “Tree bark re-identification using a deep-learning feature descriptor.” 2020 17th Conference on Computer and Robot Vision (CRV) (2020): 25-32.
- Rodenbeck, Kai, René Heller and Laurent Gizon. “Exomoon indicators in high-precision transit light curves.” Astronomy & Astrophysics (2020): n. pag.
- Rodionov, Sergey, Alexey Potapov, Hugo Latapie, Enzo Fenoglio and Maxim Peterson. “Improving Deep Models of Person Re-identification for Cross-Dataset Usage.” AIAI (2018).
- Roffo, Giorgio. “Ranking to Learn and Learning to Rank: On the Role of Ranking in Pattern Recognition Applications.” ArXiv abs/1706.05933 (2017): n. pag.
- Romanini, Daniele, Sune Lehmann and Mikko Kivelä. “Privacy and uniqueness of neighborhoods in social networks.” Scientific Reports 11 (2021): n. pag.
- Roman-Jimenez, Geoffrey, Patrice Guyot, Thierry Malon, Sylvie Chambon, Vincent Charvillat, Alain Crouzil, André Péninou, Julien Pinquier, Florence Sèdes and Christine Sénac. “Improving Vehicle Re-Identification using CNN Latent Spaces: Metrics Comparison and Track-to-track Extension.” IET Comput. Vis. 15 (2021): 85-98.
- Rosenbush, Alexander E.. “Review of light curves of novae in the modified scales. III. V1047 Cen at 2019.” arXiv: Solar and Stellar Astrophysics (2020): n. pag.
- Ruiz, Idoia, Bogdan Raducanu, Rakesh Mehta and Jaume Amores. “Optimizing Speed/Accuracy Trade-Off for Person Re-identification via Knowledge Distillation.” Eng. Appl. Artif. Intell. 87 (2020): n. pag.
- Saito, Yuki, Takuma Nakamura, Hirotaka Hachiya and Kenji Fukumizu. “Exchangeable Deep Neural Networks for Set-to-Set Matching and Learning.” ECCV (2020).
- Sakic, Ermin, Nemanja Đerić and Wolfgang Kellerer. “MORPH: An Adaptive Framework for Efficient and Byzantine Fault-Tolerant SDN Control Plane.” IEEE Journal on Selected Areas in Communications 36 (2018): 2158-2174.
- Sanakoyeu, Artsiom, Pingchuan Ma, Vadim Tschernezki and Björn Ommer. “Improving Deep Metric Learning by Divide and Conquer.” IEEE transactions on pattern analysis and machine intelligence PP (2021): n. pag.
- Sanakoyeu, Artsiom, Vadim Tschernezki, Uta Büchler and Björn Ommer. “Divide and Conquer the Embedding Space for Metric Learning.” 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2019): 471-480.
- Sarfraz, M. Saquib, Arne Schumann, Andreas Eberle and Rainer Stiefelhagen. “A Pose-Sensitive Embedding for Person Re-identification with Expanded Cross Neighborhood Re-ranking.” 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition (2018): 420-429.
- Schaefer, Erik, Nhien-An Le-Khac and M. Scanlon. “Integration of Ether Unpacker into Ragpicker for plugin-based Malware Analysis and Identification.” ArXiv abs/1708.01731 (2017): n. pag.
- Schipani, Pietro, M. Gonzalez, F. Perrotta, Salvatore Savarese, Mirko Colapietro, Adriano Ghedina, Marcos Hernandez Diaz and H. Perez Ventura. “Towards new servo control algorithms at the TNG telescope.” Astronomical Telescopes + Instrumentation (2020).
- Schneider, Lucas, Manuel Steinbrecher, Levente Rózsa, Juba Bouaziz, Krisztián Palotás, Manuel dos Santos Dias, Samir Lounis, Jens Wiebe and Roland

Wiesendanger. “Magnetism and in-gap states of 3d transition metal atoms on superconducting Re.” npj Quantum Materials 4 (2019): 1-8.
- Schneider, Stefan, Graham W. Taylor, Stefan S. Linquist and Stefan C. Kremer. “Past, present and future approaches using computer vision for animal re-identification from camera trap data.” Methods in Ecology and Evolution 10 (2019): 461 - 470.
- Schneider, Stefan, Graham W. Taylor, Stefan S. Linquist and Stefan C. Kremer. “Similarity Learning Networks for Animal Individual Re-Identification - Beyond the Capabilities of a Human Observer.” 2020 IEEE Winter Applications of Computer Vision Workshops (WACVW) (2020): 44-52.
- Schroth, Christian A. and Michael Muma. “Robust M-Estimation Based Bayesian Cluster Enumeration for Real Elliptically Symmetric Distributions.” IEEE Transactions on Signal Processing 69 (2021): 3525-3540.
- Schumann, Arne, Shaogang Gong and Tobias Schuchert. “Deep learning prototype domains for person re-identification.” 2017 IEEE International Conference on Image Processing (ICIP) (2017): 1767-1771.
- Schüssler, R. X., Hendrik Bekker, M. Brass, H. Cakir, José R. Crespo López-Urrutia, M. Door, P Filianin, Zolt’an Harman, Maurits W. Haverkort, W. J. Huang, Paul Indelicato, Christoph H. Keitel, C. M. König, K. Kromer, M. Müller, Yu. N. Novikov, A. Rischka, Ch. Schweiger, Sven Sturm, Stefan Ulmer, Sergey Eliseev and Klaus Blaum. “Detection of metastable electronic states by Penning trap mass spectrometry.” Nature 581 (2020): 42-46.
- Schwinn, Leo, An Nguyen, René Raab, Leon Bungert, Daniel Tenbrinck, Dario Zanca, Martin Burger and Bjoern M. Eskofier. “Identifying Untrustworthy Predictions in Neural Networks by Geometric Gradient Analysis.” ArXiv abs/2102.12196 (2021): n. pag.
- Sebastian, Clint, Raffaele Imbriaco, Egor Bondarev and Peter H. N. de With. “Dual Embedding Expansion for Vehicle Re-identification.” 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW) (2020): 2475-2484.
- Seidel, Paul. “Fukaya A_{∞}-structures associated to Lefschetz fibrations. IV 1/2.” Journal of Symplectic Geometry 10 (2020): 325-388.
- Sekara, Vedran, Enys Mones and Håkan Jonsson. “Temporal Limits of Privacy in Human Behavior.” ArXiv abs/1806.03615 (2018): n. pag.
- Serbetci, Ayse and Yusuf Sinan Akgül. “End-to-end training of CNN ensembles for person re-identification.” Pattern Recognit. 104 (2020): 107319.
- Shahsavarani, Sara, Morteza Analoui and Reza Shoja Ghiass. “M^2 Deep-ID: A Novel Model for Multi-View Face Identification Using Convolutional Deep Neural Networks.” ArXiv abs/2001.07871 (2020): n. pag.
- Shalam, Daniel and Simon Korman. “The Self-Optimal-Transport Feature Transform.” ArXivabs/2204.03065 (2022): n. pag.
- Shapoval, Volodymyr, P. Braun-Munzinger and Yu. M. Sinyukov. “K ∗ (892) and ϕ(1020) production and their decay into the hadronic medium at the Large Hadron Collider.” Nuclear Physics 968 (2017): 391-402.
- Sharma, Anil, Saket Anand and Sanjit Krishnan Kaul. “Intelligent Querying for Target Tracking in Camera Networks using Deep Q-Learning with n-Step Bootstrapping.” ArXiv abs/2004.09632 (2020): n. pag.

- Sharma, Charu, Siddhant Raj Kapil and David Chapman. “Person Re-Identification with a Locally Aware Transformer.” ArXiv abs/2106.03720 (2021): n. pag.
- Sharma, Sagar and Keke Chen. “Disguised-Nets: Image Disguising for Privacy-preserving Outsourced Deep Learning.” arXiv: Learning (2019): n. pag.
- Shen, Chen, Guo-Jun Qi, Rongxin Jiang, Zhongming Jin, Hongwei Yong, Yaowu Chen and Xiansheng Hua. “Sharp Attention Network via Adaptive Sampling for Person Re-Identification.” IEEE Transactions on Circuits and Systems for Video Technology 29 (2019): 3016-3027.
- Shen, Dong, Shuai Zhao, Jinming Hu, Hao Feng, Deng Cai and Xiaofei He. “ES-Net: Erasing Salient Parts to Learn More in Re-Identification.” IEEE Transactions on Image Processing 30 (2021): 1676-1686.
- Shen, Fei, Jianqing Zhu, Xiaobin Zhu, Yi Xie and Jingchang Huang. “Exploring Spatial Significance via Hybrid Pyramidal Graph Network for Vehicle Re-identification.” ArXiv abs/2005.14684 (2021): n. pag.
- Shen, Fei, Yi Xie, Jianqing Zhu, Xiaobin Zhu and Huanqiang Zeng. “GiT: Graph Interactive Transformer for Vehicle Re-identification.” ArXiv abs/2107.05475 (2021): n. pag.
- Shen, Fei, Zhe Wang, Zijun Wang, Xiaode Fu, Jiayi Chen and Xiaoyu Du. “A Competitive Method for Dog Nose-print Re-identification.” ArXiv abs/2205.15934 (2022): n. pag.
- Shen, Yantao, Hongsheng Li, Shuai Yi, Dapeng Chen and Xiaogang Wang. “Person Re-identification with Deep Similarity-Guided Graph Neural Network.” ECCV (2018).
- Shen, Yantao, Hongsheng Li, Tong Xiao, Shuai Yi, Dapeng Chen and Xiaogang Wang. “Deep Group-Shuffling Random Walk for Person Re-identification.” 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition (2018): 2265-2274.
- Shen, Yantao, Tong Xiao, Hongsheng Li, Shuai Yi and Xiaogang Wang. “End-to-End Deep Kronecker-Product Matching for Person Re-identification.” 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition (2018): 6886-6895.
- Shen, Yantao, Tong Xiao, Hongsheng Li, Shuai Yi and Xiaogang Wang. “Learning Deep Neural Networks for Vehicle Re-ID with Visual-spatio-Temporal Path Proposals.” 2017 IEEE International Conference on Computer Vision (ICCV) (2017): 1918-1927.
- Shenoi, Abhijeet, Mihir Patel, JunYoung Gwak, Patrick Goebel, Amir Sadeghian, Hamid Rezatofighi, Roberto Martin Martin and Silvio Savarese. “JRMOT: A Real-Time 3D Multi-Object Tracker and a New Large-Scale Dataset.” 2020 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS) (2020): 10335-10342.
- Sheshkal, Sajad Amouei, Kazim Fouladi-Ghaleh and Hossein Aghababa. “An Improved Person Re-identification Method by light-weight convolutional neural network.” 2020 10th International Conference on Computer and Knowledge Engineering (ICCKE) (2020): 463-468.
- Shete, Kedar Prashant and Stephen M. de Bruyn Kops. “Area of scalar isosurfaces in homogeneous isotropic turbulence as a function of Reynolds and Schmidt numbers.” Journal of Fluid Mechanics 883 (2019): n. pag.

- Shi, Claudia, Dhanya Sridhar, Vishal Misra and David M. Blei. “On the Assumptions of Synthetic Control Methods.” AISTATS (2022).
- Shi, Hailin, Yang Yang, Xiangyu Zhu, Shengcai Liao, Zhen Lei, Weishi Zheng and S. Li. “Embedding Deep Metric for Person Re-identification: A Study Against Large Variations.” ArXivabs/1611.00137 (2016): n. pag.
- Shi, Yanpei, Qiang Huang and Thomas Hain. “Speaker Re-identification with Speaker Dependent Speech Enhancement.” INTERSPEECH (2020).
- Shi, Zhiyuan, Timothy M. Hospedales and Tao Xiang. “Transferring a semantic representation for person re-identification and search.” 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (2015): 4184-4193.
- Shree, Vikram, Wei-Lun Chao and Mark E. Campbell. “An Empirical Study of Person Re-Identification with Attributes.” 2019 28th IEEE International Conference on Robot and Human Interactive Communication (RO-MAN) (2019): 1-8.
- Shridharan, B, Blesson Mathew, Sabu Nidhi, Ravikumar Anusha, Roy Arun, Sreeja S. Kartha and Yerra Bharat Kumar. “Discovery of 2716 hot emission-line stars from LAMOST DR5.” Research in Astronomy and Astrophysics 21 (2021): n. pag.
- Shu, Xiujun, Gezhong Li, Xiao Wang, Weijian Ruan and Qi Tian. “Semantic-Guided Pixel Sampling for Cloth-Changing Person Re-Identification.” IEEE Signal Processing Letters 28 (2021): 1365-1369.
- Shu, Xiujun, Xiao Wang, Shiliang Zhang, Xian Zhang, Yuanqi Chen, Gezhong Li and Qi Tian. “Large-Scale Spatio-Temporal Person Re-identification: Algorithm and Benchmark.” ArXivabs/2105.15076 (2021): n. pag.
- Shu, Xiujun, Yusheng Tao, Ruizhi Qiao, Bo Ke, Wei Wen and Bo Ren. “Head and Body: Unified Detector and Graph Network for Person Search in Media.” ArXiv abs/2111.13888 (2021): n. pag.
- Shuai, Bing, Andrew G. Berneshawi, Davide Modolo and Joseph Tighe. “Multi-Object Tracking with Siamese Track-RCNN.” ArXiv abs/2004.07786 (2020): n. pag.
- Si, Jianlou, Honggang Zhang, Chun-Guang Li, Jason Kuen, Xiangfei Kong, Alex Chichung Kot and G. Wang. “Dual Attention Matching Network for Context-Aware Feature Sequence Based Person Re-identification.” 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition(2018): 5363-5372.
- Siarohin, Aliaksandr, Stéphane Lathuilière, E. Sangineto and N. Sebe. “Appearance and Pose-Conditioned Human Image Generation Using Deformable GANs.” IEEE Transactions on Pattern Analysis and Machine Intelligence 43 (2021): 1156-1171.
- Silverberg, Steven M., Hans Moritz Günther, Jinyoung Serena Kim, David A. Principe and Scott J. Wolk. “What’s Behind the Elephant’s Trunk? Identifying Young Stellar Objects on the Outskirts of IC 1396.” The Astronomical Journal 162 (2021): n. pag.
- Singh, Krishna Kumar, Hao Yu, Aron Sarmasi, Gautam Pradeep and Yong Jae Lee. “Hide-and-Seek: A Data Augmentation Technique for Weakly-Supervised Localization and Beyond.” ArXivabs/1811.02545 (2018): n. pag.
- Singh, Ritambhara, Jack Lanchantin, Gabriel Robins and Yanjun Qi. “Transfer String Kernel for Cross-Context DNA-Protein Binding Prediction.” IEEE/ACM Transactions on Computational Biology and Bioinformatics 16 (2019): 1524-1536.

- Singh, S., Krishna P. Miyapuram and Shanmuganathan Raman. “DeepPFCN: Deep Parallel Feature Consensus Network For Person Re-Identification.” ArXiv abs/1911.07776 (2020): n. pag.
- Siv, Ratha, Matei Mancas, Bernard Gosselin, Dona Valy and Sokchenda Sreng. “People Tracking and Re-Identifying in Distributed Contexts: Extension Study of PoseTReID.” ArXiv abs/2205.10086 (2022): n. pag.
- Slawski, Martin and Bodhisattva Sen. “Permuted and Unlinked Monotone Regression in Rd: an approach based on mixture modeling and optimal transport.” ArXiv abs/2201.03528 (2022): n. pag.
- Smerdov, Anton, Bo Zhou, Paul Lukowicz and Andrey Somov. “Collection and Validation of Psycophysiological Data from Professional and Amateur Players: a Multimodal eSports Dataset.” ArXiv abs/2011.00958 (2020): n. pag.
- Smith, David B., Kanchana Thilakarathna and Mohamed Ali Kâafar. “More Flexible Differential Privacy: The Application of Piecewise Mixture Distributions in Query Release.” ArXivabs/1707.01189 (2017): n. pag.
- Smith, Russell J and Thomas E. Collett. “A fully-spectroscopic triple-source-plane lens: the Jackpot completed.” (2021).
- Solà, Joan, Joan Vallve-Navarro, Joaquim Ayuso i Casals, Jérémie Deray, Médéric Fourmy, Dinesh Atchuthan and J. Andrade-Cetto. “Wolf: A Modular Estimation Framework for Robotics Based on Factor Graphs.” IEEE Robotics and Automation Letters 7 (2022): 4710-4717.
- Soleymani, Roghayeh, Eric Granger and Giorgio Fumera. “Progressive Boosting for Class Imbalance.” ArXiv abs/1706.01531 (2017): n. pag.
- Song, Guanglu, Biao Leng, Yu Liu, Congrui Hetang and Shaofan Cai. “Region-based Quality Estimation Network for Large-scale Person Re-identification.” AAAI (2018).
- Song, Liangchen, Cheng Wang, Lefei Zhang, Bo Du, Q. Zhang, Chang Huang and Xinggang Wang. “Unsupervised Domain Adaptive Re-Identification: Theory and Practice.” ArXiv abs/1807.11334 (2020): n. pag.
- Sovrasov, Vladislav and Dmitry Sidnev. “Building Computationally Efficient and Well-Generalizing Person Re-Identification Models with Metric Learning.” 2020 25th International Conference on Pattern Recognition (ICPR) (2021): 639-646.
- Špaňhel, Jakub, Jakub Sochor, Roman Juránek, Petr Dobes, Vojtech Bartl and Adam Herout. “Learning Feature Aggregation in Temporal Domain for Re-Identification.” ArXiv abs/1903.05244 (2020): n. pag.
- Spielberg, Stephen P., Aditya Tulsyan, Nathan P. Lawrence, Philip D. Loewen and Ratna Bhushan Gopaluni. “Deep Reinforcement Learning for Process Control: A Primer for Beginners.” ArXivabs/2004.05490 (2020): n. pag.
- Srinivasan, Usha and Rangachari Kidambi. “A sorting algorithm for complex eigenvalues.” ArXivabs/2006.14254 (2020): n. pag.
- Staiger, Douglas O. and James H. Stock. “Instrumental Variables Regression with Weak Instruments.” Econometrics eJournal (1994): n. pag.
- Steil, Julian, Inken Hagestedt, Michael Xuelin Huang and Andreas Bulling. “Privacy-aware eye tracking using differential privacy.” Proceedings of the 11th ACM Symposium on Eye Tracking Research & Applications (2019): n. pag.
- Stennett, Maria, Daniel I. Rubenstein and Tilo Burghardt. “Towards Individual Grevy’s Zebra Identification via Deep 3D Fitting and Metric Learning.” (2022).

- Styles, Olly, Tanaya Guha, Victor Sanchez and Alex Chichung Kot. “Multi-Camera Trajectory Forecasting: Pedestrian Trajectory Prediction in a Network of Cameras.” 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW) (2020): 4379-4382.
- Su, Chi, Jianing Li, Shiliang Zhang, Junliang Xing, Wen Gao and Qi Tian. “Pose-Driven Deep Convolutional Model for Person Re-identification.” 2017 IEEE International Conference on Computer Vision (ICCV) (2017): 3980-3989.
- Su, Chi, Shiliang Zhang, Junliang Xing, Wen Gao and Qi Tian. “Deep Attributes Driven Multi-Camera Person Re-identification.” ECCV (2016).
- Su, Fang and Jingyan Wang. “Domain transfer convolutional attribute embedding.” Journal of Experimental & Theoretical Artificial Intelligence 30 (2018): 811 - 829.
- Su, Xinxing, Yingtian Zou, Yu Cheng, Shuangjie Xu, Mo Yu and Pan Zhou. “Spatial-Temporal Synergic Residual Learning for Video Person Re-Identification.” ArXiv abs/1807.05799 (2018): n. pag.
- Suh, Yumin, Jingdong Wang, Siyu Tang, Tao Mei and Kyoung Mu Lee. “Part-Aligned Bilinear Representations for Person Re-identification.” ArXiv abs/1804.07094 (2018): n. pag.
- Sumari, Felix O., Luigy Machaca, Jose Huaman, Esteban Walter Gonzalez Clua and Joris Michel Guerin. “Towards Practical Implementations of Person Re-Identification from Full Video Frames.” ArXiv abs/2009.01377 (2020): n. pag.
- Sun, Chenggui and Lingling Song. “Product Re-identification System in Fully Automated Defect Detection.” ArXiv abs/2112.10324 (2021): n. pag.
- Sun, He, Mingkun Li and Chun-Guang Li. “Hybrid Contrastive Learning with Cluster Ensemble for Unsupervised Person Re-identification.” ArXiv abs/2201.11995 (2021): n. pag.
- Sun, Pei, Jinkun Cao, Yi Jiang, Zehuan Yuan, Song Bai, Kris Kitani and Ping Luo. “DanceTrack: Multi-Object Tracking in Uniform Appearance and Diverse Motion.” (2021).
- Sun, Peng, Peiwen Lin, Guangliang Cheng, Jianping Shi, Jiawan Zhang and Xi Li. “OVSNet : Towards One-Pass Real-Time Video Object Segmentation.” ArXiv abs/1905.10064 (2019): n. pag.
- Sun, Shijie, Naveed Akhtar, Huansheng Song, Chaoyang Zhang, Jianxin Li and Ajmal S. Mian. “Benchmark Data and Method for Real-Time People Counting in Cluttered Scenes Using Depth Sensors.” IEEE Transactions on Intelligent Transportation Systems 20 (2019): 3599-3612.
- Sun, Shitong, Guile Wu and Shaogang Gong. “Decentralised Person Re-Identification with Selective Knowledge Aggregation.” ArXiv abs/2110.11384 (2021): n. pag.
- Sun, Xiaoxiao and Liang Zheng. “Dissecting Person Re-Identification From the Viewpoint of Viewpoint.” 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2019): 608-617
- Sun, Xiaoxiao, Yunzhong Hou, Weijian Deng, Hongdong Li and Liang Zheng. “Ranking Models in Unlabeled New Environments.” 2021 IEEE/CVF International Conference on Computer Vision (ICCV) (2021): 11741-11751.
- Sun, Yanqiu, Minxian Li and Jianfeng Lu. “Part-based Multi-stream Model for Vehicle Searching.” 2018 24th International Conference on Pattern Recognition (ICPR) (2018): 1372-1377.

- Sun, Yifan, Changmao Cheng, Yuhan Zhang, Chi Zhang, Liang Zheng, Zhongdao Wang and Yichen Wei. “Circle Loss: A Unified Perspective of Pair Similarity Optimization.” 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2020): 6397-6406.
- Sun, Yifan, Liang Zheng, Weijian Deng and Shengjin Wang. “SVDNet for Pedestrian Retrieval.” 2017 IEEE International Conference on Computer Vision (ICCV) (2017): 3820-3828.
- Sun, Yifan, Qin Xu, Yali Li, Chi Zhang, Yikang Li, Shengjin Wang and Jian Sun. “Perceive Where to Focus: Learning Visibility-Aware Part-Level Features for Partial Person Re-Identification.” 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2019): 393-402.
- Sundararaman, Ramanathan, Cédric Braga, Éric Marchand and Julien Pettré. “Tracking Pedestrian Heads in Dense Crowd.” 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2021): 3864-3874.
- Suprem, Abhijit and Calton Pu. “Looking GLAMORous: Vehicle Re-Id in Heterogeneous Cameras Networks with Global and Local Attention.” ArXiv abs/2002.02256 (2020): n. pag.
- Suprem, Abhijit, Rodrigo Alves Lima, Bruno Padilha, João Eduardo Ferreira and Calton Pu. “Robust, Extensible, and Fast: Teamed Classifiers for Vehicle Tracking and Vehicle Re-ID in Multi-Camera Networks.” arXiv: Computer Vision and Pattern Recognition (2019): n. pag.
- Tabrez, Aaquib, Matthew B. Luebbers and Bradley Hayes. “Automated Failure-Mode Clustering and Labeling for Informed Car-To-Driver Handover in Autonomous Vehicles.” ArXivabs/2005.04439 (2020): n. pag.
- Tagore, Nirbhay Kumar, Ayushman Singh, Sumanth Manche and Pratik Chattopadhyay. “Deep Learning based Person Re-identification.” ArXiv abs/2005.03293 (2020): n. pag.
- Taha, Ahmed, Yi-Ting Chen, Xitong Yang, Teruhisa Misu and Larry S. Davis. “Exploring Uncertainty in Conditional Multi-Modal Retrieval Systems.” ArXiv abs/1901.07702 (2019): n. pag.
- Taherkhani, Fariborz, Ali Dabouei, Sobhan Soleymani, Jeremy M. Dawson and Nasser M. Nasrabadi. “Attribute Guided Sparse Tensor-Based Model for Person Re-Identification.” ArXivabs/2108.04352 (2021): n. pag.
- Takács, Kristóf, Bálint Varga and Vince Grolmusz. “PDB_Amyloid: an extended live amyloid structure list from the PDB.” FEBS Open Bio 9 (2019): 185 - 190.
- Talavera, Estefanía, Alexandre Cola, Nicolai Petkov and Petia Radeva. “Towards Egocentric Person Re-Identification and Social Pattern Analysis.” APPIS (2018).
- Tamura, Masato and Tomokazu Murakami. “Augmented Hard Example Mining for Generalizable Person Re-Identification.” ArXiv abs/1910.05280 (2019): n. pag.
- Tan, Hongchen, Xiuping Liu, Shengjing Tian, Baocai Yin and Xin Li. “MHSA-Net: Multi-Head Self-Attention Network for Occluded Person Re-Identification.” ArXiv abs/2008.04015 (2020): n. pag.
- Tan, Hongchen, Xiuping Liu, Yuhao Bian, Huasheng Wang and Baocai Yin. “Incomplete Descriptor Mining With Elastic Loss for Person Re-Identification.” IEEE Transactions on Circuits and Systems for Video Technology 32 (2022): 160-171.

- Tang, Chunren, Dingyu Xue and Dongyue Chen. “Feature Diversity Learning with Sample Dropout for Unsupervised Domain Adaptive Person Re-identification.” ArXiv abs/2201.10212 (2022): n. pag.
- Tang, Hongming, Anna M M Scaife and J. Patrick Leahy. “Transfer learning for radio galaxy classification.” Monthly Notices of the Royal Astronomical Society 488 (2019): 3358-3375.
- Tang, Li, Yi Wang and Lap-Pui Chau. “Looking Twice for Partial Clues: Weakly-supervised Part-Mentored Attention Network for Vehicle Re-Identification.” ArXiv abs/2107.08228 (2021): n. pag.
- Tang, Zheng and Jenq-Neng Hwang. “MOANA: An Online Learned Adaptive Appearance Model for Robust Multiple Object Tracking in 3D.” IEEE Access 7 (2019): 31934-31945.
- Tang, Zheng, Milind R. Naphade, Ming-Yu Liu, Xiaodong Yang, Stan Birchfield, Shuo Wang, Ratnesh Kumar, D. Anastasiu and Jenq-Neng Hwang. “CityFlow: A City-Scale Benchmark for Multi-Target Multi-Camera Vehicle Tracking and Re-Identification.” 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2019): 8789-8798.
- Tang, Zheng, Milind R. Naphade, Stan Birchfield, Jonathan Tremblay, William Hodge, Ratnesh Kumar, Shuo Wang and Xiaodong Yang. “PAMTRI: Pose-Aware Multi-Task Learning for Vehicle Re-Identification Using Highly Randomized Synthetic Data.” 2019 IEEE/CVF International Conference on Computer Vision (ICCV) (2019): 211-220.
- Tangirala, Bhavesh, Ishan Bhandari, Dániel László, Deepak K. Gupta, Rajat Mani Thomas and Devanshu Arya. “Livestock Monitoring with Transformer.” ArXiv abs/2111.00801 (2021): n. pag.
- Tao, Ran, Arnold W. M. Smeulders and Shih-Fu Chang. “Generic Instance Search and Re-identification from One Example via Attributes and Categories.” ArXiv abs/1605.07104 (2016): n. pag.
- Tao, Ran, Efstratios Gavves and Arnold W. M. Smeulders. “Siamese Instance Search for Tracking.” 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (2016): 1420-1429.
- Tappert, C., Nikolaus Vogt, A. Ederoclite, Linda Schmidtobreick, M. Vučković and L. L. Becegato. “The luminosity evolution of nova shells.” arXiv: Solar and Stellar Astrophysics (2020): n. pag.
- Taufique, Abu Md Niamul and Andreas E. Savakis. “LABNet: Local Graph Aggregation Network with Class Balanced Loss for Vehicle Re-Identification.” Neurocomputing 463 (2021): 122-132.
- Taufique, Abu Md Niamul, Andreas E. Savakis, Michael Braun, Daniel B. Kubacki, Ethan Dell, Lei Qian and Sean M. O’Rourke. “SIAM-REID: confuser aware Siamese tracker with re-identification feature.” Optical Engineering + Applications (2021).
- Tay, Chiat-Pin, Sharmili Roy and Kim-Hui Yap. “AANet: Attribute Attention Network for Person Re-Identifications.” 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)(2019): 7127-7136.
- Tekumalla, Ramya and J. Banda. “A large-scale Twitter dataset for drug safety applications mined from publicly existing resources.” ArXiv abs/2003.13900 (2020): n. pag.

- Teng, Hehan, Tao He, Yuchen Guo and Guiguang Ding. “A High-Accuracy Unsupervised Person Re-identification Method Using Auxiliary Information Mined from Datasets.” ArXiv abs/2205.03124 (2022): n. pag.
- Teng, Hehan, Tao He, Yuchen Guo, Zhenhua Guo and Guiguang Ding. “A Free Lunch to Person Re-identification: Learning from Automatically Generated Noisy Tracklets.” ArXiv abs/2204.00891 (2022): n. pag.
- Tesfaye, Alemu. “Constrained Dominant sets and Its applications in computer vision.” arXiv: Computer Vision and Pattern Recognition (2020): n. pag.
- Thoreau, Michael and Navinda Kottege. “Deep Similarity Metric Learning for Real-Time Pedestrian Tracking.” arXiv: Computer Vision and Pattern Recognition (2018): n. pag.
- Tian, Jiajie, Zhu Teng, Baopeng Zhang, Yanxue Wang and Jianping Fan. “Imitating Targets from all sides: An Unsupervised Transfer Learning method for Person Re-identification.” Int. J. Mach. Learn. Cybern. 12 (2021): 2281-2295.
- Tian, Lu and Shengjin Wang. “Metric Learning in Codebook Generation of Bag-of-Words for Person Re-identification.” ArXiv abs/1704.02492 (2019): n. pag.
- Tian, Xudong, Zhizhong Zhang, Shaohui Lin, Yanyun Qu, Yuan Xie and Lizhuang Ma. “Farewell to Mutual Information: Variational Distillation for Cross-Modal Person Re-Identification.” 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2021): 1522-1531.
- Truong, Quang-Trung, Hy Dang, Zhankai Ye, Minh Le Nguyen and Bo Mei. “Image-based Vehicle Re-identification Model with Adaptive Attention Modules and Metadata Re-ranking.” ArXivabs/2007.01818 (2020): n. pag.
- Tu, Chaoping, Yin Zhao and Longjun Cai. “ESA-ReID: Entropy-Based Semantic Feature Alignment for Person re-ID.” ArXiv abs/2007.04644 (2020): n. pag.
- Tu, Ján, C. Chen, X. Huang, J. He and Xiaoping Guan. “Discriminative Feature Representation with Spatio-temporal Cues for Vehicle Re-identification.” ArXiv abs/2011.06852 (2020): n. pag.
- Ullah, Imdad, Roksana Boreli and Salil S. Kanhere. “Privacy in targeted advertising: A survey.” ArXiv abs/2009.06861 (2020): n. pag.
- Ustinova, E., Yaroslav Ganin and Victor S. Lempitsky. “Multiregion Bilinear Convolutional Neural Networks for Person Re-Identification.” arXiv: Computer Vision and Pattern Recognition (2015): n. pag.
- Valev, Krassimir, Arne Schumann, Lars Wilko Sommer and Jürgen Beyerer. “A systematic evaluation of recent deep learning architectures for fine-grained vehicle classification.” Defense + Security (2018).
- Vamosi, Stefan, Michaela D. Platzer and Thomas Reutterer. “AI-based Re-identification of Behavioral Clickstream Data.” ArXiv abs/2201.10351 (2022): n. pag.
- Varior, Rahul Rama, Bing Shuai, Jiwen Lu, Dong Xu and G. Wang. “A Siamese Long Short-Term Memory Architecture for Human Re-identification.” ECCV (2016).
- Varior, Rahul Rama, Mrinal Haloi and G. Wang. “Gated Siamese Convolutional Neural Network Architecture for Human Re-identification.” ECCV (2016).
- Vats, Kanav, Mehrnaz Fani, David A Clausi and John S. Zelek. “Evaluating deep tracking models for player tracking in broadcast ice hockey video.” ArXiv abs/2205.10949 (2022): n. pag.

- Vélez, Ivette, Caleb Rascón and Gibran Fuentes Pineda. “Lightweight Speaker Verification for Online Identification of New Speakers with Short Segments.” Appl. Soft Comput. 95 (2020): 106704.
- Venkatesaramani, Rajagopal, Bradley A. Malin and Yevgeniy Vorobeychik. “Re-identification of Individuals in Genomic Datasets Using Public Face Images.” Science advances 7 47 (2021): eabg3296 .
- Verde, Sebastiano, Cecilia Pasquini, Federica Lago, Alessa Goller, Francesco G. B. De Natale, Alessandro Piva and Giulia Boato. “Multi-clue reconstruction of sharing chains for social media images.” ArXiv abs/2108.02515 (2021): n. pag.
- Verma, Akriti, Valeh Moghaddam and Adnan Anwar. “Data-driven behavioural biometrics for continuous and adaptive user verification using Smartphone and Smartwatch.” ArXivabs/2110.03149 (2021): n. pag.
- Vinokurov, Alexander, Kirill Atapin and Y Solovyeva. “Optical Counterpart to the Ultraluminous X-Ray Source in the UGC 6456 Galaxy.” The Astrophysical Journal 893 (2020): n. pag.
- Vishwakarma, Dinesh Kumar and Sakshi Upadhyay. “A Deep Structure of Person Re-Identification Using Multi-Level Gaussian Models.” IEEE Transactions on Multi-Scale Computing Systems 4 (2018): 513-521.
- Voigt, Saskia Nuñez von, Stephan A. Fahrenkrog-Petersen, Dominik Janssen, Agnes Koschmider, Florian Tschorsch, Felix Mannhardt, Olaf Landsiedel and Matthias Weidlich. “Quantifying the Re-identification Risk of Event Logs for Process Mining.” Advanced Information Systems Engineering12127 (2020): 252 - 267.
- Vu, Xuan-Son, S. Tran and Lili Jiang. “dpUGC: Learn Differentially Private Representation for User Generated Contents.” ArXiv abs/1903.10453 (2019): n. pag.
- Wan, Fangbin, Yang Wu, Xuelin Qian and Yanwei Fu. “When Person Re-identification Meets Changing Clothes.” 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW) (2020): 3620-3628.
- Wan, Lin, Qianyan Jing, Zongyuan Sun, Chuang Zhang, Zhihang Li and Yehansen Chen. “Self-Supervised Modality-Aware Multiple Granularity Pre-Training for RGB-Infrared Person Re-Identification.” ArXiv abs/2112.06147 (2021): n. pag.
- Wan, Lin, Zongyuan Sun, Qianyan Jing, Yehansen Chen, Lijing Lu and Zhihang Li. “G2DA: Geometry-Guided Dual-Alignment Learning for RGB-Infrared Person Re-Identification.” ArXivabs/2106.07853 (2021): n. pag.
- Wang, Brian H., Yan Wang, Kilian Q. Weinberger and Mark E. Campbell. “Deep Person Re-identification for Probabilistic Data Association in Multiple Pedestrian Tracking.” ArXivabs/1810.08565 (2018): n. pag.
- Wang, Chi, Ya-Liang Chang, Shang-Ta Yang, Dong Chen and Shang-Hong Lai. “Unified Representation Learning for Cross Model Compatibility.” ArXiv abs/2008.04821 (2020): n. pag.
- Wang, Dongkai and Shiliang Zhang. “Unsupervised Person Re-Identification via Multi-Label Classification.” 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)(2020): 10978-10987.
- Wang, Fakai, Kang Zheng, Le Lu, Jing Xiao, Min Wu and Shun Miao. “Automatic Vertebra Localization and Identification in CT by Spine Rectification and Anatomically-constrained Optimization.” 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)(2021): 5276-5284.

- Wang, Fan, Lei Luo, En Zhu, Siwei Wang and Jun Long. “Multi-object Tracking with a Hierarchical Single-branch Network.” MMM (2022).
- Wang, Gaoang, Mingli Song and Jenq-Neng Hwang. “Recent Advances in Embedding Methods for Multi-Object Tracking: A Survey.” ArXiv abs/2205.10766 (2022): n. pag.
- Wang, Gaoang, Renshu Gu, Zuozhu Liu, Weijie Hu, Mingli Song and Jenq-Neng Hwang. “Track without Appearance: Learn Box and Tracklet Embedding with Local and Global Motion Patterns for Vehicle Tracking.” 2021 IEEE/CVF International Conference on Computer Vision (ICCV) (2021): 9856-9866.
- Wang, Gaoang, Yizhou Wang, Haotian Zhang, Renshu Gu and Jenq-Neng Hwang. “Exploit the Connectivity: Multi-Object Tracking with TrackletNet.” Proceedings of the 27th ACM International Conference on Multimedia (2019): n. pag.
- Wang, Guan’an, Shaogang Gong, Jian Cheng and Zeng-Huang Hou. “Faster Person Re-Identification.” ECCV (2020).
- Wang, Guan’an, Shuo Yang, Huanyu Liu, Zhicheng Wang, Yang Yang, Shuliang Wang, Gang Yu, Erjin Zhou and Jian Sun. “High-Order Information Matters: Learning Relation and Topology for Occluded Person Re-Identification.” 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2020): 6448-6457.
- Wang, Guan’an, Tianzhu Zhang, Jian Cheng, Si Liu, Yang Yang and Zeng-Huang Hou. “RGB-Infrared Cross-Modality Person Re-Identification via Joint Pixel and Feature Alignment.” 2019 IEEE/CVF International Conference on Computer Vision (ICCV) (2019): 3622-3631.
- Wang, Guan’an, Tianzhu Zhang, Yang Yang, Jian Cheng, Jianlong Chang, Xu Liang and Zeng-Huang Hou. “Cross-Modality Paired-Images Generation for RGB-Infrared Person Re-Identification.” ArXiv abs/2002.04114 (2020): n. pag.
- Wang, Guangcong, Jianhuang Lai, Pei-Yu Huang and Xiaohua Xie. “Spatial-Temporal Person Re-identification.” ArXiv abs/1812.03282 (2019): n. pag.
- Wang, Guangcong, Jianhuang Lai, Zhenyu Xie and Xiaohua Xie. “Discovering Underlying Person Structure Pattern with Relative Local Distance for Person Re-identification.” ArXivabs/1901.10100 (2019): n. pag.
- Wang, Guangrun, Guangcong Wang, Xujie Zhang, Jianhuang Lai, Zhengtao Yu and Liang Lin. “Weakly Supervised Person Re-ID: Differentiable Graphical Learning and a New Benchmark.” IEEE Transactions on Neural Networks and Learning Systems 32 (2021): 2142-2156.
- Wang, Guangrun, Keze Wang and Liang Lin. “Adaptively Connected Neural Networks.” 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2019): 1781-1790.
- Wang, Guangrun, Liang Lin, Rongcong Chen, Guangcong Wang and Jiqi Zhang. “Joint Learning of Neural Transfer and Architecture Adaptation for Image Recognition.” IEEE transactions on neural networks and learning systems PP (2021): n. pag.
- Wang, Guanshuo, Yufeng Yuan, Jiwei Li, Shiming Ge and Xi Zhou. “Receptive Multi-Granularity Representation for Person Re-Identification.” IEEE Transactions on Image Processing 29 (2020): 6096-6109.
- Wang, Guanshuo, Yufeng Yuan, Xiong Chen, Jiwei Li and Xi Zhou. “Learning Discriminative Features with Multiple Granularities for Person Re-

Identification.” Proceedings of the 26th ACM international conference on Multimedia (2018): n. pag.
- Wang, Han, Chen Wang and Lihua Xie. “Intensity Scan Context: Coding Intensity and Geometry Relations for Loop Closure Detection.” 2020 IEEE International Conference on Robotics and Automation (ICRA) (2020): 2095-2101.
- Wang, Han, Chen Wang and Lihua Xie. “Online Visual Place Recognition via Saliency Re-identification.” 2020 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)(2020): 5030-5036.
- Wang, Hanxiao, Shaogang Gong and Tao Xiang. “Highly Efficient Regression for Scalable Person Re-Identification.” ArXiv abs/1612.01341 (2016): n. pag.
- Wang, Hanxiao, Xiatian Zhu, Shaogang Gong and Tao Xiang. “Person Re-identification in Identity Regression Space.” International Journal of Computer Vision 126 (2018): 1288 - 1310.
- Wang, Haochen, Jiayi Shen, Yongtuo Liu, Yan Gao and Efstratios Gavves. “NFormer: Robust Person Re-identification with Neighbor Transformer.” ArXiv abs/2204.09331 (2022): n. pag.
- Wang, Haoran, Yue Fan, Zexin Wang, Licheng Jiao and Bernt Schiele. “Parameter-Free Spatial Attention Network for Person Re-Identification.” ArXiv abs/1811.12150 (2018): n. pag.
- Wang, Hongjun, Guangrun Wang, Ya Li, Dongyu Zhang and Liang Lin. “Transferable, Controllable, and Inconspicuous Adversarial Attacks on Person Re-identification With Deep Mis-Ranking.” 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2020): 339-348.
- Wang, Huibing, Jinjia Peng, Dongyan Chen, Guangqi Jiang, Tongtong Zhao and Xianping Fu. “Attribute-Guided Feature Learning Network for Vehicle Reidentification.” IEEE MultiMedia 27 (2020): 112-121.
- Wang, Huibing, Jinjia Peng, Guangqi Jiang, Fengqiang Xu and Xianping Fu. “Discriminative Feature and Dictionary Learning with Part-aware Model for Vehicle Re-identification.” Neurocomputing 438 (2021): 55-62.
- Wang, Jiabao, Y. Li, Yangshuo Zhang, Zhuang Miao and Rui Zhang. “A heterogeneous branch and multi-level classification network for person re-identification.” ArXiv abs/2006.01367 (2020): n. pag.
- Wang, Jiabao, Yang Li and Zhuang Miao. “Ensemble Feature for Person Re-Identification.” ArXivabs/1901.05798 (2019): n. pag.
- Wang, Jiabao, Yang Li, Shanshan Jiao, Zhuang Miao and Rui Zhang. “Grafted network for person re-identification.” Signal Process. Image Commun. 80 (2020): n. pag.
- Wang, Jiabao, Yang Li, Xiu-Shen Wei, Hang Li, Zhuang Miao and Rui Zhang. “Bridge the Gap between Supervised and Unsupervised Learning for Fine-Grained Classification.” ArXivabs/2203.00441 (2022): n. pag.
- Wang, Jian, Yunshan Zhong, Yachun Li, Chi Zhang and Yichen Wei. “Re-Identification Supervised Texture Generation.” 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2019): 11838-11848.
- Wang, Jiayun, Sanping Zhou, Jinjun Wang and Qiqi Hou. “Deep ranking model by large adaptive margin learning for person re-identification.” Pattern Recognit. 74 (2018): 241-252.
- Wang, Jingya, Xiatian Zhu, Shaogang Gong and Wei Li. “Transferable Joint Attribute-Identity Deep Learning for Unsupervised Person Re-identification.” 2018

IEEE/CVF Conference on Computer Vision and Pattern Recognition (2018): 2275-2284.
- Wang, Jinjun, Rui Shi, Qiqi Hou, Yihong Gong and Nanning Zheng. “Large Margin Learning in Set-to-Set Similarity Comparison for Person Reidentification.” IEEE Transactions on Multimedia 20 (2018): 593-604.
- Wang, Kan, Changxing Ding, Stephen J. Maybank and Dacheng Tao. “CDPM: Convolutional Deformable Part Models for Semantically Aligned Person Re-Identification.” IEEE Transactions on Image Processing 29 (2020): 3416-3428.
- Wang, Kan, Pengfei Wang, Changxing Ding and Dacheng Tao. “Batch Coherence-Driven Network for Part-Aware Person Re-Identification.” IEEE Transactions on Image Processing 30 (2021): 3405-3418.
- Wang, Mei and Weihong Deng. “Deep Visual Domain Adaptation: A Survey.” Neurocomputing 312 (2018): 135-153.
- Wang, Menglin, Baisheng Lai, Haokun Chen, Jianqiang Huang, Xiaojin Gong and Xiansheng Hua. “Towards Precise Intra-camera Supervised Person Re-Identification.” 2021 IEEE Winter Conference on Applications of Computer Vision (WACV) (2021): 3228-3237.
- Wang, Menglin, Baisheng Lai, Jianqiang Huang, Xiaojin Gong and Xiansheng Hua. “Camera-aware Proxies for Unsupervised Person Re-Identification.” AAAI (2021).
- Wang, Menglin, Baisheng Lai, Zhongming Jin, Xiaojin Gong, Jianqiang Huang and Xiansheng Hua. “Deep Active Learning for Video-based Person Re-identification.” ArXiv abs/1812.05785 (2018): n. pag.
- Wang, Menglin, Jiachen Li, Baisheng Lai, Xiaojin Gong and Xiansheng Hua. “Offline-Online Associated Camera-Aware Proxies for Unsupervised Person Re-identification.” (2022).
- Wang, Peng, Bingliang Jiao, L. Yang, Yifei Yang, Shizhou Zhang, Wei Wei and Yanning Zhang. “Vehicle Re-Identification in Aerial Imagery: Dataset and Approach.” 2019 IEEE/CVF International Conference on Computer Vision (ICCV) (2019): 460-469.
- Wang, Pengfei, Changxing Ding, Wentao Tan, Mingming Gong, Kui Jia and Dacheng Tao. “Uncertainty-aware Clustering for Unsupervised Domain Adaptive Object Re-identification.” ArXivabs/2108.09682 (2022): n. pag.
- Wang, Pengfei, Changxing Ding, Zhiyin Shao, Zhibin Hong, Sheng Zhang and Dacheng Tao. “Quality-aware Part Models for Occluded Person Re-identification.” IEEE Transactions on Multimedia (2022): n. pag.
- Wang, Pichao, Fan Wang and Hao Li. “Image-to-Video Re-Identification via Mutual Discriminative Knowledge Transfer.” ICASSP (2022).
- Wang, Qi, Sikai Bai, Junyu Gao, Yuan Yuan and Xuelong Li. “Unsupervised Domain Adaptive Learning via Synthetic Data for Person Re-identification.” ArXiv abs/2109.05542 (2021): n. pag.
- Wang, Taiqing, Shaogang Gong, Xiatian Zhu and Shengjin Wang. “Person Re-Identification by Discriminative Selection in Video Ranking.” IEEE Transactions on Pattern Analysis and Machine Intelligence 38 (2016): 2501-2514.
- Wang, Tao, Hong Liu, Pinhao Song, Tianyu Guo and Wei Shi. “Pose-guided Feature Disentangling for Occluded Person Re-identification Based on Transformer.” ArXiv abs/2112.02466 (2021): n. pag.
- Wang, Weinong, Wenjie Pei, Qiong Cao, Shu Liu, Guangming Lu and Yu-Wing Tai. “Push for Center Learning via Orthogonalization and Subspace Masking for

Person Re-Identification." IEEE Transactions on Image Processing 30 (2021): 907-920.
- Wang, Wenhao, Fang Zhao, Shengcai Liao and Ling Shao. "Attentive WaveBlock: Complementarity-Enhanced Mutual Networks for Unsupervised Domain Adaptation in Person Re-Identification and Beyond." IEEE Transactions on Image Processing 31 (2022): 1532-1544.
- Wang, Wenhao, Shengcai Liao, Fang Zhao, Cuicui Kang and Ling Shao. "DomainMix: Learning Generalizable Person Re-Identification Without Human Annotations." ArXiv abs/2011.11953 (2020): n. pag.
- Wang, Xiao, Zi-Han Chen, Rui Yang, Bin Luo and Jin Tang. "Improved Hard Example Mining by Discovering Attribute-based Hard Person Identity." ArXiv abs/1905.02102 (2019): n. pag.
- Wang, Xiaodong, Zhedong Zheng, Yang He, Fei Yan, Zhi-qiang Zeng and Yi Yang. "Progressive Local Filter Pruning for Image Retrieval Acceleration." ArXiv abs/2001.08878 (2020): n. pag.
- Wang, Xiaohong, Chao Li and Xiangcai Ma. "Cross-modal Local Shortest Path and Global Enhancement for Visible-Thermal Person Re-Identification." (2022).
- Wang, Xinglu. "Adversarial Multi-scale Feature Learning for Person Re-identification." ArXivabs/2012.14061 (2020): n. pag.
- Wang, Xinglu. "Person Re-identification with Adversarial Triplet Embedding." ArXivabs/2012.14057 (2020): n. pag.
- Wang, Xinshao, Elyor Kodirov, Yang Hua and Neil Martin Robertson. "ID-aware Quality for Set-based Person Re-identification." ArXiv abs/1911.09143 (2019): n. pag.
- Wang, Xinshao, Yang Hua, Elyor Kodirov, Guosheng Hu and Neil Martin Robertson. "Deep Metric Learning by Online Soft Mining and Class-Aware Attention." ArXiv abs/1811.01459 (2019): n. pag.
- Wang, Xueping, Min Liu, Dripta S. Raychaudhuri, S. Paul, Yaonan Wang and Amit K. Roy-Chowdhury. "Learning Person Re-Identification Models From Videos With Weak Supervision." IEEE Transactions on Image Processing 30 (2021): 3017-3028.
- Wang, Xueping, Rameswar Panda, Min Liu, Yaonan Wang and Amit K. Roy-Chowdhury. "Exploiting Global Camera Network Constraints for Unsupervised Video Person Re-Identification." IEEE Transactions on Circuits and Systems for Video Technology 31 (2021): 4020-4030.
- Wang, Xueping, Shasha Li, Min Liu, Yaonan Wang and Amit K. Roy-Chowdhury. "Multi-Expert Adversarial Attack Detection in Person Re-identification Using Context Inconsistency." 2021 IEEE/CVF International Conference on Computer Vision (ICCV) (2021): 15077-15087.
- Wang, Yan, Lequn Wang, Yurong You, Xu Zou, Vincent Chen, Serena Li, Gao Huang, Bharath Hariharan and Kilian Q. Weinberger. "Resource Aware Person Re-identification Across Multiple Resolutions." 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition (2018): 8042-8051.
- Wang, Yanan, Shengcai Liao and Ling Shao. "Surpassing Real-World Source Training Data: Random 3D Characters for Generalizable Person Re-Identification." Proceedings of the 28th ACM International Conference on Multimedia (2020): n. pag.

- Wang, Yanan, Xuezhi Liang and Shengcai Liao. “Cloning Outfits from Real-World Images to 3D Characters for Generalizable Person Re-Identification.” ArXiv abs/2204.02611 (2022): n. pag.
- Wang, Yi, Frederick Lia, Ke Wang, Kevin McNamara, Yanzhou Ji, Xiaoyu Chong, Shunli Shang, Zi-kui Liu, Richard P. Martukanitz and Long-Qing Chen. “A Thermochemical Database from High-throughput First-Principles Calculations and Its Application to Analyzing Phase Evolution in AM-fabricated IN718.” arXiv: Materials Science (2020): n. pag.
- Wang, Yue and Jun Zhang. “Revisiting the electronic phase diagram of YBa2Cu3Oy via temperature derivative of in-plane resistivity.” arXiv: Superconductivity (2017): n. pag.
- Wang, Yujiang, Jie Shen, Stavros Petridis and Maja Pantic. “A real-time and unsupervised face Re-Identification system for Human-Robot Interaction.” Pattern Recognit. Lett. 128 (2019): 559-568.
- Wang, Zheng, Z. Wang, Yinqiang Zheng, Yang Wu, Wenjun Zeng and Shin’ichi Satoh. “Beyond Intra-modality: A Survey of Heterogeneous Person Re-identification.” IJCAI (2020).
- Wang, Zhibo, Siyan Zheng, Mengkai Song, Qian Wang, Alireza Rahimpour and Hairong Qi. “advPattern: Physical-World Attacks on Deep Person Re-Identification via Adversarially Transformable Patterns.” 2019 IEEE/CVF International Conference on Computer Vision (ICCV)(2019): 8340-8349.
- Wang, Zhikang, Feng Zhu, Shixiang Tang, Rui Zhao, Lihuo He and Jiangning Song. “Feature Erasing and Diffusion Network for Occluded Person Re-Identification.” ArXiv abs/2112.08740 (2021): n. pag.
- Wang, Zhikang, Lihuo He, Xinbo Gao and Jane Shen. “Robust Person Re-Identification through Contextual Mutual Boosting.” ArXiv abs/2009.07491 (2020): n. pag.
- Wang, Zhongdao, Jingwei Zhang, Liang Zheng, Yixuan Liu, Yifan Sun, Yali Li and Shengjin Wang. “CycAs: Self-supervised Cycle Association for Learning Re-identifiable Descriptions.” ECCV(2020).
- Wang, Zhongdao, Liang Zheng and Shengjin Wang. “Query Adaptive Late Fusion for Image Retrieval.” ArXiv abs/1810.13103 (2018): n. pag.
- Wang, Zhongxiang, Masoud Hamedi and Stanley Ernest Young. “Methodology for Calculating Latency of GPS Probe Data.” Transportation Research Record 2645 (2017): 76 - 85.
- Wang, Zhongxiang, Masoud Hamedi, Elham Sharifi and Stanley Ernest Young. “Cross-Vendor and Cross-State Analysis of GPS Probe Data Latency.” Transportation Research Record 2672 (2018): 180 - 191.
- Wang, Zongge, Xin Yuan, T. Yamasaki, Yutian Lin, Xin Xu and Wenjun Zeng. “Re-identification = Retrieval + Verification: Back to Essence and Forward with a New Metric.” ArXiv abs/2011.11506 (2020): n. pag.
- Watson, Darach, C. J. Hansen, Jonatan Selsing, Andreas Koch, Daniele B. Malesani, Anja C. Andersen, J. P. U. Fynbo, Almudena Arcones, Andreas Bauswein, Stefano Covino, Aniello Grado, Kasper E. Heintz, Leslie K. Hunt, Chryssa Kouveliotou, Giorgos Leloudas, Andrew J. Levan, P. A. Mazzali and E. Pian. “Identification of strontium in the merger of two neutron stars.” Nature 574 (2019): 497-500.

- Wei, Longhui, Shiliang Zhang, Hantao Yao, Wen Gao and Qi Tian. “GLAD: Global-Local-Alignment Descriptor for Pedestrian Retrieval.” Proceedings of the 25th ACM international conference on Multimedia (2017): n. pag.
- Wei, Longhui, Shiliang Zhang, Wen Gao and Qi Tian. “Person Transfer GAN to Bridge Domain Gap for Person Re-identification.” 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition (2018): 79-88.
- Wei, Shengyun, Ruoyu Guo, Cheng Cui, Bin Lu, Shuilong Dong, Tingquan Gao, Yuning Du, Ying Zhou, Xueying Lyu, Qiwen Liu, Xiaoguang Hu, Dianhai Yu and Yanjun Ma. “PP-ShiTu: A Practical Lightweight Image Recognition System.” ArXiv abs/2111.00775 (2021): n. pag.
- Wei, Xiu-Shen, Chen-Lin Zhang, Lingqiao Liu, Chunhua Shen and Jianxin Wu. “Coarse-to-fine: A RNN-based hierarchical attention model for vehicle re-identification.” ACCV (2018).
- Weisenthal, Samuel J., Caroline M. Quill, Samir A. Farooq, Henry A. Kautz and Martin S. Zand. “Predicting acute kidney injury at hospital re-entry using high-dimensional electronic health record data.” PLoS ONE 13 (2018): n. pag.
- Wenger, Emily, Francesca Falzon, Josephine Passananti, Haitao Zheng and Ben Y. Zhao. “Assessing Privacy Risks from Feature Vector Reconstruction Attacks.” ArXiv abs/2202.05760 (2022): n. pag.
- White, Nicholas E.. “The Gamow Explorer: A Gamma-Ray Burst Mission to Study the High Redshift Universe.” arXiv: Instrumentation and Methods for Astrophysics (2020): n. pag.
- Wieczorek, Mikolaj, Andrzej Michalowski, Anna M Wróblewska and Jacek Dabrowski. “A Strong Baseline for Fashion Retrieval with Person Re-Identification Models.” ArXiv abs/2003.04094 (2020): n. pag.
- Wieczorek, Mikolaj, Barbara Rychalska and Jacek Dabrowski. “On the Unreasonable Effectiveness of Centroids in Image Retrieval.” ICONIP (2021).
- Windberger, Alexander, et al. “Analysis of the fine structure of Sn11+-Sn14+ ions by optical spectroscopy in an electron-beam ion trap.” Physical Review A 94 (2016): 012506.
- Wojke, Nicolai and Alex Bewley. “Deep Cosine Metric Learning for Person Re-identification.” 2018 IEEE Winter Conference on Applications of Computer Vision (WACV) (2018): 748-756.
- Wojke, Nicolai, Alex Bewley and Dietrich Paulus. “Simple online and realtime tracking with a deep association metric.” 2017 IEEE International Conference on Image Processing (ICIP) (2017): 3645-3649.
- Wu, Ancong, Weishi Zheng and Jianhuang Lai. “Robust Depth-Based Person Re-Identification.” IEEE Transactions on Image Processing 26 (2017): 2588-2603.
- Wu, Anpeng, Kun Kuang, Junkun Yuan, Bo Li, Pan Zhou, Jianrong Tao, Qiang Zhu, Yueting Zhuang and Fei Wu. “Learning Decomposed Representation for Counterfactual Inference.” ArXivabs/2006.07040 (2020): n. pag.
- Wu, Chaoyang, Wenhang Ge, Ancong Wu and Xiaobin Chang. “Camera-Conditioned Stable Feature Generation for Isolated Camera Supervised Person Re-IDentification.” ArXiv abs/2203.15210 (2022): n. pag.
- Wu, Di, Chao Wang, Yong Wu and De-shuang Huang. “Attention Deep Model With Multi-Scale Deep Supervision for Person Re-Identification.” IEEE Transactions on Emerging Topics in Computational Intelligence 5 (2021): 70-78.

- Wu, Di, Hongwei Yang and De-shuang Huang. “Omni-directional Feature Learning for Person Re-identification.” ArXiv abs/1812.05319 (2018): n. pag.
- Wu, Di, Kun Zhang, Si-Jia Zheng and De-shuang Huang. “Random Occlusion-recovery for Person Re-identification.” ArXiv abs/1809.09970 (2019): n. pag.
- Wu, Guile and Shaogang Gong. “Decentralised Learning from Independent Multi-Domain Labels for Person Re-Identification.” AAAI (2021).
- Wu, Haibin, Po-chun Hsu, Ji Gao, Shanshan Zhang, Shen Huang, Jian Kang, Zhiyong Wu, Helen M. Meng and Hung-yi Lee. “Adversarial Sample Detection for Speaker Verification by Neural Vocoders.” ICASSP (2022).
- Wu, Jiacheng, Jian-Xun Wang and Shawn C. Shadden. “Adding Constraints to Bayesian Inverse Problems.” AAAI (2019).
- Wu, Lin and Yang Wang. “Where to Focus: Deep Attention-based Spatially Recurrent Bilinear Networks for Fine-Grained Visual Recognition.” ArXiv abs/1709.05769 (2017): n. pag.
- Wu, Lin, Chunhua Shen and Anton van den Hengel. “Deep Linear Discriminant Analysis on Fisher Networks: A Hybrid Architecture for Person Re-identification.” ArXiv abs/1606.01595 (2017): n. pag.
- Wu, Lin, Chunhua Shen and Anton van den Hengel. “Deep Recurrent Convolutional Networks for Video-based Person Re-identification: An End-to-End Approach.” ArXiv abs/1606.01609 (2016): n. pag.
- Wu, Lin, Chunhua Shen and Anton van den Hengel. “PersonNet: Person Re-identification with Deep Convolutional Neural Networks.” ArXiv abs/1601.07255 (2016): n. pag.
- Wu, Lin, Richang Hong, Yang Wang and M. Wang. “Cross-Entropy Adversarial View Adaptation for Person Re-Identification.” IEEE Transactions on Circuits and Systems for Video Technology 30 (2020): 2081-2092.
- Wu, Lin, Y. Wang, Junbin Gao and Xue Li. “Where-and-When to Look: Deep Siamese Attention Networks for Video-Based Person Re-Identification.” IEEE Transactions on Multimedia 21 (2019): 1412-1424.
- Wu, Lin, Yang Wang, Hongzhi Yin, Meng Wang and Ling Shao. “Few-Shot Deep Adversarial Learning for Video-Based Person Re-Identification.” IEEE Transactions on Image Processing 29 (2020): 1233-1245.
- Wu, Lin, Yang Wang, Junbin Gao and Dacheng Tao. “Deep Co-attention based Comparators For Relative Representation Learning in Person Re-identification.” ArXiv abs/1804.11027 (2018): n. pag.
- Wu, Lin, Yang Wang, Junbin Gao and Xue Li. “Deep adaptive feature embedding with local sample distributions for person re-identification.” Pattern Recognit. 73 (2018): 275-288.
- Wu, Lin, Yang Wang, Ling Shao and Meng Wang. “3D PersonVLAD: Learning Deep Global Representations for Video-based Person Re-identification.” ArXiv abs/1812.10222 (2018): n. pag.
- Wu, Lin, Yang Wang, Xue Li and Junbin Gao. “What-and-Where to Match: Deep Spatially Multiplicative Integration Networks for Person Re-identification.” ArXiv abs/1707.07074 (2018): n. pag.
- Wu, Lin, Yang Wang, ZongYuan Ge, Qichang Hu and Xue Li. “Structured Deep Hashing with Convolutional Neural Networks for Fast Person Re-identification.” ArXiv abs/1702.04179 (2018): n. pag.

- Wu, Mingjie, Yongfei Zhang, Tianyu Zhang and Wenqi Zhang. “Background Segmentation for Vehicle Re-Identification.” MMM (2020).
- Wu, Shangxuan, Ying-Cong Chen, Xiang Li, Ancong Wu, Jinjie You and Weishi Zheng. “An enhanced deep feature representation for person re-identification.” 2016 IEEE Winter Conference on Applications of Computer Vision (WACV) (2016): 1-8.
- Wu, Shengsen, Liang Chen, Yihang Lou, Yan Bai, Tao Bai, Minghua Deng and Ling-yu Duan. “Neighborhood Consensus Contrastive Learning for Backward-Compatible Representation.” ArXivabs/2108.03372 (2021): n. pag.
- Wu, Xiaofu, Ben Xie, Shiliang Zhao, Suofei Zhang, Yong Xiao and Ming Li. “Diversity-Achieving Slow-DropBlock Network for Person Re-Identification.” ArXiv abs/2002.04414 (2020): n. pag.
- Wu, Yiming, Omar El Farouk Bourahla, Xi Li, Fei Wu and Qi Tian. “Adaptive Graph Representation Learning for Video Person Re-Identification.” IEEE Transactions on Image Processing 29 (2020): 8821-8830.
- Wu, Yiming, Xintian Wu, Xi Li and Jian Tian. “MGH: Metadata Guided Hypergraph Modeling for Unsupervised Person Re-identification.” Proceedings of the 29th ACM International Conference on Multimedia (2021): n. pag.
- Wu, Yuhang, Tengteng Huang, Haotian Yao, Chi Zhang, Yuanjie Shao, Chuchu Han, Changxin Gao and Nong Sang. “Multi-Centroid Representation Network for Domain Adaptive Person Re-ID.” ArXiv abs/2112.11689 (2021): n. pag.
- Wu, Zizhang, Man Wang, Lingxiao Yin, Weiwei Sun, Jason Wang and Huangbin Wu. “Vehicle Re-ID for Surround-view Camera System.” ArXiv abs/2006.16503 (2020): n. pag.
- Wu, Zizhang, Wenkai Zhang, Jizheng Wang, Man Wang, Yuan-Zhu Gan, Xinchao Gou, Muqing Fang and Jin-Young Song. “Disentangling and Vectorization: A 3D Visual Perception Approach for Autonomous Driving Based on Surround-View Fisheye Cameras.” 2021 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS) (2021): 5576-5582.
- Xia, Bryan (Ning), Yuan Gong, Yizhe Zhang and Christian Poellabauer. “Second-Order Non-Local Attention Networks for Person Re-Identification.” 2019 IEEE/CVF International Conference on Computer Vision (ICCV) (2019): 3759-3768.
- Xiang, Suncheng, Guanjie You, Mengyuan Guan, Hao Chen, Feng Wang, Ting Liu and Yuzhuo Fu. “Less is More: Learning from Synthetic Data with Fine-grained Attributes for Person Re-Identification.” ArXiv abs/2109.10498 (2021): n. pag.
- Xiang, Suncheng, Yuzhuo Fu, Guanjie You and Ting Liu. “Attribute analysis with synthetic dataset for person re-identification.” ArXiv abs/2006.07139 (2020): n. pag.
- Xiang, Suncheng, Yuzhuo Fu, Guanjie You and Ting Liu. “Taking A Closer Look at Synthesis: Fine-Grained Attribute Analysis for Person Re-Identification.” ICASSP 2021 - 2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (2021): 3765-3769.
- Xiang, Suncheng, Yuzhuo Fu, Mengyuan Guan and Ting Liu. “Learning from Self-Discrepancy via Multiple Co-teaching for Cross-Domain Person Re-Identification.” ArXiv abs/2104.02265 (2021): n. pag.

- Xiang, Suncheng, Zirui Zhang, Mengyuan Guan, Hao Chen, Binghai Yan, Ting Liu and Yuzhuo Fu. "VTBR: Semantic-based Pretraining for Person Re-Identification." ArXiv abs/2110.05074 (2021): n. pag.
- Xiang, Wangmeng, Jianqiang Huang, Xianbiao Qi, Xiansheng Hua and Lei Zhang. "Homocentric Hypersphere Feature Embedding for Person Re-Identification." 2019 IEEE International Conference on Image Processing (ICIP) (2019): 1237-1241.
- Xiao, Hao, Weiyao Lin, Bin Sheng, Ke Lu, Junchi Yan, Jingdong Wang, Errui Ding, Yihao Zhang and Hongkai Xiong. "Group Re-Identification: Leveraging and Integrating Multi-Grain Information." Proceedings of the 26th ACM international conference on Multimedia (2018): n. pag.
- Xiao, Qiqi, Haowen Luo and Chi Zhang. "Margin Sample Mining Loss: A Deep Learning Based Method for Person Re-identification." ArXiv abs/1710.00478 (2017): n. pag.
- Xiao, Qiqi, Kelei Cao, Haonan Chen, Fangyue Peng and Chi Zhang. "Cross Domain Knowledge Transfer for Person Re-identification." ArXiv abs/1611.06026 (2016): n. pag.
- Xiao, Tong, Hongsheng Li, Wanli Ouyang and Xiaogang Wang. "Learning Deep Feature Representations with Domain Guided Dropout for Person Re-identification." 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (2016): 1249-1258.
- Xiao, Tong, Shuang Li, Bochao Wang, Liang Lin and Xiaogang Wang. "Joint Detection and Identification Feature Learning for Person Search." 2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (2017): 3376-3385.
- Xie, Ben, Xiaofu Wu, Suofei Zhang, Shiliang Zhao and Ming Li. "Learning Diverse Features with Part-Level Resolution for Person Re-Identification." PRCV (2020).
- Xie, Pengyuan, Xin Xu, Zheng Wang and T. Yamasaki. "Unsupervised Video Person Re-Identification via Noise and Hard Frame Aware Clustering." 2021 IEEE International Conference on Multimedia and Expo (ICME) (2021): 1-6.
- Xie, Qiaokang, Wen-gang Zhou, Guo-Jun Qi, Qi Tian and Houqiang Li. "Progressive Unsupervised Person Re-Identification by Tracklet Association With Spatio-Temporal Regularization." IEEE Transactions on Multimedia 23 (2021): 597-610.
- Xie, Zhongwei, Lin Li, Xian Zhong and Luo Zhong. "Image-to-Video Person Re-Identification by Reusing Cross-modal Embeddings." ArXiv abs/1810.03989 (2018): n. pag.
- Xing, Yu, Benjamin J. Gravell, Xingkang He, Karl Henrik Johansson and Tyler Holt Summers. "Linear System Identification Under Multiplicative Noise from Multiple Trajectory Data." 2020 American Control Conference (ACC) (2020): 5157-5261.
- Xiong, Fu, Yanghua Xiao, Zhiguo Cao, Kaicheng Gong, Zhiwen Fang and Joey Tianyi Zhou. "Towards Good Practices on Building Effective CNN Baseline Model for Person Re-identification." ArXiv abs/1807.11042 (2018): n. pag.
- Xu, Boqiang, Jian Liang, Lingxiao He and Zhenan Sun. "META: Mimicking Embedding via oThers' Aggregation for Generalizable Person Re-identification." ArXiv abs/2112.08684 (2021): n. pag.

- Xu, Boqiang, Lingxiao He, Xingyu Liao, Wu Liu, Zhenan Sun and Tao Mei. “Black Re-ID: A Head-shoulder Descriptor for the Challenging Problem of Person Re-Identification.” Proceedings of the 28th ACM International Conference on Multimedia (2020): n. pag.
- Xu, Han, Junning Li, Liqiang Liu, Yu Wang, Haidong Yuan and Xin Wang. “Generalizable control for quantum parameter estimation through reinforcement learning.” npj Quantum Information 5 (2019): 1-8.
- Xu, Jing, Rui Zhao, Feng Zhu, Huaming Wang and Wanli Ouyang. “Attention-Aware Compositional Network for Person Re-identification.” 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition (2018): 2119-2128.
- Xu, Peng and Xiatian Zhu. “DeepChange: A Large Long-Term Person Re-Identification Benchmark with Clothes Change.” (2021).
- Xu, Shuangjie, Yu Cheng, Kang Gu, Yang Yang, Shiyu Chang and Pan Zhou. “Jointly Attentive Spatial-Temporal Pooling Networks for Video-Based Person Re-identification.” 2017 IEEE International Conference on Computer Vision (ICCV) (2017): 4743-4752.
- Xu, Tiantu, Kaiwen Shen, Yang Fu, Humphrey Shi and Felix Xiaozhu Lin. “Clique: Spatiotemporal Object Re-identification at the City Scale.” ArXiv abs/2012.09329 (2020): n. pag.
- Xu, Xin, Lei Liu, Weifeng Liu, Meng Xiao Wang and Ruimin Hu. “Person Re-Identification via Active Hard Sample Mining.” ArXiv abs/2004.04912 (2020): n. pag.
- Xu, Yan, Yu-Jhe Li, Xinshuo Weng and Kris Kitani. “Wide-Baseline Multi-Camera Calibration using Person Re-Identification.” 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2021): 13129-13138.
- Xu, Yuhao and Jiakui Wang. “A unified neural network for object detection, multiple object tracking and vehicle re-identification.” ArXiv abs/1907.03465 (2019): n. pag.
- Xu, Zichuan, Jiangkai Wu, Qiufen Xia, Pan Zhou, Jiankang Ren and Huizhi Liang. “Identity-Aware Attribute Recognition via Real-Time Distributed Inference in Mobile Edge Clouds.” Proceedings of the 28th ACM International Conference on Multimedia (2020): n. pag.
- Xuan, Shiyu and Shiliang Zhang. “Intra-Inter Camera Similarity for Unsupervised Person Re-Identification.” 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2021): 11921-11930.
- Xue, Lantian, Yixiong Zou, Peixi Peng, Yonghong Tian and Tiejun Huang. “Annotation Efficient Person Re-Identification with Diverse Cluster-Based Pair Selection.” ArXiv abs/2203.05395 (2022): n. pag.
- Xue, Mengge, Bowen Yu, Zhenyu Zhang, Tingwen Liu, Yue Zhang and Bin Wang. “Coarse-to-Fine Pre-training for Named Entity Recognition.” EMNLP (2020).
- Yadav, Ankit and Dinesh Kumar Vishwakarma. “Person Re-Identification using Deep Learning Networks: A Systematic Review.” ArXiv abs/2012.13318 (2020): n. pag.
- Yaghoubi, Ehsan, Diana Borza, S. V. Aruna Kumar and Hugo Proença. “Person re-identification: Implicitly defining the receptive fields of deep learning classification frameworks.” Pattern Recognit. Lett. 145 (2021): 23-29.

- Yala, Adam, Victor Quach, Homa Esfahanizadeh, Rafael G. L. D'Oliveira, Ken R. Duffy, Muriel M'edard, T. Jaakkola and Regina Barzilay. "Syfer: Neural Obfuscation for Private Data Release." ArXiv abs/2201.12406 (2022): n. pag.
- Yan, Cheng, Guansong Pang, Xiao Bai and Chunhua Shen. "Unified Multifaceted Feature Learning for Person Re-Identification." ArXiv abs/1911.08651 (2019): n. pag.
- Yan, Cheng, Guansong Pang, Xiao Bai, Changhong Liu, Xin Ning, Lin Gu and Jun Zhou. "Beyond Triplet Loss: Person Re-Identification With Fine-Grained Difference-Aware Pairwise Loss." IEEE Transactions on Multimedia 24 (2022): 1665-1677.
- Yan, Fei, Krystian Mikolajczyk and Josef Kittler. "Person Re-Identification with Vision and Language." 2018 24th International Conference on Pattern Recognition (ICPR) (2018): 2136-2141.
- Yan, Shiyang, Jun Xu, Yuai Liu and Lin Xu. "HorNet: A Hierarchical Offshoot Recurrent Network for Improving Person Re-ID via Image Captioning." ArXiv abs/1908.04915 (2019): n. pag.
- Yan, Tianyi, Kuan Zhu, Haiyun guo, Guibo Zhu, Ming Tang and Jinqiao Wang. "Plug-and-Play Pseudo Label Correction Network for Unsupervised Person Re-identification." (2022).
- Yan, Yichao, Bingbing Ni, Zhichao Song, Chao Ma, Yan Yan and Xiaokang Yang. "Person Re-identification via Recurrent Feature Aggregation." ECCV (2016).
- Yan, Yichao, Jie Qin, Bingbing Ni, Jiaxin Chen, Li Liu, Fan Zhu, Weishi Zheng, Xiaokang Yang and Ling Shao. "Learning Multi-Attention Context Graph for Group-Based Re-Identification." IEEE transactions on pattern analysis and machine intelligence PP (2020): n. pag.
- Yan, Yichao, Jie Qin, Jiaxin Chen, Li Liu, Fan Zhu, Ying Tai and Ling Shao. "Learning Multi-Granular Hypergraphs for Video-Based Person Re-Identification." 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2020): 2896-2905.
- Yan, Yichao, Jingpeng Li, Jie Qin, Song Bai, Shengcai Liao, Li Liu, Fan Zhu and Ling Shao. "Anchor-Free Person Search." 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2021): 7686-7695.
- Yan, Yichao, Jinpeng Li, Shengcai Liao, Jie Qin, Bingbing Ni, Xiaokang Yang and Ling Shao. "Exploring Visual Context for Weakly Supervised Person Search." ArXiv abs/2106.10506 (2021): n. pag.
- Yan, Yichao, Junjie Li, Shengcai Liao, Jie Qin, Bingbing Ni and Xiaokang Yang. "TAL: Two-stream Adaptive Learning for Generalizable Person Re-identification." (2021).
- Yan, Yichao, Qiang Zhang, Bingbing Ni, Wendong Zhang, Minghao Xu and Xiaokang Yang. "Learning Context Graph for Person Search." 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2019): 2153-2162.
- Yang, Cheng. "Copy and Paste method based on Pose for Re-identification." ArXivabs/2107.10479 (2021): n. pag.
- Yang, F., Ke Yan, Shijian Lu, Huizhu Jia, Xiaodong Xie and Wen Gao. "Attention Driven Person Re-identification." Pattern Recognit. 86 (2019): 143-155.

- Yang, Fengxiang, Ke Li, Zhun Zhong, Zhiming Luo, Xing Sun, Hao Cheng, Xiao-Wei Guo, Feiyue Huang, Rongrong Ji and Shaozi Li. “Asymmetric Co-Teaching for Unsupervised Cross Domain Person Re-Identification.” AAAI (2020).
- Yang, Fengxiang, Zhun Zhong, Zhiming Luo, Shaozi Li and N. Sebe. “Federated and Generalized Person Re-identification through Domain and Feature Hallucinating.” ArXiv abs/2203.02689 (2022): n. pag.
- Yang, Fengxiang, Zhun Zhong, Zhiming Luo, Sheng Lian and Shaozi Li. “Leveraging Virtual and Real Person for Unsupervised Person Re-Identification.” IEEE Transactions on Multimedia 22 (2020): 2444-2453.
- Yang, Fengxiang, Zhun Zhong, Zhiming Luo, Yuanzheng Cai, Yaojin Lin, Shaozi Li and N. Sebe. “Joint Noise-Tolerant Learning and Meta Camera Shift Adaptation for Unsupervised Person Re-Identification.” 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2021): 4853-4862.
- Yang, Kaiwen and Xinmei Tian. “Domain-Class Correlation Decomposition for Generalizable Person Re-Identification.” ArXiv abs/2106.15206 (2022): n. pag.
- Yang, L., Yunlong Wang, Lingqiao Liu, Peng Wang, Lu Chi, Zehuan Yuan, Changhu Wang and Yanning Zhang. “Center Prediction Loss for Re-identification.” ArXiv abs/2104.14746 (2021): n. pag.
- Yang, Lu, Hongbang Liu, Jinghao Zhou, Lingqiao Liu, Lei Zhang, Peng Wang and Yanning Zhang. “Pluggable Weakly-Supervised Cross-View Learning for Accurate Vehicle Re-Identification.” ArXivabs/2103.05376 (2021): n. pag.
- Yang, Lu, Lingqiao Liu, Yunlong Wang, Peng Wang and Yanning Zhang. “Multi-Domain Joint Training for Person Re-Identification.” ArXiv abs/2201.01983 (2022): n. pag.
- Yang, Q., Ancong Wu and Weishi Zheng. “Person Re-Identification by Contour Sketch Under Moderate Clothing Change.” IEEE Transactions on Pattern Analysis and Machine Intelligence 43 (2021): 2029-2046.
- Yang, Qiuling, Mario Coutiño, Gang Wang, Georgios B. Giannakis and Geert Leus. “Learning connectivity and higher-order interactions in radial distribution grids.” ICASSP 2020 - 2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (2020): 5555-5559.
- Yang, Wanxiang, Y. Yan and Si Chen. “Adaptive deep metric embeddings for person re-identification under occlusions.” ArXiv abs/2002.02603 (2019): n. pag.
- Yang, Xun, M. Wang and Dacheng Tao. “Person Re-Identification With Metric Learning Using Privileged Information.” IEEE Transactions on Image Processing 27 (2018): 791-805.
- Yang, Xun, Meng Wang, Richang Hong, Qi Tian and Yong Rui. “Enhancing Person Re-identification in a Self-Trained Subspace.” ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM) 13 (2017): 1 - 23.
- Yang, Yang, Shengcai Liao, Zhen Lei and S. Li. “Learning Efficient Image Representation for Person Re-Identification.” ArXiv abs/1707.02319 (2017): n. pag.
- Yang, Zizheng, Xin Jin, Kecheng Zheng and Feng Zhao. “Unleashing the Potential of Unsupervised Pre-Training with Intra-Identity Regularization for Person Re-Identification.” ArXiv abs/2112.00317 (2021): n. pag.
- Yao, Aihuan, Jiahao Qi and Ping Zhong. “Self-aligned Spatial Feature Extraction Network for UAV Vehicle Re-identification.” ArXiv abs/2201.02836 (2022): n. pag.

- Yao, Hantao and Changsheng Xu. “Dual Cluster Contrastive learning for Object Re-Identification.” (2021).
- Yao, Hantao, Shiliang Zhang, Richang Hong, Yongdong Zhang, Changsheng Xu and Qi Tian. “Deep Representation Learning With Part Loss for Person Re-Identification.” IEEE Transactions on Image Processing 28 (2019): 2860-2871.
- Yao, Yue, Liang Zheng, Xiaodong Yang, Milind Napthade and Tom Gedeon. “Attribute Descent: Simulating Object-Centric Datasets on the Content Level and Beyond.” ArXiv abs/2202.14034 (2022): n. pag.
- Yao, Yue, Liang Zheng, Xiaodong Yang, Milind R. Naphade and Tom Gedeon. “Simulating Content Consistent Vehicle Datasets with Attribute Descent.” ECCV (2020).
- Ye, Dengpan, Chuanxi Chen, Changrui Liu, H. Wang and Shunzhi Jiang. “Detection Defense Against Adversarial Attacks with Saliency Map.” ArXiv abs/2009.02738 (2021): n. pag.
- Ye, Hanjing, Jieting Zhao, Yaling Pan, Weinan Chen and Hong Zhang. “Following Closely: A Robust Monocular Person Following System for Mobile Robot.” ArXiv abs/2204.10540 (2022): n. pag.
- Ye, Hanrong, Hong Liu, Fanyang Meng and Xia Li. “Bi-Directional Exponential Angular Triplet Loss for RGB-Infrared Person Re-Identification.” IEEE Transactions on Image Processing 30 (2021): 1583-1595.
- Ye, Mang, Andy Jinhua Ma, Liang Zheng, Jiawei Li and Pong Chi Yuen. “Dynamic Label Graph Matching for Unsupervised Video Re-identification.” 2017 IEEE International Conference on Computer Vision (ICCV) (2017): 5152-5160.
- Ye, Mang, Jianbing Shen, David J. Crandall, Ling Shao and Jiebo Luo. “Dynamic Dual-Attentive Aggregation Learning for Visible-Infrared Person Re-Identification.” ArXiv abs/2007.09314 (2020): n. pag.
- Ye, Mang, Jianbing Shen, Gaojie Lin, Tao Xiang, Ling Shao and Steven C. H. Hoi. “Deep Learning for Person Re-Identification: A Survey and Outlook.” IEEE Transactions on Pattern Analysis and Machine Intelligence 44 (2022): 2872-2893.
- Yin, Junhui, Jiayan Qiu, Siqing Zhang, Jiyang Xie, Zhanyu Ma and Jun Guo. “Unsupervised Person Re-identification via Simultaneous Clustering and Consistency Learning.” ArXiv abs/2104.00202 (2021): n. pag.
- Yin, Junhui, Jiayan Qiu, Siqing Zhang, Zhanyu Ma and Jun Guo. “SSKD: Self-Supervised Knowledge Distillation for Cross Domain Adaptive Person Re-Identification.” 2021 7th IEEE International Conference on Network Intelligence and Digital Content (IC-NIDC) (2021): 81-85.
- Yin, Junhui, Zhanyu Ma, Jiyang Xie, Shibo Nie, Kongming Liang and Jun Guo. “DF^2AM: Dual-level Feature Fusion and Affinity Modeling for RGB-Infrared Cross-modality Person Re-identification.” ArXiv abs/2104.00226 (2021): n. pag.
- Yin, Zhou, Weishi Zheng, Ancong Wu, Hong-Xing Yu, Hai Wan, Xiaowei Guo, Feiyue Huang and Jianhuang Lai. “Adversarial Attribute-Image Person Re-identification.” IJCAI (2018).
- You, Jinjie, Ancong Wu, Xiang Li and Weishi Zheng. “Top-Push Video-Based Person Re-identification.” 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)(2016): 1345-1353.
- Yozin, Cameron and Kenji Bekki. “The global warming of group satellite galaxies.” Monthly Notices of the Royal Astronomical Society 460 (2016): 3968-3974.

- Yu, Fufu, Xinyang Jiang, Yifei Gong, Shizhen Zhao, Xiao-Wei Guo, Weishi Zheng, Feng Zheng and Xing Sun. “Devil’s in the Details: Aligning Visual Clues for Conditional Embedding in Person Re-Identification.” arXiv: Computer Vision and Pattern Recognition (2020): n. pag.
- Yu, Henry H., Jiang Liu, Hao Sun, Ziwen Wang and Haotian Zhang. “GetNet: Get Target Area for Image Pairing.” 2019 International Conference on Image and Vision Computing New Zealand (IVCNZ) (2019): 1-6.
- Yu, Hong-Xing and Weishi Zheng. “Weakly Supervised Discriminative Feature Learning With State Information for Person Identification.” 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2020): 5527-5537.
- Yu, Hong-Xing, Ancong Wu and Weishi Zheng. “Cross-View Asymmetric Metric Learning for Unsupervised Person Re-Identification.” 2017 IEEE International Conference on Computer Vision (ICCV) (2017): 994-1002.
- Yu, Hong-Xing, Ancong Wu and Weishi Zheng. “Unsupervised Person Re-Identification by Deep Asymmetric Metric Embedding.” IEEE Transactions on Pattern Analysis and Machine Intelligence42 (2020): 956-973.
- Yu, Hong-Xing, Weishi Zheng, Ancong Wu, Xiaowei Guo, Shaogang Gong and Jianhuang Lai. “Unsupervised Person Re-Identification by Soft Multilabel Learning.” 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2019): 2143-2152.
- Yu, Jongmin and Hyeontaek Oh. “Unsupervised Person Re-identification via Multi-Label Prediction and Classification based on Graph-Structural Insight.” ArXiv abs/2106.08798 (2021): n. pag.
- Yu, Jongmin and Hyeontaek Oh. “Unsupervised Vehicle Re-Identification via Self-supervised Metric Learning using Feature Dictionary.” 2021 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS) (2021): 3806-3813.
- Yu, Jongmin, Junsik Kim, Minkyung Kim and Hyeontaek Oh. “Camera-Tracklet-Aware Contrastive Learning for Unsupervised Vehicle Re-Identification.” ArXiv abs/2109.06401 (2021): n. pag.
- Yu, Qian, Xiaobin Chang, Yi-Zhe Song, Tao Xiang and Timothy M. Hospedales. “The Devil is in the Middle: Exploiting Mid-level Representations for Cross-Domain Instance Matching.” ArXivabs/1711.08106 (2017): n. pag.
- Yu, Rui, Dawei Du, Rodney LaLonde, Daniel S. Davila, Christopher Funk, A. Hoogs and Brian Clipp. “Cascade Transformers for End-to-End Person Search.” ArXiv abs/2203.09642 (2022): n. pag.
- Yu, Rui, Zhichao Zhou, Song Bai and Xiang Bai. “Divide and Fuse: A Re-ranking Approach for Person Re-identification.” ArXiv abs/1708.04169 (2017): n. pag.
- Yu, Rui, Zhiyong Dou, Song Bai, Zhaoxiang Zhang, Yongchao Xu and Xiang Bai. “Hard-Aware Point-to-Set Deep Metric for Person Re-identification.” ECCV (2018).
- Yu, Shijie, Dapeng Chen, Rui Zhao, Haobin Chen and Yu Qiao. “Neighbourhood-guided Feature Reconstruction for Occluded Person Re-Identification.” ArXiv abs/2105.07345 (2021): n. pag.
- Yu, Shijie, Feng Zhu, Dapeng Chen, Rui Zhao, Haobin Chen, Shixiang Tang, Jinguo Zhu and Yu Qiao. “Multiple Domain Experts Collaborative Learning: Multi-

Source Domain Generalization For Person Re-Identification." ArXiv abs/2105.12355 (2021): n. pag.
- Yu, Shijie, Shihua Li, Dapeng Chen, Rui Zhao, Junjie Yan and Yu Qiao. "COCAS: A Large-Scale Clothes Changing Person Dataset for Re-Identification." 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2020): 3397-3406.
- Yu, Zeng, Tianrui Li, Ning Yu, Xun Gong, Ke Chen and Yi Pan. "Three-Stream Convolutional Networks for Video-based Person Re-Identification." 2019 IEEE 14th International Conference on Intelligent Systems and Knowledge Engineering (ISKE) (2019): 598-606.
- Yu, Zhengxu, Yilun Zhao, Bin Hong, Zhongming Jin, Jianqiang Huang, Deng Cai and Xiansheng Hua. "Apparel-invariant Feature Learning for Apparel-changed Person Re-identification." ArXivabs/2008.06181 (2020): n. pag.
- Yuan, Meng, Seyed Yahya Nikouei, Alem Fitwi, Yu Chen and Yunxi Dong. "Minor Privacy Protection Through Real-time Video Processing at the Edge." 2020 29th International Conference on Computer Communications and Networks (ICCCN) (2020): 1-6.
- Yuan, Mingyue, Dong Yin, Jingwen Ding, Yuhao Luo, Zhipeng Zhou, Chengfeng Zhu and Rui Zhang. "A framework with updateable joint images re-ranking for Person Re-identification." ArXivabs/1803.02983 (2018): n. pag.
- Yuan, Ye, Wuyang Chen, Tianlong Chen, Yang Yang, Zhou Ren, Zhangyang Wang and Gang Hua. "Calibrated Domain-Invariant Learning for Highly Generalizable Large Scale Re-Identification." 2020 IEEE Winter Conference on Applications of Computer Vision (WACV) (2020): 3578-3587.
- Yuan, Ye, Wuyang Chen, Yang Yang and Zhangyang Wang. "In Defense of the Triplet Loss Again: Learning Robust Person Re-Identification with Fast Approximated Triplet Loss and Label Distillation." 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW) (2020): 1454-1463.
- Yuqi, Zhang, Xu Xianzhe, Chen Weihua, Wang Yaohua, Zhang Fangyi, Wang Fan and Li Hao. "2nd Place Solution to Google Landmark Retrieval 2021." (2021).
- Zahra, Asma, Nazia Perwaiz, M. Shahzad and Muhammad Moazam Fraz. "Person Re-identification: A Retrospective on Domain Specific Open Challenges and Future Trends." ArXivabs/2202.13121 (2022): n. pag.
- Zakria, Jianhua Deng, Muhammad Saddam Khokhar, Muhammad Umar Aftab, Jingye Cai, Rajesh Kumar and Jay Kumar. "Trends in Vehicle Re-identification Past, Present, and Future: A Comprehensive Review." ArXiv abs/2102.09744 (2021): n. pag.
- Zamprogno, Marco, Marco Passon, Niki Martinel, Giuseppe Serra, Giuseppe Lancioni, Christian Micheloni, Carlo Tasso and Gian Luca Foresti. "Video-Based Convolutional Attention for Person Re-Identification." ICIAP (2019).
- Zang, Xianghao, Ge Li and Wei Gao. "Multi-direction and Multi-scale Pyramid in Transformer for Video-based Pedestrian Retrieval." ArXiv abs/2202.06014 (2022): n. pag.
- Zang, Xianghao, Gezhong Li, Wei Gao and Xiujun Shu. "Exploiting Robust Unsupervised Video Person Re-identification." IET Image Process. 16 (2022): 729-741.

- Zang, Xianghao, Gezhong Li, Wei Gao and Xiujun Shu. “Learning to Disentangle Scenes for Person Re-identification.” Image Vis. Comput. 116 (2021): 104330.
- Zavala, Jorge A.. “A Tentative Emission Line at $z = 5.8$ from a 3 mm Selected Galaxy.” Research Notes of the AAS 5 (2021): n. pag.
- Zeng, Kaiwei, Munan Ning, Yaohua Wang and Yang Guo. “Hierarchical Clustering With Hard-Batch Triplet Loss for Person Re-Identification.” 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2020): 13654-13662.
- Zeng, Kaiwei. “Energy Clustering for Unsupervised Person Re-identification.” ArXivabs/1909.00112 (2020): n. pag.
- Zeng, Tingting and Prabir Barooah. “An adaptive MPC scheme for energy-efficient control of building HVAC systems.” ArXiv abs/2102.03856 (2021): n. pag.
- Zeng, Zelong, Zhixiang Wang, Zheng Wang, Yung-Yu Chuang and Shin’ichi Satoh. “Illumination-Adaptive Person Re-identification.” IEEE Transactions on Multimedia 22 (2019): 3064-3074.
- Zhai, Sulan, Shunqiang Liu, Xiao Wang and Jin Tang. “FMT: fusing multi-task convolutional neural network for person search.” Multimedia Tools and Applications 78 (2019): 31605 - 31616.
- Zhai, Yao, Xun Guo, Yan Lu and Houqiang Li. “In Defense of the Classification Loss for Person Re-Identification.” 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW) (2019): 1526-1535.
- Zhai, Yunpeng, Qixiang Ye, Shijian Lu, Mengxi Jia, Rongrong Ji and Yonghong Tian. “Multiple Expert Brainstorming for Domain Adaptive Person Re-identification.” ArXiv abs/2007.01546 (2020): n. pag.
- Zhai, Yunpeng, Shijian Lu, Qixiang Ye, Xuebo Shan, Jie Chen, Rongrong Ji and Yonghong Tian. “AD-Cluster: Augmented Discriminative Clustering for Domain Adaptive Person Re-Identification.” 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2020): 9018-9027.
- Zhan, Fangneng, Shijian Lu and Aoran Xiao. “Spatial-Aware GAN for Unsupervised Person Re- identification.” 2020 25th International Conference on Pattern Recognition (ICPR) (2021): 6889-6896.
- Zhan, Yuting, Alex Kyllo, Afra Jahanbakhsh Mashhadi and Hamed Haddadi. “Privacy-Aware Human Mobility Prediction via Adversarial Networks.” ArXiv abs/2201.07519 (2022): n. pag.
- Zhang, Can, Hong Liu, Wenting Guo and Mang Ye. “Multi-Scale Cascading Network with Compact Feature Learning for RGB-Infrared Person Re-Identification.” 2020 25th International Conference on Pattern Recognition (ICPR) (2021): 8679-8686.
- Zhang, Chengyuan, Lei Zhu and Shichao Zhang. “PAC-GAN: An Effective Pose Augmentation Scheme for Unsupervised Cross-View Person Re-identification.” ArXiv abs/1906.01792 (2020): n. pag.
- Zhang, Chengyuan, Lin Wu and Yang Wang. “Crossing Generative Adversarial Networks for Cross-View Person Re-identification.” ArXiv abs/1801.01760 (2019): n. pag.
- Zhang, Chongzhen, Jianrui Wang, Gary G. Yen, Chaoqiang Zhao, Qiyu Sun, Yang Tang, Feng Qian and Jürgen Kurths. “When Autonomous Systems Meet Accuracy and Transferability through AI: A Survey.” Patterns 1 (2020): n. pag.

- Zhang, Enwei, Xinyang Jiang, Hao Cheng, Ancong Wu, Fufu Yu, Ke Li, Xiao-Wei Guo, Feng Zheng, Weishi Zheng and Xing Sun. “One for More: Selecting Generalizable Samples for Generalizable ReID Model.” AAAI (2021).
- Zhang, Guoqing, Junchuan Yang, Yuhui Zheng, Yi Wu and Shengyong Chen. “Hybrid-Attention Guided Network with Multiple Resolution Features for Person Re-Identification.” Inf. Sci. 578 (2021): 525-538.
- Zhang, Guoqing, Yuhao Chen, Weisi Lin, Arun Kumar Chandran and Xuan Jing. “Low Resolution Information Also Matters: Learning Multi-Resolution Representations for Person Re-Identification.” IJCAI (2021).
- Zhang, Guoqing, Yuhao Chen, Yang Dai, Yuhui Zheng and Yi Wu. “Reference-Aided Part-Aligned Feature Disentangling for Video Person Re-Identification.” 2021 IEEE International Conference on Multimedia and Expo (ICME) (2021): 1-6.
- Zhang, Guoqing, Yuying Ge, Zhicheng Dong, Hao Wang, Yuhui Zheng and Shengyong Chen. “Deep High-Resolution Representation Learning for Cross-Resolution Person Re-Identification.” IEEE Transactions on Image Processing 30 (2021): 8913-8925.
- Zhang, Guowen, Pingping Zhang, Jinqing Qi and Huchuan Lu. “HAT: Hierarchical Aggregation Transformers for Person Re-identification.” Proceedings of the 29th ACM International Conference on Multimedia (2021): n. pag.
- Zhang, Hongliang, Shoudong Han, Xiaofeng Pan and Jun Zhao. “ANL: Anti-Noise Learning for Cross-Domain Person Re-Identification.” ArXiv abs/2012.13853 (2020): n. pag.
- Zhang, Jiabin, Zheng Zhu, Wei Zou, Peng Li, Yanwei Li, Hu Su and Guan Huang. “FastPose: Towards Real-time Pose Estimation and Tracking via Scale-normalized Multi-task Networks.” ArXiv abs/1908.05593 (2019): n. pag.
- Zhang, Jianfu, Naiyan Wang and Liqing Zhang. “Multi-shot Pedestrian Re-identification via Sequential Decision Making.” 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition (2018): 6781-6789.
- Zhang, Jiangning, L. Liu, Chao Xu and Yong Liu. “Hierarchical and Efficient Learning for Person Re-Identification.” ArXiv abs/2005.08812 (2020): n. pag.
- Zhang, Jimuyang, Sanping Zhou, Jinjun Wang and Dong Huang. “Frame-wise Motion and Appearance for Real-time Multiple Object Tracking.” ArXiv abs/1905.02292 (2019): n. pag.
- Zhang, Jimuyang, Sanping Zhou, Xin Chang, Fangbin Wan, Jinjun Wang, Yang Wu and Dong Huang. “Multiple Object Tracking by Flowing and Fusing.” ArXiv abs/2001.11180 (2020): n. pag.
- Zhang, Kun, Guangyi Lv, Le Wu, Enhong Chen, Qi Liu and Meng Wang. “LadRa-Net: Locally-Aware Dynamic Re-read Attention Net for Sentence Semantic Matching.” IEEE transactions on neural networks and learning systems PP (2021): n. pag.
- Zhang, Le, Zenglin Shi, Joey Tianyi Zhou, Ming-Ming Cheng, Yun Liu, Jiawang Bian, Zeng Zeng and Chunhua Shen. “Ordered or Orderless: A Revisit for Video Based Person Re-Identification.” IEEE Transactions on Pattern Analysis and Machine Intelligence 43 (2021): 1460-1466.
- Zhang, Lei, Helen Gray, Xujiong Ye, Lisa Collins and Nigel M. Allinson. “Automatic individual pig detection and tracking in surveillance videos.” ArXiv abs/1812.04901 (2018): n. pag.

- Zhang, Lei, Xiaofu Wu, Suofei Zhang and Zirui Yin. “Branch-Cooperative OSNet for Person Re-Identification.” ArXiv abs/2006.07206 (2020): n. pag.
- Zhang, Li, Tao Xiang and Shaogang Gong. “Learning a Discriminative Null Space for Person Re-identification.” 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)(2016): 1239-1248.
- Zhang, Ping, Zhenxiang Tao, Wenjie Yang, Minze Chen, Shan Ding, Xiaodong Liu, Rui Yang and Hui Zhang. “Unveiling personnel movement in a larger indoor area with a non-overlapping multi-camera system.” ArXiv abs/2104.04662 (2021): n. pag.
- Zhang, Ruimao, Jingyu Li, Hongbin Sun, Yuying Ge, Ping Luo, Xiaogang Wang and Liang Lin. “SCAN: Self-and-Collaborative Attention Network for Video Person Re-Identification.” IEEE Transactions on Image Processing 28 (2019): 4870-4882.
- Zhang, Shaoxiong, Yunhong Wang, Tianrui Chai, Annan Li and Anil K. Jain. “RealGait: Gait Recognition for Person Re-Identification.” ArXiv abs/2201.04806 (2022): n. pag.
- Zhang, Shizhou, Qi Zhang, Xing Wei, Peng Wang, Bingliang Jiao and Yanning Zhang. “Person Re-Identification in Aerial Imagery.” IEEE Transactions on Multimedia 23 (2021): 281-291.
- Zhang, Shizhou, Yifei Yang, Peng Wang, Guoqiang Liang, Xiuwei Zhang and Yanning Zhang. “Attend to the Difference: Cross-Modality Person Re-Identification via Contrastive Correlation.” IEEE Transactions on Image Processing 30 (2021): 8861-8872.
- Zhang, Suofei, Zirui Yin, Xiofu Wu, Kun Wang, Quan Zhou and Bin Kang. “FPB: Feature Pyramid Branch for Person Re-Identification.” ArXiv abs/2108.01901 (2021): n. pag.
- Zhang, Tianyu, Lingxi Xie, Longhui Wei, Yongfei Zhang, Bo Li and Qi Tian. “Single Camera Training for Person Re-identification.” ArXiv abs/1909.10848 (2020): n. pag.
- Zhang, Tianyu, Lingxi Xie, Longhui Wei, Zijie Zhuang, Yongfei Zhang, Bo Li and Qi Tian. “UnrealPerson: An Adaptive Pipeline towards Costless Person Re-identification.” 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2021): 11501-11510.
- Zhang, Tianyu, Longhui Wei, Lingxi Xie, Zijie Zhuang, Yongfei Zhang, Bo Li and Qi Tian. “Spatiotemporal Transformer for Video-based Person Re-identification.” ArXiv abs/2103.16469 (2021): n. pag.
- Zhang, Wei, Shengnan Hu, Kang Liu and Zhengjun Zha. “Learning Compact Appearance Representation for Video-Based Person Re-Identification.” IEEE Transactions on Circuits and Systems for Video Technology 29 (2019): 2442-2452.
- Zhang, Xiao, Yixiao Ge, Yu Qiao and Hongsheng Li. “Refining Pseudo Labels with Clustering Consensus over Generations for Unsupervised Object Re-identification.” 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2021): 3435-3444.
- Zhang, Xinyu, Dong Gong, Jiewei Cao and Chunhua Shen. “Memorizing Comprehensively to Learn Adaptively: Unsupervised Cross-Domain Person Re-ID with Multi-level Memory.” ArXivabs/2001.04123 (2020): n. pag.

- Zhang, Xinyu, Dongdong Li, Zhigang Wang, Jian Wang, Errui Ding, Javen Qinfeng Shi, Zhaoxi Zhang and Jingdong Wang. “Implicit Sample Extension for Unsupervised Person Re-Identification.” ArXiv abs/2204.06892 (2022): n. pag.
- Zhang, Xinyu, Jiewei Cao, Chunhua Shen and Mingyu You. “Self-Training With Progressive Augmentation for Unsupervised Cross-Domain Person Re-Identification.” 2019 IEEE/CVF International Conference on Computer Vision (ICCV) (2019): 8221-8230.
- Zhang, Xinyu, Xinlong Wang, Jiawang Bian, Chunhua Shen and Mingyu You. “Diverse Knowledge Distillation for End-to-End Person Search.” AAAI (2021).
- Zhang, Xuan, Haowen Luo, Xing Fan, Weilai Xiang, Yixiao Sun, Qiqi Xiao, Wei Jiang, Chi Zhang and Jian Sun. “AlignedReID: Surpassing Human-Level Performance in Person Re-Identification.” ArXivabs/1711.08184 (2017): n. pag.
- Zhang, Yan, Binyu He, Li Sun and Qingli Li. “Progressive Multi-Stage Feature Mix for Person Re-Identification.” ICASSP 2021 - 2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (2021): 2765-2769.
- Zhang, Yan, Zhilin Zheng, Binyu He and Li Sun. “Learning Posterior and Prior for Uncertainty Modeling in Person Re-Identification.” ArXiv abs/2007.08785 (2020): n. pag.
- Zhang, Yi-Fan, Hanlin Zhang, Zhang Zhang, Da Li, Zhen Jia, Liang Wang and Tieniu Tan. “Learning Domain Invariant Representations for Generalizable Person Re-Identification.” ArXivabs/2103.15890 (2021): n. pag.
- Zhang, Yifu, Chunyu Wang, Xinggang Wang, Wenjun Zeng and Wenyu Liu. “FairMOT: On the Fairness of Detection and Re-identification in Multiple Object Tracking.” Int. J. Comput. Vis. 129 (2021): 3069-3087.
- Zhang, Yifu, Chunyu Wang, Xinggang Wang, Wenyu Liu and Wenjun Zeng. “VoxelTrack: Multi-Person 3D Human Pose Estimation and Tracking in the Wild.” IEEE transactions on pattern analysis and machine intelligence PP (2022): n. pag.
- Zhang, Ying, Tao Xiang, Timothy M. Hospedales and Huchuan Lu. “Deep Mutual Learning.” 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition (2018): 4320-4328.
- Zhang, Yingying, Qiaoyong Zhong, Liang Ma, Di Xie and Shiliang Pu. “Learning Incremental Triplet Margin for Person Re-identification.” AAAI (2019).
- Zhang, Yulin, Bo Ma, Longyao Liu and Xin Yi. “Self-Paced Uncertainty Estimation for One-shot Person Re-Identification.” ArXiv abs/2104.09152 (2021): n. pag.
- Zhang, Yuqi, Qiang Qi, Chong Liu, Weihua Chen, Fan Wang, Hao Li and Rong Jin. “Graph Convolution for Re-ranking in Person Re-identification.” ICASSP (2022).
- Zhang, Yu-ying, Thomas. H. Reiprich, P. Christian Schneider, Nicolas Clerc, Andrea Merloni, Axel Schwope, Katharina Borm, Heinz Andernach, César Augusto Caretta and Xiang-Ping Wu. “HIFLUGCS: X-ray luminosity -- dynamical mass relation and its implications for mass calibrations with the SPIDERS and 4MOST surveys.” arXiv: Cosmology and Nongalactic Astrophysics (2016): n. pag.
- Zhang, Zhiguang. “Ranking and Classification driven Feature Learning for Person Re_identification.” ArXiv abs/1912.11630 (2019): n. pag.

- Zhang, Zhimeng, Jianan Wu, Xuan Zhang and Chi Zhang. “Multi-Target, Multi-Camera Tracking by Hierarchical Clustering: Recent Progress on DukeMTMC Project.” ArXiv abs/1712.09531 (2017): n. pag.
- Zhang, Zhimin, Zheng Wang and Weiwen Hu. “Unsupervised Manga Character Re-identification via Face-body and Spatial-temporal Associated Clustering.” ArXiv abs/2204.04621 (2022): n. pag.
- Zhang, Zhizheng, Cuiling Lan, Wenjun Zeng and Zhibo Chen. “Densely Semantically Aligned Person Re-Identification.” 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2019): 667-676.
- Zhang, Zhizheng, Cuiling Lan, Wenjun Zeng and Zhibo Chen. “Multi-Granularity Reference-Aided Attentive Feature Aggregation for Video-Based Person Re-Identification.” 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2020): 10404-10413.
- Zhang, Zhizheng, Cuiling Lan, Wenjun Zeng, Quanzeng You, Zicheng Liu, Kecheng Zheng and Zhibo Chen. “Disentanglement-based Cross-Domain Feature Augmentation for Effective Unsupervised Domain Adaptive Person Re-identification.” ArXiv abs/2103.13917 (2021): n. pag.
- Zhang, Zhizheng, Cuiling Lan, Wenjun Zeng, Xin Jin and Zhibo Chen. “Relation-Aware Global Attention for Person Re-Identification.” 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2020): 3183-3192.
- Zhang, Zhizheng, Cuiling Lan, Wenjun Zeng, Zhibo Chen and Shih-Fu Chang. “Beyond Triplet Loss: Meta Prototypical N-tuple Loss for Person Re-identification.” IEEE Transactions on Multimedia(2021): n. pag.
- Zhang, Zhulin, Dong Li, Jinhua Wu, Yunda Sun and Li Zhang. “MVB: A Large-Scale Dataset for Baggage Re-Identification and Merged Siamese Networks.” PRCV (2019).
- Zhang, Zikai, Bineng Zhong, Shengping Zhang, Zhenjun Tang, Xin Liu and Zhaoxiang Zhang. “Distractor-Aware Fast Tracking via Dynamic Convolutions and MOT Philosophy.” 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2021): 1024-1033.
- Zhang, Ziyue, Richard Y. D. Xu, Shuai Jiang, Y. Li, Congzhentao Huang and Chen Deng. “Illumination Adaptive Person Reid Based on Teacher-Student Model and Adversarial Training.” 2020 IEEE International Conference on Image Processing (ICIP) (2020): 2321-2325.
- Zhang, Ziyue, Shuai Jiang, Congzhentao Huang and Richard Yi Da Xu. “Resolution-Invariant Person Reid Based On Feature Transformation And Self-Weighted Attention.” 2021 IEEE International Conference on Image Processing (ICIP) (2021): 1134-1138.
- Zhang, Ziyue, Shuai Jiang, Congzhentao Huang, Y. Li and Richard Yi Da Xu. “RGB-IR Cross-modality Person ReID based on Teacher-Student GAN Model.” Pattern Recognit. Lett. 150 (2021): 155-161.
- Zhao, Jia-jun, Yifan Zhao, Jia Li, Ke Yan and Yonghong Tian. “Heterogeneous Relational Complement for Vehicle Re-identification.” 2021 IEEE/CVF International Conference on Computer Vision (ICCV) (2021): 205-214.
- Zhao, Jian, Jianshu Li, Yu Cheng, Li Zhou, Terence Sim, Shuicheng Yan and Jiashi Feng. “Understanding Humans in Crowded Scenes: Deep Nested Adversarial

Learning and A New Benchmark for Multi-Human Parsing." ArXiv abs/1804.03287 (2018): n. pag.
- Zhao, Kun, Arnold Wiliem, Shaokang Chen and Brian C. Lovell. "Convex Class Model on Symmetric Positive Definite Manifolds." ArXiv abs/1806.05343 (2019): n. pag.
- Zhao, Liming, Xi Li, Yueting Zhuang and Jingdong Wang. "Deeply-Learned Part-Aligned Representations for Person Re-identification." 2017 IEEE International Conference on Computer Vision (ICCV) (2017): 3239-3248.
- Zhao, Shizhen, Changxin Gao, Jun Zhang, Hao Cheng, Chuchu Han, Xinyang Jiang, Xiao-Wei Guo, Weishi Zheng, Nong Sang and Xing Sun. "Do Not Disturb Me: Person Re-identification Under the Interference of Other Pedestrians." ArXiv abs/2008.06963 (2020): n. pag.
- Zhao, Yunbin, Song-Chun Zhu, Dongsheng Wang and Zhiwei Liang. "Short Range Correlation Transformer for Occluded Person Re-Identification." ArXiv abs/2201.01090 (2022): n. pag.
- Zhao, Yuyang, Zhun Zhong, Fengxiang Yang, Zhiming Luo, Yaojin Lin, Shaozi Li and N. Sebe. "Learning to Generalize Unseen Domains via Memory-based Multi-Source Meta-Learning for Person Re-Identification." 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2021): 6273-6282.
- Zhao, Zilong, Jichang Zhao, Yukie Sano, Orr Levy, Hideki Takayasu, Misako Takayasu, Daqing Li and Shlomo Havlin. "Fake news propagates differently from real news even at early stages of spreading." EPJ Data Science 9 (2020): 1-14.
- Zheng, Aihua, Xia Sun, Chenglong Li and Jin Tang. "Viewpoint-aware Progressive Clustering for Unsupervised Vehicle Re-identification." ArXiv abs/2011.09099 (2021): n. pag.
- Zheng, Aihua, Xianmin Lin, Chenglong Li, Ran He and Jin Tang. "Attributes Guided Feature Learning for Vehicle Re-identification." ArXiv abs/1905.08997 (2021): n. pag.
- Zheng, Dingyuan, Jimin Xiao, Kaizhu Huang and Yao Zhao. "Segmentation Mask Guided End-to-End Person Search." ArXiv abs/1908.10179 (2020): n. pag.
- Zheng, Feng, Cheng Deng, Xing Sun, Xinyang Jiang, Xiaowei Guo, Zongqiao Yu, Feiyue Huang and Rongrong Ji. "Pyramidal Person Re-IDentification via Multi-Loss Dynamic Training." 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2019): 8506-8514.
- Zheng, Kecheng, Cuiling Lan, Wenjun Zeng, Jiawei Liu, Zhizheng Zhang and Zhengjun Zha. "Pose-Guided Feature Learning with Knowledge Distillation for Occluded Person Re-Identification." Proceedings of the 29th ACM International Conference on Multimedia (2021): n. pag.
- Zheng, Kecheng, Cuiling Lan, Wenjun Zeng, Zhizheng Zhang and Zhengjun Zha. "Exploiting Sample Uncertainty for Domain Adaptive Person Re-Identification." ArXiv abs/2012.08733 (2021): n. pag.
- Zheng, Kecheng, Jiawei Liu, Wei Wu, Liang Li and Zhengjun Zha. "Calibrated Feature Decomposition for Generalizable Person Re-Identification." ArXiv abs/2111.13945 (2021): n. pag.
- Zheng, Kecheng, Wu Liu, Lingxiao He, Tao Mei, Jiebo Luo and Zhengjun Zha. "Group-aware Label Transfer for Domain Adaptive Person Re-identification." 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2021): 5306-5315.

- Zheng, Liang, Hengheng Zhang, Shaoyan Sun, Manmohan Chandraker, Yi Yang and Qi Tian. “Person Re-identification in the Wild.” 2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (2017): 3346-3355.
- Zheng, Liang, Yi Yang and Alexander Hauptmann. “Person Re-identification: Past, Present and Future.” ArXiv abs/1610.02984 (2016): n. pag.
- Zheng, Liang, Yujia Huang, Huchuan Lu and Yi Yang. “Pose-Invariant Embedding for Deep Person Re-Identification.” IEEE Transactions on Image Processing 28 (2019): 4500-4509.
- Zheng, Meng, Srikrishna Karanam and Richard J. Radke. “Measuring the Temporal Behavior of Real-World Person Re-Identification.” ArXiv abs/1808.05499 (2018): n. pag.
- Zheng, Meng, Srikrishna Karanam, Terrence Chen, Richard J. Radke and Ziyan Wu. “Towards Visually Explaining Similarity Models.” ArXiv abs/2008.06035 (2020): n. pag.
- Zheng, Meng, Srikrishna Karanam, Terrence Chen, Richard J. Radke and Ziyan Wu. “Visual Similarity Attention.” (2019).
- Zheng, Meng, Srikrishna Karanam, Ziyan Wu and Richard J. Radke. “Re-Identification With Consistent Attentive Siamese Networks.” 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2019): 5728-5737.
- Zheng, Y., “Multi-Level Attention for Unsupervised Person Re-Identification.” ArXivabs/2201.03141 (2022): n. pag.
- Zheng, Zhedong, Liang Zheng and Yi Yang. “A Discriminatively Learned CNN Embedding for Person Reidentification.” ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM) 14 (2018): 1 - 20.
- Zheng, Zhedong, Liang Zheng and Yi Yang. “Pedestrian Alignment Network for Large-scale Person Re-Identification.” IEEE Transactions on Circuits and Systems for Video Technology 29 (2019): 3037-3045.
- Zheng, Zhedong, Liang Zheng and Yi Yang. “Unlabeled Samples Generated by GAN Improve the Person Re-identification Baseline in Vitro.” 2017 IEEE International Conference on Computer Vision (ICCV) (2017): 3774-3782.
- Zheng, Zhedong, Nenggan Zheng and Yi Yang. “Parameter-Efficient Person Re-identification in the 3D Space.” arXiv: Computer Vision and Pattern Recognition (2020): n. pag.
- Zheng, Zhedong, Tao Ruan, Yunchao Wei, Yi Yang and Tao Mei. “VehicleNet: Learning Robust Visual Representation for Vehicle Re-Identification.” IEEE Transactions on Multimedia 23 (2021): 2683-2693.
- Zheng, Zhedong, Xiaodong Yang, Zhiding Yu, Liang Zheng, Yi Yang and Jan Kautz. “Joint Discriminative and Generative Learning for Person Re-Identification.” 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2019): 2133-2142.
- Zhong, Yin, Xiaoyu Wang and Shiliang Zhang. “Robust Partial Matching for Person Search in the Wild.” 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2020): 6826-6834.
- Zhong, Zhun, Liang Zheng, Donglin Cao and Shaozi Li. “Re-ranking Person Re-identification with k-Reciprocal Encoding.” 2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)(2017): 3652-3661.

- Zhong, Zhun, Liang Zheng, Guoliang Kang, Shaozi Li and Yi Yang. “Random Erasing Data Augmentation.” AAAI (2020).
- Zhong, Zhun, Liang Zheng, Zhedong Zheng, Shaozi Li and Yi Yang. “Camera Style Adaptation for Person Re-identification.” 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition (2018): 5157-5166.
- Zhong, Zhun, Liang Zheng, Zhiming Luo, Shaozi Li and Yezhou Yang. “Learning to Adapt Invariance in Memory for Person Re-Identification.” IEEE Transactions on Pattern Analysis and Machine Intelligence 43 (2021): 2723-2738.
- Zhong, Zhun, Liang Zheng, Zhiming Luo, Shaozi Li and Yi Yang. “Invariance Matters: Exemplar Memory for Domain Adaptive Person Re-Identification.” 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2019): 598-607.
- Zhou, Hongpeng, Chahine Ibrahim and Wei Pan. “A Sparse Bayesian Deep Learning Approach for Identification of Cascaded Tanks Benchmark.” ArXiv abs/1911.06847 (2019): n. pag.
- Zhou, Jieming, Soumava Kumar Roy, Pengfei Fang, Mehrtash Tafazzoli Harandi and Lars Petersson. “Cross-Correlated Attention Networks for Person Re-Identification.” ArXivabs/2006.09597 (2020): n. pag.
- Zhou, Jun, Yuhang Lu, Kang Zheng, Karen Smith, Colin Wilder and Song Wang. “Design Identification of Curve Patterns on Cultural Heritage Objects: Combining Template Matching and CNN-based Re-Ranking.” ArXiv abs/1805.06862 (2018): n. pag.
- Zhou, Kaiyang and Tao Xiang. “Torchreid: A Library for Deep Learning Person Re-Identification in Pytorch.” ArXiv abs/1910.10093 (2019): n. pag.
- Zhou, Kaiyang, Yongxin Yang, Andrea Cavallaro and Tao Xiang. “Learning Generalisable Omni-Scale Representations for Person Re-Identification.” IEEE transactions on pattern analysis and machine intelligence PP (2021): n. pag.
- Zhou, Kaiyang, Yongxin Yang, Andrea Cavallaro and Tao Xiang. “Omni-Scale Feature Learning for Person Re-Identification.” 2019 IEEE/CVF International Conference on Computer Vision (ICCV)(2019): 3701-3711.
- Zhou, Mengxin, Hongye Liu, Zhekun Lv, Weiheng Hong and Xiai Chen. “Motion-Aware Transformer For Occluded Person Re-identification.” ArXiv abs/2202.04243 (2022): n. pag.
- Zhou, Qin, Heng Fan, Hang Su, Hua Yang, Shibao Zheng and Haibin Ling. “Weighted Bilinear Coding over Salient Body Parts for Person Re-identification.” ArXiv abs/1803.08580 (2020): n. pag.
- Zhou, Qin, Heng Fan, Hua Yang, Hang Su, Shibao Zheng, Shuang Wu and Haibin Ling. “Robust and Efficient Graph Correspondence Transfer for Person Re-Identification.” IEEE Transactions on Image Processing 30 (2021): 1623-1638.
- Zhou, Qin, Heng Fan, Shibao Zheng, Hang Su, Xinzhe Li, Shuang Wu and Haibin Ling. “Graph Correspondence Transfer for Person Re-identification.” ArXiv abs/1804.00242 (2018): n. pag.
- Zhou, Sanping, Jinjun Wang, Deyu Meng, Xiaomeng Xin, Yubing Li, Yihong Gong and Nanning Zheng. “Deep self-paced learning for person re-identification.” ArXiv abs/1710.05711 (2018): n. pag.
- Zhou, Sanping, Jinjun Wang, Deyu Meng, Yudong Liang, Yihong Gong and Nanning Zheng. “Discriminative Feature Learning With Foreground Attention for

Person Re-Identification." IEEE Transactions on Image Processing 28 (2019): 4671-4684.
- Zhou, Tianfei, Jianwu Li, Xueyi Li and Ling Shao. "Target-Aware Object Discovery and Association for Unsupervised Video Multi-Object Segmentation." 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2021): 6981-6990.
- Zhou, Yunhao, Yi Wang and Lap-Pui Chau. "Moving Towards Centers: Re-ranking with Attention and Memory for Re-identification." ArXiv abs/2105.01447 (2021): n. pag.
- Zhu, Fuqing, Xiangwei Kong, Haiyan Fu and Qi Tian. "Pseudo-positive regularization for deep person re-identification." Multimedia Systems 24 (2017): 477-489.
- Zhu, Fuqing, Xiangwei Kong, Liang Zheng, Haiyan Fu and Qi Tian. "Part-Based Deep Hashing for Large-Scale Person Re-Identification." IEEE Transactions on Image Processing 26 (2017): 4806-4817.
- Zhu, Hao, Yang Yuan, Guosheng Hu, Xiang Wu and Neil Martin Robertson. "Imbalance Robust Softmax for Deep Embeeding Learning." ArXiv abs/2011.11155 (2020): n. pag.
- Zhu, Haowei, Wenjing Ke, Dong Li, Ji Liu, Lu Tian and Yi Shan. "Dual Cross-Attention Learning for Fine-Grained Visual Categorization and Object Re-Identification." ArXiv abs/2205.02151 (2022): n. pag.
- Zhu, Jianqing, H. Zeng, Jingchang Huang, Shengcai Liao, Zhen Lei, Canhui Cai and Lixin Zheng. "Vehicle Re-Identification Using Quadruple Directional Deep Learning Features." IEEE Transactions on Intelligent Transportation Systems 21 (2020): 410-420.
- Zhu, Jianqing, H. Zeng, Shengcai Liao, Zhen Lei, Canhui Cai and Lixin Zheng. "Deep Hybrid Similarity Learning for Person Re-Identification." IEEE Transactions on Circuits and Systems for Video Technology 28 (2018): 3183-3193.
- Zhu, Kuan, Haiyun Guo, Shiliang Zhang, Yaowei Wang, Gaopan Huang, Honglin Qiao, Jing Liu, Jinqiao Wang and Ming Tang. "AAformer: Auto-Aligned Transformer for Person Re-Identification." ArXiv abs/2104.00921 (2021): n. pag.
- Zhu, Kuan, Haiyun Guo, Tianyi Yan, Yousong Zhu, Jinqiao Wang and Ming Tang. "PASS: Part-Aware Self-Supervised Pre-Training for Person Re-Identification." (2022).
- Zhu, Kuan, Haiyun Guo, Zhiwei Liu, Ming Tang and Jinqiao Wang. "Identity-Guided Human Semantic Parsing for Person Re-Identification." ArXiv abs/2007.13467 (2020): n. pag.
- Zhu, Lei, Qi She, Duo Li, Yanye Lu, Xuejing Kang, Jie Hu and Changhu Wang. "Unifying Nonlocal Blocks for Neural Networks." 2021 IEEE/CVF International Conference on Computer Vision (ICCV)(2021): 12272-12281.
- Zhu, Lei, Qi She, Lidan Zhang and Ping Guo. "A Spectral Nonlocal Block for Neural Networks." ArXiv abs/1911.01059 (2019): n. pag.
- Zhu, Rixing, Jianwu Fang, Hongke Xu, Hongkai Yu and Jianru Xue. "DCDLearn: Multi-order Deep Cross-distance Learning for Vehicle Re-Identification." ArXiv abs/2003.11315 (2020): n. pag.
- Zhu, Xiangping, Pietro Morerio and Vittorio Murino. "Unsupervised Domain-Adaptive Person Re-Identification Based on Attributes." 2019 IEEE International Conference on Image Processing (ICIP) (2019): 4110-4114.

- Zhu, Xiangping, Xiatian Zhu, Minxian Li, Pietro Morerio, Vittorio Murino and Shaogang Gong. “Intra-Camera Supervised Person Re-Identification.” Int. J. Comput. Vis. 129 (2021): 1580-1595.
- Zhu, Xiangping, Xiatian Zhu, Minxian Li, Vittorio Murino and Shaogang Gong. “Intra-Camera Supervised Person Re-Identification: A New Benchmark.” 2019 IEEE/CVF International Conference on Computer Vision Workshop (ICCVW) (2019): 1079-1087.
- Zhu, Xiangyu, Zhenbo Luo, Pei Fu and Xiang Ji. “VOC-RelD: Vehicle Re-identification based on Vehicle-Orientation-Camera.” 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW) (2020): 2566-2573.
- Zhu, Yuanxin, Zhao Yang, Li Wang, Sai Zhao, Xiao Hu and Dapeng Tao. “Hetero-Center Loss for Cross-Modality Person Re-Identification.” Neurocomputing 386 (2020): 97-109.
- Zhu, Zhen, Tengteng Huang, Baoguang Shi, Miao Yu, Bofei Wang and Xiang Bai. “Progressive Pose Attention Transfer for Person Image Generation.” 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2019): 2342-2351.
- Zhu, Zhen, Tengteng Huang, Mengde Xu, Baoguang Shi, Wenqing Cheng and Xiang Bai. “Progressive and Aligned Pose Attention Transfer for Person Image Generation.” IEEE transactions on pattern analysis and machine intelligence PP (2021): n. pag.
- Zhu, Zhihui, Xinyang Jiang, Feng Zheng, Xiao-Wei Guo, Feiyue Huang, Weishi Zheng and Xing Sun. “Viewpoint-Aware Loss with Angular Regularization for Person Re-Identification.” AAAI (2020).
- Zhuang, Weiming, Xin Gan, Yonggang Wen and Shuai Zhang. “Optimizing Performance of Federated Person Re-identification: Benchmarking and Analysis.” ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM) (2022): n. pag.
- Zhuang, Weiming, Yonggang Wen and Shuai Zhang. “Joint Optimization in Edge-Cloud Continuum for Federated Unsupervised Person Re-identification.” Proceedings of the 29th ACM International Conference on Multimedia (2021): n. pag.
- Zhuang, Weiming, Yonggang Wen, Xuesen Zhang, Xin Gan, Daiying Yin, Dongzhan Zhou, Shuai Zhang and Shuai Yi. “Performance Optimization of Federated Person Re-identification via Benchmark Analysis.” Proceedings of the 28th ACM International Conference on Multimedia (2020): n. pag.
- Zhuang, Zijie, Haizhou Ai, Long Chen and Chong Shang. “Cross-Resolution Person Re-identification with Deep Antithetical Learning.” ArXiv abs/1810.10221 (2018): n. pag.
- Zhuang, Zijie, Longhui Wei, Lingxi Xie, Tianyu Zhang, Hengheng Zhang, Haozhe Wu, Haizhou Ai and Qi Tian. “Rethinking the Distribution Gap of Person Re-identification with Camera-Based Batch Normalization.” ECCV (2020).
- Zhuge, Chaoran, Yujie Peng, Yadong Li, Jiangbo Ai and Junru Chen. “Attribute-guided Feature Extraction and Augmentation Robust Learning for Vehicle Re-identification.” 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW) (2020): 2632-2637.

- Zhuo, Jiaxuan, Jianhuang Lai and Peijia Chen. “A Novel Teacher-Student Learning Framework For Occluded Person Re-Identification.” ArXiv abs/1907.03253 (2019): n. pag.
- Zhuo, Jiaxuan, Zeyu Chen, Jianhuang Lai and Guangcong Wang. “Occluded Person Re-Identification.” 2018 IEEE International Conference on Multimedia and Expo (ICME) (2018): 1-6.
- Zimmer, Ephraim, Christian Burkert, Tom Petersen and Hannes Federrath. “PEEPLL: privacy-enhanced event pseudonymisation with limited linkability.” Proceedings of the 35th Annual ACM Symposium on Applied Computing (2020): n. pag.
- Zou, Yang, Xiaodong Yang, Zhiding Yu, B. V. K. Vijaya Kumar and Jan Kautz. “Joint Disentangling and Adaptation for Cross-Domain Person Re-Identification.” ArXiv abs/2007.10315 (2020): n. pag.
- Zwattendorfer, Bernd and Daniel Slamanig. “The Austrian eID ecosystem in the public cloud: How to obtain privacy while preserving practicality.” J. Inf. Secur. Appl. 27-28 (2016): 35-53.

Annex III: Singling out

- Aggarwal, Abhinav, Shiva Prasad Kasiviswanathan, Zekun Xu, Oluwaseyi Feyisetan and Nathanael Teissier. “Reconstructing Test Labels from Noisy Loss Functions.” AISTATS (2022).
- Akram, Raja Naeem, Iakovos Gurulian, Carlton Shepherd, Konstantinos Markantonakis and Keith Mayes. “Empirical Evaluation of Ambient Sensors as Proximity Detection Mechanism for Mobile Payments.” ArXiv abs/1601.07101 (2016): n. pag.
- Almeida, Paulo José Fernandes and Diego Napp Avelli. “A new class of convolutional codes and its use in the McEliece Cryptosystem.” ArXiv abs/1804.08955 (2018): n. pag.
- Altay, Ayca, Melike Baykal-Gürsoy and Pernille Hemmer. “Behavior Associations in Lone-Actor Terrorists.” Terrorism and Political Violence (2020): n. pag.
- Amerini, Irene, Tiberio Uricchio, Lamberto Ballan and Roberto Caldelli. “Localization of JPEG Double Compression Through Multi-domain Convolutional Neural Networks.” 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW) (2017): 1865-1871.
- Arcolezi, Héber H., Jean-François Couchot, Bechara al Bouna and Xiaokui Xiao. “Random Sampling Plus Fake Data: Multidimensional Frequency Estimates With

Local Differential Privacy." Proceedings of the 30th ACM International Conference on Information & Knowledge Management(2021): n. pag.
- Avizheh, Sepideh, Reihaneh Safavi-Naini and Siamak Fayyaz Shahandashti. "A New Look at the Refund Mechanism in the Bitcoin Payment Protocol." Financial Cryptography (2018).
- Bala, Rajni, Sooryansh Asthana and Vasumathy Ravishankar. "Contextuality-based quantum conferencing." Quantum Inf. Process. 20 (2021): 352.
- Balliu, Musard, Mads Dam and Roberto Guanciale. "InSpectre: Breaking and Fixing Microarchitectural Vulnerabilities by Formal Analysis." Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (2020): n. pag.
- Baussnern, Samuel von, J. Otterbach, Adrian Loy, Mathieu Salzmann and Thomas Wollmann. "DAAIN: Detection of Anomalous and Adversarial Input using Normalizing Flows." ArXivabs/2105.14638 (2021): n. pag.
- Beelen, Peter, Martin Bossert, Sven Puchinger and Johan Sebastian Rosenkilde. "Structural Properties of Twisted Reed-Solomon Codes with Applications to Cryptography." 2018 IEEE International Symposium on Information Theory (ISIT) (2018): 946-950.
- Bensalem, Mounir, Ítalo Barbosa Brasileiro, André C. Drummond and Admela Jukan. "Embedding Jamming Attacks into Physical Layer Models in Optical Networks." 2020 International Conference on Optical Network Design and Modeling (ONDM) (2020): 1-6.
- Bhagoji, Arjun Nitin, Supriyo Chakraborty, Prateek Mittal and Seraphin B. Calo. "Analyzing Federated Learning through an Adversarial Lens." ICML (2019).
- Bhandari, Shweta, Wafa Ben Jaballah, Vineeta Jain, Vijay Laxmi, Akka Zemmari, Manoj Singh Gaur, Mohamed Mosbah and Mauro Conti. "Android inter-app communication threats and detection techniques." Comput. Secur. 70 (2017): 392-421.
- Breuer, Peter T. and Jonathan P. Bowen. "A First Practical Fully Homomorphic Crypto-Processor Design: The Secret Computer is Nearly Here." ArXiv abs/1510.05278 (2015): n. pag.
- Burruss, Matthew P., Shreyas Ramakrishna and A. Dubey. "Deep-RBF Networks for Anomaly Detection in Automotive Cyber-Physical Systems." 2021 IEEE International Conference on Smart Computing (SMARTCOMP) (2021): 55-60.
- Chien, Tzu-Chiao, Olivia T. Lanes, C. Liu, X. Cao, Pinlei Lu, S. Motz, G. Liu, David Pekker and Michael J. Hatridge. "Multiparametric amplification and qubit measurement with a Kerr-free Josephson ring modulator." Physical Review A (2020): n. pag.
- Chowdhary, Ankur, Sailik Sengupta, Dijiang Huang and S. Kambhampati. "Markov Game Modeling of Moving Target Defense for Strategic Detection of Threats in Cloud Networks." ArXivabs/1812.09660 (2018): n. pag.
- Cohen, Aloni and Kobbi Nissim. "Towards formalizing the GDPR's notion of singling out." Proceedings of the National Academy of Sciences of the United States of America 117 (2020): 8344 - 8352.
- Cohen, Aloni. "Attacks on Deidentification's Defenses." ArXiv abs/2202.13470 (2022): n. pag.
- Costa, Gabriele and Andrea Valenza. "Why Charles Can Pen-test: an Evolutionary Approach to Vulnerability Testing." ArXiv abs/2011.13213 (2020): n. pag.
- Cozzolino, Davide, Matthias Nießner and Luisa Verdoliva. "Audio-Visual Person-of-Interest DeepFake Detection." ArXiv abs/2204.03083 (2022): n. pag.

- Craven, Matthew J. and John Robert Woodward. “Evolution of group-theoretic cryptology attacks using hyper-heuristics.” Journal of Mathematical Cryptology 16 (2021): 49 - 63.
- Datta, Prerit, Natalie R. Lodinger, Akbar Siami Namin and Keith S. Jones. “Cyber-Attack Consequence Prediction.” ArXiv abs/2012.00648 (2020): n. pag.
- D’Costa, Daryll Ralph and Robert Abbas. “5G enabled Mobile Edge Computing security for Autonomous Vehicles.” ArXiv abs/2202.00005 (2022): n. pag.
- Dias, Micael A. and Francisco Marcos de Assis. “Evaluating the Eavesdropper Entropy via Bloch-Messiah Decomposition.” 2021 IEEE Conference on Communications and Network Security (CNS)(2021): 1-6.
- Do, Kien, Haripriya Harikumar, Hung Le, Dung Nguyen, T. Tran, Santu Rana, Dang Nguyen, Willy Susilo and Svetha Venkatesh. “Towards Effective and Robust Neural Trojan Defenses via Input Filtering.” ArXiv abs/2202.12154 (2022): n. pag.
- Duy, Phan The, Hien Do Hoang, Do Thi Thu Hien, Anh Gia-Tuan Nguyen and Van-Hau Pham. “B-DAC: A Decentralized Access Control Framework on Northbound Interface for Securing SDN Using Blockchain.” J. Inf. Secur. Appl. 64 (2022): 103080.
- Elkoumy, Gamal, Alisa Pankova and Marlon Dumas. “Differentially Private Release of Event Logs for Process Mining.” ArXiv abs/2201.03010 (2022): n. pag.
- Elkoumy, Gamal, Alisa Pankova and Marlon Dumas. “Mine Me but Don’t Single Me Out: Differentially Private Event Logs for Process Mining.” 2021 3rd International Conference on Process Mining (ICPM) (2021): 80-87.
- Elkoumy, Gamal, Alisa Pankova and Marlon Dumas. “Privacy-Preserving Directly-Follows Graphs: Balancing Risk and Utility in Process Mining.” ArXiv abs/2012.01119 (2020): n. pag.
- Fabris, Marco and Daniel Zelazo. “Secure Consensus via Objective Coding: Robustness Analysis to Channel Tampering.” ArXiv abs/2107.04276 (2022): n. pag.
- Fett, Daniel, Ralf Küsters and Guido Schmitz. “A Comprehensive Formal Security Analysis of OAuth 2.0.” Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (2016): n. pag.
- Fett, Daniel, Ralf Küsters and Guido Schmitz. “The Web SSO Standard OpenID Connect: In-depth Formal Security Analysis and Security Guidelines.” 2017 IEEE 30th Computer Security Foundations Symposium (CSF) (2017): 189-202.
- Fine, Joel, Kirill Krasnov and Dmitri Panov. “A gauge theoretic approach to Einstein 4-manifolds.” arXiv: Differential Geometry (2013): n. pag.
- Fischer, Florian, Matthew Niedermaier, Thomas Hanka, Peter Knauer and Dominik Merli. “Analysis of Industrial Device Architectures for Real-Time Operations under Denial of Service Attacks.” ICICS (2020).
- Fredes, Luis, Amitai Linker and Daniel Remenik. “Coexistence for a population model with forest fire epidemics.” (2018).
- Frigo, Pietro, Emanuele Vannacci, Hasan Hassan, Victor van der Veen, Onur Mutlu, Cristiano Giuffrida, Herbert Bos and Kaveh Razavi. “TRRespass: Exploiting the Many Sides of Target Row Refresh.” 2020 IEEE Symposium on Security and Privacy (SP) (2020): 747-762.
- Gao, Ruiyuan, Ming Dun, Hailong Yang, Zhongzhi Luan and Depei Qian. “Privacy for Rescue: A New Testimony Why Privacy is Vulnerable In Deep Models.” ArXiv abs/2001.00493 (2020): n. pag.
- Geng, Maojie, Tianhong Xu, Ying Chen and Tian-Yu Ye. “Semiquantum Private Comparison of Size Relationship Based on d-level Single-Particle States.” (2022).

- Geng, Maojie, Ying Chen, Tianhong Xu and Tian-Yu Ye. “Single-state semiquantum private comparison based on Bell states.” (2021).
- Gosain, Devashish, Anshika Agarwal, Sahil Shekhawat, Hrishikesh B. Acharya and Sambuddho Chakravarty. “Mending Wall: On the Implementation of Censorship in India.” ArXivabs/1806.06518 (2017): n. pag.
- Groza, Bogdan. “Traffic models with adversarial vehicle behaviour.” ArXiv abs/1701.07666 (2017): n. pag.
- Guo, Shangwei, Tianwei Zhang, Han-Zhou Yu, Xiaofei Xie, L. Ma, Tao Xiang and Yang Liu. “Byzantine-Resilient Decentralized Stochastic Gradient Descent.” IEEE Transactions on Circuits and Systems for Video Technology 32 (2022): 4096-4106.
- Hachimi, Marouane, Georges Kaddoum, Ghyslain Gagnon and Poulmanogo Illy. “Multi-stage Jamming Attacks Detection using Deep Learning Combined with Kernelized Support Vector Machine in 5G Cloud Radio Access Networks.” 2020 International Symposium on Networks, Computers and Communications (ISNCC) (2020): 1-5.
- Hada, Suryabhan Singh, Miguel ‘A. Carreira-Perpin’an and Arman Zharmagambetov. “Sparse Oblique Decision Trees: A Tool to Understand and Manipulate Neural Net Features.” ArXivabs/2104.02922 (2021): n. pag.
- Harks, Tobias, Mona Henle, Max Klimm, Jannik Matuschke and Anja Schedel. “Multi-Leader Congestion Games with an Adversary.” ArXiv abs/2112.07435 (2021): n. pag.
- Hong, Sanghyun, Michael Panaitescu-Liess, Yigitcan Kaya and Tudor Dumitras. “Qu-ANTI-zation: Exploiting Quantization Artifacts for Achieving Adversarial Outcomes.” ArXiv abs/2110.13541 (2021): n. pag.
- Hosp, Julian, Toby Hoenisch and Paul Kittiwongsunthorn. “COMIT - Cryptographically-secure Off-chain Multi-asset Instant Transaction Network.” ArXiv abs/1810.02174 (2018): n. pag.
- Huang, Ke-Wen, Huiming Wang, Yongpeng Wu and Robert Schober. “Pilot Spoofing Attack by Multiple Eavesdroppers.” IEEE Transactions on Wireless Communications 17 (2018): 6433-6447.
- Huber, Manuel, Stefan Hristozov, Simon Ott, Vasil Sarafov and Marcus Peinado. “The Lazarus Effect: Healing Compromised Devices in the Internet of Small Things.” Proceedings of the 15th ACM Asia Conference on Computer and Communications Security (2020): n. pag.
- Islam, Saad, Koksal Mus, Richa Singh, Patrick Schaumont and Berk Sunar. “Signature Correction Attack on Dilithium Signature Scheme.” ArXiv abs/2203.00637 (2022): n. pag.
- Jia, Yunhan, Yantao Lu, Junjie Shen, Qi Alfred Chen, Zhenyu Zhong and Tao Wei. “Fooling Detection Alone is Not Enough: First Adversarial Attack against Multiple Object Tracking.” ArXivabs/1905.11026 (2019): n. pag.
- Koch, Julia and Christian Reitwießner. “A Predictable Incentive Mechanism for TrueBit.” ArXivabs/1806.11476 (2018): n. pag.
- Krawiecka, Klaudia, Simon Birnbach, Simon Eberz and Ivan Martinovic. “BeeHIVE: Behavioral Biometric System based on Object Interactions in Smart Environments.” ArXiv abs/2202.03845 (2022): n. pag.
- Kumar, Kuraganti Chetan, Paul Robert Bryan, Gurunath Gurrala, Ashish Joglekar, Arun Babu Puthuparambil, Rajesh Sundaresan and Himanshu Tyagi. “A Distributed Hierarchy Framework for Enhancing Cyber Security of Control Center Applications.” ArXiv abs/2010.04955 (2020): n. pag.

- Leiba, Oded, Yechiav Yitzchak, Ron Bitton, Asaf Nadler and Asaf Shabtai. “Incentivized Delivery Network of IoT Software Updates Based on Trustless Proof-of-Distribution.” 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (2018): 29-39.
- Li, Weikang, Sirui Lu and Dong-Ling Deng. “Quantum federated learning through blind quantum computing.” Science China Physics, Mechanics & Astronomy 64 (2021): 1-8.
- Li, Xirong, Yang Zhou, Jie Wang, Hailan Lin, Jianchun Zhao, Dayong Ding, Weihong Yu and You-xin Chen. “Multi-Modal Multi-Instance Learning for Retinal Disease Recognition.” Proceedings of the 29th ACM International Conference on Multimedia (2021): n. pag.
- Liu, Li-juan, Zhihui Li, Zhaowei Han and Dan-Li Zhi. “A quantum secret sharing scheme with verifiable function.” The European Physical Journal D 74 (2020): 1-8.
- Lou, Yang, Yaodong He, Lin Wang, Kim Fung Tsang and Guanrong Chen. “Knowledge-Based Prediction of Network Controllability Robustness.” IEEE transactions on neural networks and learning systems PP (2021): n. pag.
- Meißner, Dominik, Frank Kargl and Benjamin Erb. “WAIT: protecting the integrity of web applications with binary-equivalent transparency.” Proceedings of the 36th Annual ACM Symposium on Applied Computing (2021): n. pag.
- Mosafi, Itay, Eli David and Nathan S. Netanyahu. “Stealing Knowledge from Protected Deep Neural Networks Using Composite Unlabeled Data.” 2019 International Joint Conference on Neural Networks (IJCNN) (2019): 1-8.
- Naha, Arunava, André M. H. Teixeira, Anders Ahlén and Subhrakanti Dey. “Quickest Detection of Deception Attacks in Networked Control Systems with Physical Watermarking.” (2021).
- Nautsch, Andreas, Xin Wang, Nicholas W. D. Evans, Tomi H. Kinnunen, Ville Vestman, Massimiliano Todisco, Héctor Delgado, Md. Sahidullah, Junichi Yamagishi and Kong-Aik Lee. “ASVspoof 2019: Spoofing Countermeasures for the Detection of Synthesized, Converted and Replayed Speech.” IEEE Transactions on Biometrics, Behavior, and Identity Science 3 (2021): 252-265.
- Nguyen, Binh Van, Minh Tuan Nguyen, Hyoyoung Jung and Kiseon Kim. “Designing Anti-Jamming Receivers for NR-DCSK Systems Utilizing ICA, WPD, and VMD Methods.” IEEE Transactions on Circuits and Systems II: Express Briefs 66 (2019): 1522-1526.
- Pan, Yanjun, Yao Zheng and Ming Li. “ROBin: Known-Plaintext Attack Resistant Orthogonal Blinding via Channel Randomization.” IEEE INFOCOM 2020 - IEEE Conference on Computer Communications (2020): 1927-1936.
- Pazos, José Carlos, Jean-Sébastien Légaré, Ivan Beschastnikh and William Aiello. “Precise XSS detection and mitigation with Client-side Templates.” ArXiv abs/2005.07826 (2020): n. pag.
- Rahman, Mohammad Ashiqur, Md Hasan Shahriar, Mohamadsaleh Jafari and Rahat Masum. “Novel Attacks against Contingency Analysis in Power Grids.” ArXiv abs/1911.00928 (2019): n. pag.
- Rajput, Mohit Narayan and Maroti Deshmukh. “A Technique to Share Multiple Secret Images.” ArXiv abs/1611.09261 (2016): n. pag.
- Raponi, Simone and Roberto Di Pietro. “A Longitudinal Study on Web-Sites Password Management (in)Security: Evidence and Remedies.” IEEE Access 8 (2020): 52075-52090.

- Ravikumar, Deepak, Sangamesh Kodge, Isha Garg and Kaushik Roy. “TREND: Transferability based Robust ENsemble Design.” ArXiv abs/2008.01524 (2022): n. pag.
- Rodríguez, Sandra Servia, Liang Wang, Jianxin R. Zhao, Richard Mortier and Hamed Haddadi. “Privacy-Preserving Personal Model Training.” 2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI) (2018): 153-164.
- Salehghaffari, Hossein and Mahdiyeh Khodaparastan. “Hardware-In-The-Loop Vulnerability Analysis of a Single-Machine Infinite-Bus Power System.” 2019 IEEE Power & Energy Society General Meeting (PESGM) (2019): 1-5.
- Salwey, Benno and Stefan Wolf. “Stronger attacks on causality-based key agreement.” 2016 IEEE International Symposium on Information Theory (ISIT) (2016): 2254-2258.
- Sanjab, Anibal and Walid Saad. “Data Injection Attacks on Smart Grids With Multiple Adversaries: A Game-Theoretic Perspective.” IEEE Transactions on Smart Grid 7 (2016): 2038-2049.
- Santos, Daniel Ricardo dos, Mario Dagrada and Elisa Costante. “Leveraging operational technology and the Internet of things to attack smart buildings.” Journal of Computer Virology and Hacking Techniques 17 (2020): 1-20.
- Satvat, Kiavash, Maliheh Shirvanian and Nitesh Saxena. “PASSAT: Single Password Authenticated Secret-Shared Intrusion-Tolerant Storage with Server Transparency.” ArXiv abs/2102.13607 (2021): n. pag.
- Sengupta, Sailik and S. Kambhampati. “Multi-agent Reinforcement Learning in Bayesian Stackelberg Markov Games for Adaptive Moving Target Defense.” ArXiv abs/2007.10457 (2020): n. pag.
- Singh, Jag Mohan and Raghavendra Ramachandra. “3D Face Morphing Attacks: Generation, Vulnerability and Detection.” (2022).
- Soni, Rahul, Naresh Shah and Jimmy D. Moore. “Fine-grained Uncertainty Modeling in Neural Networks.” ArXiv abs/2002.04205 (2020): n. pag.
- Wu, Zhenyu, Haotao Wang, Zhaowen Wang, Hailin Jin and Zhangyang Wang. “Privacy-Preserving Deep Action Recognition: An Adversarial Learning Framework and A New Dataset.” IEEE Transactions on Pattern Analysis and Machine Intelligence 44 (2022): 2126-2139.
- Xiang, Chong, Alexander Valtchanov, Saeed Mahloujifar and Prateek Mittal. “ObjectSeeker: Certifiably Robust Object Detection against Patch Hiding Attacks via Patch-agnostic Masking.” ArXiv abs/2202.01811 (2022): n. pag.
- Xu, Tianhong, Ying Chen, Maojie Geng and Tian-Yu Ye. “Single-state multi-party semiquantum key agreement protocol based on multi-particle GHZ entangled states.” (2021).
- Zhang, Cong, Jerzy Lewandowski and Yongge Ma. “Towards the self-adjointness of a Hamiltonian operator in loop quantum gravity.” Physical Review D (2018): n. pag.
- Zhang, Haijian. “A Time-Frequency Perspective on Audio Watermarking.” ArXiv abs/2002.03156 (2020): n. pag.
- Zhao, Zhengyu, Zhuoran Liu and Martha Larson. “Adversarial Robustness Against Image Color Transformation within Parametric Filter Space.” ArXiv abs/2011.06690 (2020): n. pag.

- Zheng, Tianming, Ming Liu, Deepak Puthal, P. Yi, Yue Wu and Xiangjian He. “Smart Grid: Cyber Attacks, Critical Defense Approaches, and Digital Twin.” ArXiv abs/2205.11783 (2022): n. pag.
- Ziegler, Daniel M., Seraphina Nix, Lawrence Chan, Tim Bauman, Peter Schmidt-Nielsen, Tao Lin, Adam Scherlis, Noa Nabeshima, Ben Weinstein-Raun, Daniel Haas, Buck Shlegeris and Nate Thomas. “Adversarial Training for High-Stakes Reliability.” ArXiv abs/2205.01663 (2022): n. pag.
- Zuo, Pengfei, Yu Hua, Cong Wang, Wen Xia, Shunde Cao, Yukun Zhou and Yuanyuan Sun. “Bandwidth-efficient Storage Services for Mitigating Side Channel Attack.” ArXiv abs/1703.05126 (2017): n. pag.

Annex IV: Linkage

- Aalibagi, Soroush, Hamidreza Mahyar, Ali Movaghar and Harry Eugene Stanley. “A Matrix Factorization Model for Hellinger-based Trust Management in Social Internet of Things.” arXiv: Learning (2019): n. pag.
- Abrath, Bert, Bart Coppens, Jens Van den Broeck, Brecht Wyseur, Alessandro Cabutto, Paolo Falcarin and Bjorn De Sutter. “Code Renewability for Native Software Protection.” ACM Transactions on Privacy and Security (TOPS) 23 (2020): 1 - 31.
- Adhatarao, Supriya and Cédric Lauradoux. “Exploitation and Sanitization of Hidden Data in PDF Files: Do Security Agencies Sanitize Their PDF Files?” Proceedings of the 2021 ACM Workshop on Information Hiding and Multimedia Security (2021): n. pag.
- Afaq, Amir, Zeeshan Ahmed, Noman Haider and Muhammad Imran. “Blockchain-based Collaborated Federated Learning for Improved Security, Privacy and Reliability.” ArXivabs/2201.08551 (2022): n. pag.

- Alavijeh, Mohammad Aghababaie, Behrouz Maham, Zhu Han and Walid Saad. “Truthful spectrum auction for efficient anti-jamming in cognitive radio networks.” 2017 IEEE Symposium on Computers and Communications (ISCC) (2017): 742-747.
- Aldaghri, Nasser and Hessam Mahdavifar. “Physical Layer Secret Key Generation in Static Environments.” IEEE Transactions on Information Forensics and Security 15 (2020): 2692-2705.
- Algaba, Encarnación, Andrea Prieto and Alejandro Saavedra-Nieves. “Rankings in the Zerkani network by a game theoretical approach.” ArXiv abs/2202.07730 (2022): n. pag.
- Alhawi, Omar M. K., Mustafa A. Mustafa and Lucas C. Cordeiro. “Finding Security Vulnerabilities in Unmanned Aerial Vehicles Using Software Verification.” 2019 International Workshop on Secure Internet of Things (SIOT) (2019): 1-9.
- Almeira, Nahuel, Orlando Vito Billoni and Juan Ignacio Perotti. “Scaling of percolation transitions on Erdös-Rényi networks under centrality-based attacks.” Physical review. E 101 1-1 (2020): 012306 .
- Al-Mousa, Mohammad Rasmi. “Analyzing Cyber-Attack Intention for Digital Forensics Using Case-Based Reasoning.” ArXiv abs/2101.01395 (2021): n. pag.
- Alnasser, Aljawharah and Hongjian Sun. “Global Roaming Trust-based Model for V2X Communications.” IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (2019): 1-6.
- Alrahis, Lilas, Satwik Patnaik, Muhammad Abdullah Hanif, Muhammad Shafique and Ozgur Sinanoglu. “UNTANGLE: Unlocking Routing and Logic Obfuscation Using Graph Neural Networks-based Link Prediction.” 2021 IEEE/ACM International Conference On Computer Aided Design (ICCAD) (2021): 1-9.
- Alrahis, Lilas, Satwik Patnaik, Muhammad Shafique and Ozgur Sinanoglu. “MuxLink: Circumventing Learning-Resilient MUX-Locking Using Graph Neural Network-based Link Prediction.” 2022 Design, Automation & Test in Europe Conference & Exhibition (DATE) (2022): 694-699.
- Anderson, Adam Lane, Steven R. Young, Frederick K. Reed and Jason M. Vann. “Deep Modulation (Deepmod): A Self-Taught PHY Layer for Resilient Digital Communications.” arXiv: Signal Processing (2019): n. pag.
- Anzo-Hern’andez, A., E. Campos-Cant’on and Matthew Nicol. “Itinerary synchronization in a network of nearly identical PWL systems coupled with unidirectional links and ring topology.” (2018).
- Apthorpe, Noah J., Danny Yuxing Huang, Dillon Reisman, Arvind Narayanan and Nick Feamster. “Keeping the Smart Home Private with Smart(er) IoT Traffic Shaping.” Proceedings on Privacy Enhancing Technologies 2019 (2019): 128 - 148.
- Assion, Felix, Peter Schlicht, Florens Greßner, Wiebke Günther, Fabian Hüger, Nico M. Schmidt and Umair Rasheed. “The Attack Generator: A Systematic Approach Towards Constructing Adversarial Attacks.” 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW) (2019): 1370-1379.
- Aubel, Pol Van and Erik Poll. “Security of EV-Charging Protocols.” ArXiv abs/2202.04631 (2022): n. pag.
- Avatefipour, Omid, Azeem Hafeez, Muhammad Tayyab and Hafiz Malik. “Linking received packet to the transmitter through physical-fingerprinting of controller area network.” 2017 IEEE Workshop on Information Forensics and Security (WIFS) (2017): 1-6.

- Aydeger, Abdullah, Mohammad Hossein Manshaei, Mohammad Ashiqur Rahman and Kemal Akkaya. “Strategic Defense Against Stealthy Link Flooding Attacks: A Signaling Game Approach.” IEEE Transactions on Network Science and Engineering 8 (2021): 751-764.
- Backes, Michael, Mathias Humbert, Jun Pang and Yang Zhang. “walk2friends: Inferring Social Links from Mobility Profiles.” Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (2017): n. pag.
- Bagheri, Pegah and Milad Dehghani Filabadi. “Robust-and-Cheap Framework for Network Resilience: A Novel Mixed-Integer Formulation and Solution Method.” (2021).
- Bao, Zijian, Wenbo Shi, Saru Kumari, Zhiyin Kong and Chien-Ming Chen. “Lockmix: a secure and privacy-preserving mix service for Bitcoin anonymity.” International Journal of Information Security 19 (2019): 311-321.
- Baral, Gitanjali and Nalin Asanka Gamagedara Arachchilage. “Building Confidence not to be Phished Through a Gamified Approach: Conceptualising User’s Self-Efficacy in Phishing Threat Avoidance Behaviour.” 2019 Cybersecurity and Cyberforensics Conference (CCC) (2019): 102-110.
- Barchinezhad, Soheila and Mohammad Sayad Haghighi. “Compensation of Linear Attacks to Cyber Physical Systems through ARX System Identification.” ArXiv abs/2002.05798 (2020): n. pag.
- Basta, Nardine, Ming Ding, Muhammad Ikram and Mohamed Ali Kâafar. “5G-Enabled Pseudonymity for Cooperative Intelligent Transportation System.” ArXiv abs/2203.10673 (2022): n. pag.
- Basu, Debraj, Tianbo Gu and Prasant Mohapatra. “Security Issues of Low Power Wide Area Networks in the Context of LoRa Networks.” ArXiv abs/2006.16554 (2020): n. pag.
- Batool, Komal and Muaz A. Niazi. “Tamper-Evident Complex Genomic Networks.” ArXivabs/1708.05926 (2017): n. pag.
- Behzadan, Vahid. “Cyber-Physical Attacks on UAS Networks- Challenges and Open Research Problems.” ArXiv abs/1702.01251 (2017): n. pag.
- Bellingeri, Michele, Daniele Bevacqua, Francesco Scotognella and Davide Cassi. “Abrupt efficiency collapse in real-world complex weighted networks: robustness decrease with link weights heterogeneity.” arXiv: Physics and Society (2019): n. pag.
- Bensalem, Mounir, Ítalo Barbosa Brasileiro, André C. Drummond and Admela Jukan. “Embedding Jamming Attacks into Physical Layer Models in Optical Networks.” 2020 International Conference on Optical Network Design and Modeling (ONDM) (2020): 1-6.
- B’eres, Ferenc, István András Seres, Andr’as A. Bencz’ur and Mikerah Quintyne-Collins. “Blockchain is Watching You: Profiling and Deanonymizing Ethereum Users.” 2021 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS) (2021): 69-78.
- Bertagnolli, Giulia, Riccardo Gallotti and Manlio De Domenico. “Quantifying efficient information exchange in real network flows.” arXiv: Physics and Society (2020): n. pag.
- Berthelot, Geoffroy, Liubov Tupikina, Min-Yeong Kang, B. Sapoval and Denis S. Grebenkov. “Pseudo-Darwinian evolution of physical flows in complex networks.” Scientific Reports 10 (2020): n. pag.

- Bhardwaj, Peru, John D. Kelleher, Luca Costabello and Declan O'Sullivan. "Adversarial Attacks on Knowledge Graph Embeddings via Instance Attribution Methods." ArXiv abs/2111.03120 (2021): n. pag.
- Bhardwaj, Peru, John D. Kelleher, Luca Costabello and Declan O'Sullivan. "Poisoning Knowledge Graph Embeddings via Relation Inference Patterns." ArXiv abs/2111.06345 (2021): n. pag.
- Bianchi, Gabriele. "The covariogram and Fourier–Laplace transform in ℂn." Proceedings of the London Mathematical Society 113 (2013): n. pag.
- Biondi, Pietro, Stefano Bognanni and Giampaolo Bella. "Vulnerability Assessment and Penetration Testing on IP cameras." ArXiv abs/2202.06597 (2022): n. pag.
- Blackburn, Alyssa, Christoph Huber, Yossi Eliaz, Muhammad Saad Shamim, David Weisz, Goutham Seshadri, Kevin N. Kim, S.-H. hang and Erez Lieberman Aiden. "Cooperation among an anonymous group protected Bitcoin during failures of decentralization." ArXiv abs/2206.02871 (2022): n. pag.
- Bober-Irizar, Mikel, Ilia Shumailov, Yiren Zhao, Robert D. Mullins and Nicolas Papernot. "Architectural Backdoors in Neural Networks." ArXiv abs/2206.07840 (2022): n. pag.
- Boche, Holger, Minglai Cai, Christian Deppe and Janis Noetzel. "Classical-quantum arbitrarily varying wiretap channel: Secret message transmission under jamming attacks." 2017 IEEE International Symposium on Information Theory (ISIT) (2017): 1983-1987.
- Bojovic, Petar D. and K. Savic. "Analiza bezbednosnih mehanizama OSPF protokola." ArXivabs/1712.00775 (2017): n. pag.
- Bonneau, Haggai, Ofer Biham, Reimer Kühn and Eytan Katzav. "Statistical analysis of edges and bredges in configuration model networks." Physical review. E 102 1-1 (2020): 012314 .
- Botero, Juan Diego, Weisi Guo, Guillem Mosquera, Alan Wilson, Samuel Johnson, Gicela A Aguirre-Garcia and Leonardo A Pachón. "Gang confrontation: The case of Medellin (Colombia)." PLoS ONE 14 (2019): n. pag.
- Boualouache, Abdelwahab, Sidi-Mohammed Senouci and Samira Moussaoui. "A Survey on Pseudonym Changing Strategies for Vehicular Ad-Hoc Networks." IEEE Communications Surveys & Tutorials 20 (2018): 770-790.
- Boumezbeur, Mouna, Sihem Mesnager and Kenza Guenda. "Vectorial Boolean functions and linear codes in the context of algebraic attacks." ArXiv abs/1801.01145 (2018): n. pag.
- Bradley, Stuart. "Realistic DNA Deanonymization using Phenotypic Prediction." ArXivabs/1607.07501 (2016): n. pag.
- Brasileiro, Ítalo Barbosa, Mounir Bensalem, André C. Drummond and Admela Jukan. "Jamming-Aware Control Plane in Elastic Optical Networks." ArXiv abs/2006.02896 (2020): n. pag.
- Brasser, Ferdinand, Srdjan Capkun, Alexandra Dmitrienko, Tommaso Frassetto, Kari Kostiainen, Urs Müller and Ahmad-Reza Sadeghi. "DR.SGX: Hardening SGX Enclaves against Cache Attacks with Data Location Randomization." ArXiv abs/1709.09917 (2019): n. pag.
- Breier, Jakub, Adrian Baldwin, Helen Balinsky and Yang Liu. "Risk Management Framework for Machine Learning Security." ArXiv abs/2012.04884 (2020): n. pag.

- Broeck, Jens Van den, Bart Coppens and Bjorn De Sutter. “Extended Report on the Obfuscated Integration of Software Protections.” ArXiv abs/1907.01445 (2019): n. pag.
- Buci’c, Matija and Benny Sudakov. “Large independent sets from local considerations.” arXiv: Combinatorics (2020): n. pag.
- Buttar, Hasan Mujtaba, Waqas Aman, M. Mahboob Ur Rahman and Qammer Hussain Abbasi. “Countering Active Attacks on RAFT-based IoT Blockchain Networks.” ArXiv abs/2204.00838 (2022): n. pag.
- Byrenheid, Martin, Stefanie Roos and Thorsten Strufe. “Topology Inference of Networks utilizing Rooted Spanning Tree Embeddings.” 23rd International Conference on Distributed Computing and Networking (2022): n. pag.
- Casiraghi, Giona, Antonios Garas and Frank Schweitzer. “Probing the robustness of nested multi-layer networks.” ArXiv abs/1911.03277 (2019): n. pag.
- Catarineu, Alex, Philipp Claßen, Konark Modi and Josep M. Pujol. “Preventing Attacks on Anonymous Data Collection.” ArXiv abs/1812.07927 (2018): n. pag.
- Cetinkaya, Ahmet, Hideaki Ishii and Tomohisa Hayakawa. “A Probabilistic Characterisation of Random and Malicious Communication Failures in Multi-Hop Networked Control.” SIAM J. Control. Optim. 56 (2018): 3320-3350.
- Cetinkaya, Ahmet, Hideaki Ishii and Tomohisa Hayakawa. “Event-triggered control over unreliable networks subject to jamming attacks.” 2015 54th IEEE Conference on Decision and Control (CDC)(2015): 4818-4823.
- Cetinkaya, Ahmet, Hideaki Ishii and Tomohisa Hayakawa. “Networked Control Under Random and Malicious Packet Losses.” IEEE Transactions on Automatic Control 62 (2017): 2434-2449.
- Cevallos, Alfonso and Alistair Stewart. “A verifiably secure and proportional committee election rule.” Proceedings of the 3rd ACM Conference on Advances in Financial Technologies (2021): n. pag.
- Charlier, Jérémy, Radu State and Jean Hilger. “Modeling Smart Contracts Activities: A Tensor Based Approach.” ArXiv abs/1905.09868 (2019): n. pag.
- Chatterjee, Atanu, Man Singh Manohar and Gitakrishnan Ramadurai. “Statistical Analysis of Bus Networks in India.” PLoS ONE 11 (2016): n. pag.
- Chatterjee, Atanu, Man Singh Manohar and Gitakrishnan Ramadurai. “Statistical Analysis of Bus Networks in India.” PLoS ONE 11 (2016): n. pag.
- Cheema, Muhammad Asaad, Muhammad Karam Shehzad, Hassaan Khaliq Qureshi, Syed Ali Hassan and Haejoon Jung. “A Drone-Aided Blockchain-Based Smart Vehicular Network.” IEEE Transactions on Intelligent Transportation Systems 22 (2021): 4160-4170.
- Chen, Dongyao, Kyong-Tak Cho and Kang G. Shin. “Mobile IMUs Reveal Driver’s Identity From Vehicle Turns.” ArXiv abs/1710.04578 (2017): n. pag.
- Chen, Jinyin, Dunjie Zhang, Zhaoyan Ming, Kejie Huang, Wenrong Jiang and Chen Cui. “GraphAttacker: A General Multi-Task Graph Attack Framework.” IEEE Transactions on Network Science and Engineering 9 (2022): 577-595.
- Chen, Jinyin, Haiyang Xiong, Haibin Zheng, Jian Zhang, Guodong Jiang and Yi Liu. “Dyn-Backdoor: Backdoor Attack on Dynamic Link Prediction.” ArXiv abs/2110.03875 (2021): n. pag.
- Chen, Jinyin, Jian Zhang, Zhi Ying Chen, Min Du and Qi Xuan. “Time-aware Gradient Attack on Dynamic Network Link Prediction.” ArXiv abs/1911.10561 (2021): n. pag.

- Chen, Jinyin, Xiang Lin, Dunjie Zhang, Wenrong Jiang, Guohan Huang, Hui Xiong and Yun Xiang. “Graphfool: Targeted Label Adversarial Attack on Graph Embedding.” ArXiv abs/2102.12284 (2022): n. pag.
- Chen, Jinyin, Xiang Lin, Ziqiang Shi and Yi Liu. “Link Prediction Adversarial Attack Via Iterative Gradient Attack.” IEEE Transactions on Computational Social Systems 7 (2020): 1081-1094.
- Chen, Jinyin, Yangyang Wu, Xiang Lin and Qi Xuan. “Can Adversarial Network Attack be Defended?” ArXiv abs/1903.05994 (2019): n. pag.
- Chen, Jinyin, Yangyang Wu, Xuanheng Xu, Yixian Chen, Haibin Zheng and Qi Xuan. “Fast Gradient Attack on Network Embedding.” ArXiv abs/1809.02797 (2018): n. pag.
- Chen, Jinyin, Yixian Chen, Haibin Zheng, Shijing Shen, Shanqing Yu, Dan Zhang and Qi Xuan. “MGA: Momentum Gradient Attack on Network.” IEEE Transactions on Computational Social Systems 8 (2021): 99-109.
- Chen, Jinyin, Yixian Chen, Lihong Chen, M. Zhao and Qi Xuan. “Multiscale Evolutionary Perturbation Attack on Community Detection.” IEEE Transactions on Computational Social Systems 8 (2021): 62-75.
- Chen, Juntao, Corinne Touati and Quanyan Zhu. “A Dynamic Game Analysis and Design of Infrastructure Network Protection and Recovery.” ACM SIGMETRICS Performance Evaluation Review 45 (2017): 128.
- Chen, Juntao, Corinne Touati and Quanyan Zhu. “A Dynamic Game Approach to Strategic Design of Secure and Resilient Infrastructure Network.” IEEE Transactions on Information Forensics and Security 15 (2020): 462-474.
- Chen, Juntao, Corinne Touati and Quanyan Zhu. “Optimal Secure Two-Layer IoT Network Design.” IEEE Transactions on Control of Network Systems 7 (2020): 398-409.
- Chen, Liang, Jintang Li, Jiaying Peng, Tao Xie, Zengxu Cao, Kun Xu, Xiangnan He and Zibin Zheng. “A Survey of Adversarial Learning on Graphs.” ArXiv abs/2003.05730 (2020): n. pag.
- Chen, Xi, Bo Kang, Jefrey Lijffijt and Tijl De Bie. “Adversarial Robustness of Probabilistic Network Embedding for Link Prediction.” PKDD/ECML Workshops (2021).
- Chen, Xiaofeng and Yinghu Gao. “CDEdit: A Highly Applicable Redactable Blockchain with Controllable Editing Privilege and Diversified Editing Types.” ArXiv abs/2205.07054 (2022): n. pag.
- Chen, Zekai, Dingshuo Chen, Zixuan Yuan, Xiuzhen Cheng and Xiao Zhang. “Learning Graph Structures With Transformer for Multivariate Time-Series Anomaly Detection in IoT.” IEEE Internet of Things Journal 9 (2022): 9179-9189.
- Chowdhury, Nilanjan Roy, Nandini Negi and Aranya Chakrabortty. “A New Cyber-Secure Countermeasure for LTI systems under DoS attacks.” 2019 27th Mediterranean Conference on Control and Automation (MED) (2019): 304-309.
- Chuat, Laurent, Cyrill Krähenbühl, Prateek Mittal and Adrian Perrig. “F-PKI: Enabling Innovation and Trust Flexibility in the HTTPS Public-Key Infrastructure.” ArXiv abs/2108.08581 (2022): n. pag.
- Ciaian, Pavel, d’Artis Kancs and Miroslava Rajcaniova. “Interdependencies between Mining Costs, Mining Rewards and Blockchain Security.” ArXiv abs/2102.08107 (2021): n. pag.
- Conti, Mauro, Pallavi Kaliyar and Chhagan Lal. “Reliable Group Communication Protocol for Internet of Things.” ArXiv abs/1904.04542 (2019): n. pag.

- Cotret, Pascal, Guy Gogniat and Martha Johanna Sepúlveda. “Protection of heterogeneous architectures on FPGAs: An approach based on hardware firewalls.” Microprocess. Microsystems42 (2016): 127-141.
- Courtès, Ludovic. “Building a Secure Software Supply Chain with GNU Guix.” ArXivabs/2206.14606 (2022): n. pag.
- Dahan, Mathieu and Saurabh Amin. “Network flow routing under strategic link disruptions.” 2015 53rd Annual Allerton Conference on Communication, Control, and Computing (Allerton) (2015): 353-360.
- Dahan, Mathieu and Saurabh Amin. “Security Games in Network Flow Problems.” ArXivabs/1601.07216 (2016): n. pag.
- Dai, Jiazhu, Weifeng Zhu and Xiangfeng Luo. “A Targeted Universal Attack on Graph Convolutional Network.” ArXiv abs/2011.14365 (2022): n. pag.
- Dai, Tianxiang, Philipp Jeitner, Haya Shulman and Michael Waidner. “The Hijackers Guide To The Galaxy: Off-Path Taking Over Internet Resources.” ArXiv abs/2205.05473 (2021): n. pag.
- Dailly, Antoine, Valentin Gledel and Marc Heinrich. “A generalization of Arc-Kayles.” International Journal of Game Theory 48 (2019): 491-511.
- Damer, Naser, K. Bommanna Raja, Marius Sussmilch, Sushma Krupa Venkatesh, Fadi Boutros, Meiling Fang, Florian Kirchbuchner, Raghavendra Ramachandra and Arjan Kuijper. “ReGenMorph: Visibly Realistic GAN Generated Face Morphing Attacks by Attack Re-generation.” ISVC (2021).
- Darabseh, Ala and Christina Pöpper. “Towards Security-Optimized Placement of ADS-B Sensors.” Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks (2022): n. pag.
- Darwish, Kareem, Walid Magdy and Tahar Zanouda. “Trump vs. Hillary: What Went Viral During the 2016 US Presidential Election.” SocInfo (2017).
- Das, Siddhartha Shankar, Edoardo Serra, Mahantesh Halappanavar, Alex Pothen and Ehab Al-Shaer. “V2W-BERT: A Framework for Effective Hierarchical Multiclass Classification of Software Vulnerabilities.” 2021 IEEE 8th International Conference on Data Science and Advanced Analytics (DSAA) (2021): 1-12.
- Dax, Alexander and Robert Künnemann. “On the Soundness of Infrastructure Adversaries.” 2021 IEEE 34th Computer Security Foundations Symposium (CSF) (2021): 1-16.
- Demontis, Ambra, Marco Melis, Battista Biggio, Davide Maiorca, Dan Arp, Konrad Rieck, Igino Corona, Giorgio Giacinto and Fabio Roli. “Yes, Machine Learning Can Be More Secure! A Case Study on Android Malware Detection.” IEEE Transactions on Dependable and Secure Computing16 (2019): 711-724.
- Demontis, Ambra, Paolo Russu, Battista Biggio, Giorgio Fumera and Fabio Roli. “On Security and Sparsity of Linear Classifiers for Adversarial Settings.” S+SSPR (2016).
- Derkach, Ivan and Vladyslav C. Usenko. “Applicability of Squeezed- and Coherent-State Continuous-Variable Quantum Key Distribution over Satellite Links.” Entropy 23 (2021): n. pag.
- Desfontaines, Damien, Esfandiar Mohammadi, Elisabeth Krahmer and David A. Basin. “Differential privacy with partial knowledge.” arXiv: Cryptography and Security (2019): n. pag.
- Diaz, Alejandra, Alan T. Sherman and Anupam Joshi. “Phishing in an academic community: A study of user susceptibility and behavior.” Cryptologia 44 (2020): 53 - 67.

- Dibaji, Seyed Mehran, Hideaki Ishii and Roberto Tempo. “Resilient Randomized Quantized Consensus.” IEEE Transactions on Automatic Control 63 (2018): 2508-2522.
- Ding, Hu, Fan Yang and Jiawei Huang. “Defending SVMs against poisoning attacks: the hardness and DBSCAN approach.” UAI (2021).
- Ding, Xuyang, Feng Xiao, Man Zhou and Zhibo Wang. “Active Link Obfuscation to Thwart Link-flooding Attacks for Internet of Things.” 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) (2020): 217-224.
- Dionelis, Nikolaos. “FROB: Few-shot ROBust Model for Classification and Out-of-Distribution Detection.” ArXiv abs/2111.15487 (2021): n. pag.
- Dixit, Siddharth, Meghna Chaudhary and Niteesh Sahni. “Network Learning Approaches to study World Happiness.” ArXiv abs/2007.09181 (2020): n. pag.
- Dorri, Ali, Clemence Roulin, Shantanu Pal, Sarah Baalbaki, Raja Jurdak and Salil S. Kanhere. “Device Identification in Blockchain-Based Internet of Things.” ArXiv abs/2202.09603 (2022): n. pag.
- Duddu, Vasisht, Antoine Boutet and Virat Shejwalkar. “Quantifying Privacy Leakage in Graph Embedding.” MobiQuitous 2020 - 17th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (2020): n. pag.
- Dwivedi, Rudresh and Somnath Dey. “A non-invertible cancelable fingerprint template generation based on ridge feature transformation.” ArXiv abs/1805.10853 (2018): n. pag.
- El Shafie, Ahmed, Kamel Tourki, Zhiguo Ding and Naofal Al-Dhahir. “Probabilistic Jamming/Eavesdropping Attacks to Confuse a Buffer-Aided Transmitter–Receiver Pair.” IEEE Communications Letters 21 (2017): 1549-1552.
- El-Korashy, Akram, Stelios Tsampas, Marco Patrignani, Dominique Devriese, Deepak Garg and Frank Piessens. “CapablePtrs: Securely Compiling Partial Programs Using the Pointers-as-Capabilities Principle.” 2021 IEEE 34th Computer Security Foundations Symposium (CSF) (2021): 1-16.
- Ellers, Michael, Michael Cochez, Tobias Schumacher, Markus Strohmaier and Florian Lemmerich. “Privacy Attacks on Network Embeddings.” ArXiv abs/1912.10979 (2019): n. pag.
- Elmendili, Fatna, Nisrine Maqran, Younès El Bouzekri El Idrissi and Habiba Chaoui. “A security approach based on honeypots: Protecting Online Social network from malicious profiles.” ArXivabs/1804.09988 (2018): n. pag.
- Eltayeb, Mohammed E., Junil Choi, Tareq Y. Al-Naffouri and Robert W. Heath. “Enhancing Secrecy With Multiantenna Transmission in Millimeter Wave Vehicular Communication Systems.” IEEE Transactions on Vehicular Technology 66 (2017): 8139-8151.
- Eltayeb, Mohammed E., Junil Choi, Tareq Y. Al-Naffouri and Robert W. Heath. “On the Security of Millimeter Wave Vehicular Communication Systems Using Random Antenna Subsets.” 2016 IEEE 84th Vehicular Technology Conference (VTC-Fall) (2016): 1-5.
- Erni, Simon, Martin Kotuliak, Patrick Leu, Marc Roschlin and Srdjan vCapkun. “AdaptOver: Adaptive Overshadowing Attacks in Cellular Networks.” (2021).
- Esposito, Sergio, Daniele Sgandurra and Giampaolo Bella. “ALEXA VERSUS ALEXA: Controlling Smart Speakers by Self-Issuing Voice Commands.” Proceedings

of the 2022 ACM on Asia Conference on Computer and Communications Security (2022): n. pag.
- Eu, Sen-Peng, Tung-Shan Fu, Yu-Chang Liang and Tsai-Lien Wong. “On xD-Generalizations of Stirling Numbers and Lah Numbers via Graphs and Rooks.” Electron. J. Comb. 24 (2017): 2.
- Fabris, Marco and Daniel Zelazo. “Secure Consensus via Objective Coding: Robustness Analysis to Channel Tampering.” ArXiv abs/2107.04276 (2022): n. pag.
- Faghri, Fartash, Cristina Nader Vasconcelos, David J. Fleet, Fabian Pedregosa and Nicolas Le Roux. “Bridging the Gap Between Adversarial Robustness and Optimization Bias.” ArXivabs/2102.08868 (2021): n. pag.
- Fan, Houxiang, Binghui Wang, Pan Zhou, Ang Li, Meng Pang, Zichuan Xu, Cai Fu, Hai Helen Li and Yiran Chen. “Reinforcement Learning-based Black-Box Evasion Attacks to Link Prediction in Dynamic Graphs.” 2021 IEEE 23rd Int Conf on High Performance Computing & Communications; 7th Int Conf on Data Science & Systems; 19th Int Conf on Smart City; 7th Int Conf on Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys) (2021): 933-940.
- Fang, Meiling, Fadi Boutros, Arjan Kuijper and Naser Damer. “Partial Attack Supervision and Regional Weighted Inference for Masked Face Presentation Attack Detection.” 2021 16th IEEE International Conference on Automatic Face and Gesture Recognition (FG 2021) (2021): 1-8.
- Fanti, Giulia C., Shaileshh Bojja Venkatakrishnan, Surya Bakshi, Bradley Denby, Shruti Bhargava, Andrew K. Miller and Pramod Viswanath. “Dandelion++: Lightweight Cryptocurrency Networking with Formal Anonymity Guarantees.” Abstracts of the 2018 ACM International Conference on Measurement and Modeling of Computer Systems (2018): n. pag.
- Farach-Colton, Lucas, Martin Farach-Colton, Leslie Ann Goldberg, John Lapinskas, Reut Levi, Moti Medina and Miguel A. Mosteiro. “Improved Distortion and Spam Resistance for PageRank.” arXiv: Data Structures and Algorithms (2018): n. pag.
- Fauvelle, Jean-Philippe, Alexandre Dey and Sylvain Navers. “Protection of an information system by artificial intelligence: a three-phase approach based on behaviour analysis to detect a hostile scenario.” ArXiv abs/1812.00622 (2018): n. pag.
- Ferdowsi, Aidin, Ursula Challita, Walid Saad and Narayan B. Mandayam. “Robust Deep Reinforcement Learning for Security and Safety in Autonomous Vehicle Systems.” 2018 21st International Conference on Intelligent Transportation Systems (ITSC) (2018): 307-312.
- Fernando, Matheesha and Nalin Asanka Gamagedara Arachchilage. “Why Johnny can’t rely on anti-phishing educational interventions to protect himself against contemporary phishing attacks?” ArXiv abs/2004.13262 (2020): n. pag.
- Fine, Joel, Kirill Krasnov and Dmitri Panov. “A gauge theoretic approach to Einstein 4-manifolds.” arXiv: Differential Geometry (2013): n. pag.
- Fu, Lan, Qing Guo, Felix Juefei-Xu, Hongkai Yu, Wei Feng, Yang Liu and Song Wang. “Benchmarking Shadow Removal for Facial Landmark Detection and Beyond.” ArXivabs/2111.13790 (2021): n. pag.
- Fujiwara, Mikio, Atsushi Waseda, Ryo Nojima, Shiho Moriai, Wakaha Ogata and Masahide Sasaki. “Unbreakable distributed storage with quantum key distribution network and password-authenticated secret sharing.” Scientific Reports 6 (2016): n. pag.

- G'alvez, Waldo, Francisco Sanhueza-Matamala and José A. Soto. "Approximation Algorithms for Vertex-Connectivity Augmentation on the Cycle." WAOA (2021).
- Gan, Yujian, Xinyun Chen, Qiuping Huang, Matthew Purver, John Robert Woodward, Jinxia Xie and Pengsheng Huang. "Towards Robustness of Text-to-SQL Models against Synonym Substitution." ACL (2021).
- Gao, Xiaolin, Cunlai Pu and Lunbo Li. "Cost Restrained Hybrid Attacks in Power Grids." ArXivabs/2006.12282 (2020): n. pag.
- Gao, Zhan, Elvin Isufi and Alejandro Ribeiro. "Variance-Constrained Learning for Stochastic Graph Neural Networks." ICASSP 2021 - 2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (2021): 5245-5249.
- García-Escartín, Juan Carlos and Pedro Chamorro-Posada. "Hidden Probe Attacks on Ultralong Fiber Laser Key Distribution Systems." IEEE Journal of Selected Topics in Quantum Electronics 24 (2018): 1-9.
- Garrad, P. N. and Shane Gilroy. "Developments in Connected Vehicles and the Requirement for Increased Cybersecurity." ArXiv abs/2111.11612 (2021): n. pag.
- Garrido, Josep Soler, Dominik Dold and Johannes Frank. "Machine learning on knowledge graphs for context-aware security monitoring." 2021 IEEE International Conference on Cyber Security and Resilience (CSR) (2021): 55-60.
- Gehrke, Alexander and Karen Mulleners. "Phenomenology and scaling of optimal flapping wing kinematics." Bioinspiration & Biomimetics 16 (2020): n. pag.
- Ghavasieh, Arsham, Massimo Stella, Jacob D. Biamonte and Manlio De Domenico. "Unraveling the effects of multiscale network entanglement on empirical systems." Communications Physics4 (2020): 1-10.
- Ghawash, Faiq and Waseem Abbas. "Leveraging Diversity for Achieving Resilient Consensus in Sparse Networks." ArXiv abs/1907.10742 (2019): n. pag.
- Giacon, Federico, Riccardo Aragona and Massimiliano Sala. "A proof of security for a key-policy RS-ABE scheme." ArXiv abs/1603.06635 (2016): n. pag.
- Gkounis, Dimitrios, Vasileios Kotronis, Christos K. Liaskos and Xenofontas A. Dimitropoulos. "On the Interplay of Link-Flooding Attacks and Traffic Engineering." ArXiv abs/1611.02488 (2016): n. pag.
- Goel, Karan, Nazneen Rajani, Jesse Vig, Samson Tan, Jason M. Wu, Stephan Zheng, Caiming Xiong, Mohit Bansal and Christopher R'e. "Robustness Gym: Unifying the NLP Evaluation Landscape." NAACL (2021).
- Goldfeder, Steven, Harry A. Kalodner, Dillon Reisman and Arvind Narayanan. "When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies." Proceedings on Privacy Enhancing Technologies 2018 (2018): 179 - 199.
- Gong, Kai, Jia-Jian Wu, Qing Li and Yichun Zhu. "The healing strategy by prioritizing minimum degree against localized attacks on interdependent spatially embedded networks." arXiv: Physics and Society (2018): n. pag.
- Gopika, R., Ankita Sharma and Rakesh R. Warier. "Bipartite Consensus in the Presence of Denial of Service Adversary." ArXiv abs/2107.11729 (2022): n. pag.
- Goyal, Sanjeev, Shahin Jabbari, Michael Kearns, Sanjeev Khanna and Jamie H. Morgenstern. "Strategic Network Formation with Attack and Immunization." WINE (2016).
- Gracy, Sebin, Jezdimir Milošević and Henrik Sandberg. "Actuator Security Index for Structured Systems." 2020 American Control Conference (ACC) (2020): 2993-2998.

- Grashöfer, Jan, Peter Oettig, Robin Sommer, Tim Wojtulewicz and Hannes Hartenstein. “Advancing Protocol Diversity in Network Security Monitoring.” ArXiv abs/2106.12454 (2021): n. pag.
- Greschbach, Benjamin, Tobias Pulls, Laura M. Roberts, Philipp Winter and Nick Feamster. “The Effect of DNS on Tor’s Anonymity.” ArXiv abs/1609.08187 (2017): n. pag.
- Grimsman, David, João Pedro Hespanha and Jason R. Marden. “Stackelberg Equilibria for Two-Player Network Routing Games on Parallel Networks.” 2020 American Control Conference (ACC)(2020): 5364-5369.
- Gu, Zhongshu, Hani Jamjoom, Dong Su, Heqing Huang, Jialong Zhang, Tengfei Ma, Dimitrios E. Pendarakis and Ian Molloy. “Reaching Data Confidentiality and Model Accountability on the CalTrain.” 2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) (2019): 336-348.
- Gupta, Suyash, Sajjad Rahnama, Shubham Pandey, Natacha Crooks and Mohammad Sadoghi. “Dissecting BFT Consensus: In Trusted Components we Trust!” ArXiv abs/2202.01354 (2022): n. pag.
- Gupta, Viresh and Tanmoy Chakraborty. “Adversarial Attack on Network Embeddings via Supervised Network Poisoning.” PAKDD (2021).
- Halimi, Anisa and Erman Ayday. “Efficient Quantification of Profile Matching Risk in Social Networks Using Belief Propagation.” ArXiv abs/2009.03698 (2020): n. pag.
- Han, Xiao, Leye Wang, Junjie Wu and Yuncong Yang. “Large-Scale Privacy-Preserving Network Embedding against Private Link Inference Attacks.” ArXiv abs/2205.14440 (2022): n. pag.
- Harsha, Benjamin, Robert Morton, Jeremiah Blocki, John A. Springer and Melissa Jane Dark. “Bicycle Attacks Considered Harmful: Quantifying the Damage of Widespread Password Length Leakage.” Comput. Secur. 100 (2021): 102068.
- Harshan, Jagadeesh, Sang-Yoon Chang and Yih-Chun Hu. “Insider-Attacks on Physical-Layer Group Secret-Key Generation in Wireless Networks.” 2017 IEEE Wireless Communications and Networking Conference (WCNC) (2017): 1-6.
- Hayashi, Yukio, Atsushi Tanaka and Jun Matsukubo. “Effective Self-Healing Networks against Attacks or Disasters in Resource Allocation Control.” ArXiv abs/2008.00651 (2020): n. pag.
- Hayashi, Yukio, Atsushi Tanaka and Jun Matsukubo. “More Tolerant Reconstructed Networks Using Self-Healing against Attacks in Saving Resource.” Entropy 23 (2021): n. pag.
- Hayashi, Yukio. “A new design principle of robust onion-like networks self-organized in growth.” Network Science 6 (2017): 54 - 70.
- Haydari, Ammar, H. Michael Zhang, Chen-Nee Chuah, Jane MacFarlane and Sean Peisert. “Adaptive Differential Privacy Mechanism for Aggregated Mobility Dataset.” ArXivabs/2112.08487 (2021): n. pag.
- He, Xinlei, Jinyuan Jia, Michael Backes, Neil Zhenqiang Gong and Yang Zhang. “Stealing Links from Graph Neural Networks.” ArXiv abs/2005.02131 (2021): n. pag.
- Hemberg, Erik, Jonathan Kelly, Michal Shlapentokh-Rothman, Bryn Reinstadler, Katherine Xu, Nick Rutar and Una-May O’Reilly. “BRON - Linking Attack Tactics, Techniques, and Patterns with Defensive Weaknesses, Vulnerabilities and Affected Platform Configurations.” ArXivabs/2010.00533 (2020): n. pag.

- Hoang, Dinh Thai, Ping Wang, Dusit Tao Niyato and Ekram Hossain. “Charging and Discharging of Plug-In Electric Vehicles (PEVs) in Vehicle-to-Grid (V2G) Systems: A Cyber Insurance-Based Model.” IEEE Access 5 (2017): 732-754.
- Hoang, Linh Manh, Diep N. Nguyen, J.Andrew Zhang and Dinh Thai Hoang. “Multiple Correlated Jammers Nullification using LSTM-based Deep Dueling Neural Network.” (2022).
- Hofbauer, David, Igor Ivkic, Silia Maksuti, Andreas Aldrian and Markus Tauber. “On the Cost of Security Compliance in Information Systems.” ArXiv abs/1905.06122 (2019): n. pag.
- Holohan, Naoise, Spyros Antonatos, Stefano Braghin and Pol Mac Aonghusa. “(k, ε)-Anonymity: k-Anonymity with ε-Differential Privacy.” ArXiv abs/1710.01615 (2017): n. pag.
- Hota, Ashish Ranjan and Shreyas Sundaram. “Interdependent Security Games on Networks Under Behavioral Probability Weighting.” IEEE Transactions on Control of Network Systems 5 (2018): 262-273.
- Hu, Ye, Anibal Sanjab and Walid Saad. “Dynamic Psychological Game Theory for Secure Internet of Battlefield Things (IoBT) Systems.” IEEE Internet of Things Journal 6 (2019): 3712-3726.
- Huang, Ke-Wen, Huiming Wang, Yongpeng Wu and Robert Schober. “Pilot Spoofing Attack by Multiple Eavesdroppers.” IEEE Transactions on Wireless Communications 17 (2018): 6433-6447.
- Huang, Linan and Quanyan Zhu. “Farsighted Risk Mitigation of Lateral Movement Using Dynamic Cognitive Honeypots.” GameSec (2020).
- Huang, Yudi, Ting He, Nilanjan Ray Chaudhuri and Thomas F. La Porta. “Power Grid State Estimation under General Cyber-Physical Attacks.” 2020 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)(2020): 1-6.
- Huang, Yudi, Ting He, Nilanjan Ray Chaudhuri and Thomas F. La Porta. “Verifiable Failure Localization in Smart Grid under Cyber-Physical Attacks.” ArXiv abs/2101.07129 (2021): n. pag.
- Hugues-Salas, Emilio, Foteini Ntavou, Yanni Ou, Jake E. Kennard, Catherine White, Dimitrios Gkounis, Konstantinos Nikolovgenis, George T. Kanellos, Chris Erven, Andrew Lord, Reza Nejabati and Dimitra Simeonidou. “Experimental Demonstration of DDoS Mitigation over a Quantum Key Distribution (QKD) Network Using Software Defined Networking (SDN).” 2018 Optical Fiber Communications Conference and Exposition (OFC) (2018): 1-3.
- Husain, Hisham. “Distributional Robustness with IPMs and links to Regularization and GANs.” ArXiv abs/2006.04349 (2020): n. pag.
- Hussain, Hussain, Tomislav Duricic, E. Lex, D. Helic, Markus Strohmaier and Roman Kern. “Structack: Structure-based Adversarial Attacks on Graph Neural Networks.” Proceedings of the 32nd ACM Conference on Hypertext and Social Media (2021): n. pag.
- Iacobello, Giovanni, Frieder Kaiser and David E. Rival. “Load estimation in unsteady flows from sparse pressure measurements: Application of transition networks to experimental data.” Physics of Fluids (2022): n. pag.
- Ibrahim, Sara Al Hajj and Mohamed El Baker Nassar. “Hack The Box: Fooling Deep Learning Abstraction-Based Monitors.” ArXiv abs/2107.04764 (2021): n. pag.

- Ichinose, Genki, Tomohiro Tsuchiya and Shunsuke Watanabe. “Robustness of football passing networks against continuous node and link removals.” arXiv: Physics and Society (2020): n. pag.
- Indrusiak, Leandro Soares, James Harbin and Martha Johanna Sepúlveda. “Side-channel attack resilience through route randomisation in secure real-time Networks-on-Chip.” 2017 12th International Symposium on Reconfigurable Communication-centric Systems-on-Chip (ReCoSoC)(2017): 1-8.
- Ioannidis, Vassilis N. and Georgios B. Giannakis. “Edge Dithering for Robust Adaptive Graph Convolutional Networks.” ArXiv abs/1910.09590 (2019): n. pag.
- Ioannidis, Vassilis N., Dimitris Berberidis and Georgios B. Giannakis. “GraphSAC: Detecting anomalies in large-scale graphs.” ArXiv abs/1910.09589 (2019): n. pag.
- Islam, Md. Samiul, Md. Mojammel Hossain and Mohammed A. Almukhtar. “A Survey on SDN \& SDCN Traffic Measurement: Existing Approaches and Research Challenge.” ArXivabs/2206.14236 (2022): n. pag.
- Ivanov, Nikolay, Jianzhi Lou, Ting Chen, Jin Li and Qiben Yan. “Targeting the Weakest Link: Social Engineering Attacks in Ethereum Smart Contracts.” Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security (2021): n. pag.
- Jagannath, Anu, Jithin Jagannath and Andrew L. Drozd. “High Rate-Reliability Beamformer Design for 2×2 Mimo-OFDM System Under Hostile Jamming.” 2020 29th International Conference on Computer Communications and Networks (ICCCN) (2020): 1-9.
- Jain, Adarsh, Abhishek Khanna, Jay Bhatt, Parthkumar V. Sakhiya, Shashank Kumar, Rohan S Urdhwareshe and Nilesh M Desai. “Development of NavIC synchronized fully automated inter-building QKD framework and demonstration of quantum secured video calling.” ArXivabs/2111.09716 (2021): n. pag.
- Janak, Jan, Dana Chee, Hema Retty, Artiom Baloian and Henning Schulzrinne. “Talking After Lights Out: An Ad Hoc Network for Electric Grid Recovery.” 2021 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)(2021): 181-187.
- Jang, Rhongho, Seongkwang Moon, Youngtae Noh, Aziz Mohaisen and Daehun Nyang. “Scaling Up Anomaly Detection Using In-DRAM Working Set of Active Flows Table.” ArXiv abs/1902.04143 (2019): n. pag.
- Jasser, Jasser and Ivan I. Garibay. “Resilience from Diversity: Population-based approach to harden models against adversarial attacks.” ArXiv abs/2111.10272 (2021): n. pag.
- Jawaheri, Husam Al, Mashael Al Sabah, Yazan Boshmaf and Aiman Erbad. “When A Small Leak Sinks A Great Ship: Deanonymizing Tor Hidden Service Users Through Bitcoin Transactions Analysis.” Comput. Secur. 89 (2020): n. pag.
- Jedh, Mubark, Lotfi Ben Othmane, Noor O. Ahmed and Bharat K. Bhargava. “Detection of Message Injection Attacks Onto the CAN Bus Using Similarities of Successive Messages-Sequence Graphs.” IEEE Transactions on Information Forensics and Security 16 (2021): 4133-4146.
- Jeitner, Philipp, Haya Shulman and Michael Waidner. “Pitfalls of Provably Secure Systems in Internet the Case of Chronos-NTP.” 2020 50th Annual IEEE-IFIP International Conference on Dependable Systems and Networks-Supplemental Volume (DSN-S) (2020): 49-50.

- Jeitner, Philipp, Haya Shulman and Michael Waidner. “Secure Consensus Generation with Distributed DoH.” 2020 50th Annual IEEE-IFIP International Conference on Dependable Systems and Networks-Supplemental Volume (DSN-S) (2020): 41-42.
- Ji, Shouling, Qinchen Gu, Haiqin Weng, Qianjun Liu, Pan Zhou, Qinming He, Raheem A. Beyah and Ting Wang. “De-Health: All Your Online Health Information Are Belong to Us.” 2020 IEEE 36th International Conference on Data Engineering (ICDE) (2020): 1609-1620.
- Jiang, Wenjun, Run-Ran Liu and Chun-Xiao Jia. “Depth Penetration and Scope Extension of Failures in the Cascading of Multilayer Networks.” Complex. 2020 (2020): 3578736:1-3578736:11.
- Jiang, Zhongyuan, Lichao Sun, Philip S. Yu, Hui Li, Jianfeng Ma and Yulong Shen. “Target Privacy Preserving for Social Networks.” 2020 IEEE 36th International Conference on Data Engineering (ICDE) (2020): 1862-1865.
- Kahlhofer, Mario, Michaela Hölzl and Andreas Berger. “Towards Reconstructing Multi-Step Cyber Attacks in Modern Cloud Environments with Tripwires.” Proceedings of the European Interdisciplinary Cybersecurity Conference (2020): n. pag.
- Kalantari, Ashkan, Gan Zheng, Zhen Gao, Zhu Han and Björn E. Ottersten. “Secrecy Analysis on Network Coding in Bidirectional Multibeam Satellite Communications.” IEEE Transactions on Information Forensics and Security 10 (2015): 1862-1874.
- Karthik, Anantha K. and Rick S. Blum. “Estimation Theory Based Robust Phase Offset Estimation in the Presence of Delay Attacks.” ArXiv abs/1611.05117 (2016): n. pag.
- Kashyap, G. and G. Ambika. “Link deletion in directed complex networks.” Physical A: Statistical Mechanics and its Applications (2019): n. pag.
- Kato, Fumiyuki, Yang Cao and Masatoshi Yoshikawa. “OLIVE: Oblivious and Differentially Private Federated Learning on Trusted Execution Environment.” ArXiv abs/2202.07165 (2022): n. pag.
- Kekatos, Vassilis, G. Wang, Hao Zhu and Georgios B. Giannakis. “PSSE Redux: Convex Relaxation, Decentralized, Robust, and Dynamic Approaches.” ArXiv abs/1708.03981 (2017): n. pag.
- Kepkowski, Michal, Lucjan Hanzlik, Ian D. Wood and Mohamed Ali Kâafar. “How Not to Handle Keys: Timing Attacks on FIDO Authenticator Privacy.” ArXiv abs/2205.08071 (2022): n. pag.
- Keshav, S., Wojciech M. Golab, Bernard Wong, Sajjad Rizvi and Sergey Gorbunov. “RCanopus: Making Canopus Resilient to Failures and Byzantine Faults.” ArXiv abs/1810.09300 (2018): n. pag.
- Khandaker, Muhammad R. A., Christos Masouros and Kai-Kit Wong. “Secure Full-Duplex Device-to-Device Communication.” 2017 IEEE Globecom Workshops (GC Wkshps) (2017): 1-6.
- Khattak, Sheharbano, Laurent Simon and Steven J. Murdoch. “Systemization of Pluggable Transports for Censorship Resistance.” ArXiv abs/1412.7448 (2014): n. pag.
- Khodaei, Mohammad Javad and Panagiotis Papadimitratos. “Cooperative Location Privacy in Vehicular Networks: Why Simple Mix Zones are Not Enough.” IEEE Internet of Things Journal 8 (2021): 7985-8004.
- Kim, Jung-Ho, Soo-Jeong Kim and Kwang-Il Goh. “Critical behaviors of high-degree adaptive and collective-influence percolation.” Chaos 30 7 (2020): 073131 .

- Kish, S. P., Eduardo Villaseñor, Robert A. Malaney, Kerry A. Mudge and K. J. Grant. “Feasibility assessment for practical continuous variable quantum key distribution over the satellite-to-Earth channel.” Quantum Eng. 2 (2020): n. pag.
- Kolbeinsson, Arinbjorn, Jean Kossaifi, Yannis Panagakis, Adrian Bulat, Anima Anandkumar, Ioanna Tzoulaki and Paul Matthews. “Tensor Dropout for Robust Learning.” IEEE Journal of Selected Topics in Signal Processing 15 (2021): 630-640.
- Kolluri, Aashish, Teodora Baluta, Bryan Hooi and Prateek Saxena. “LPGNet: Link Private Graph Networks for Node Classification.” ArXiv abs/2205.03105 (2022): n. pag.
- Kolokotronis, Nicholas, Konstantinos Limniotis, Stavros N. Shiaeles and Romain Griffiths. “Secured by Blockchain: Safeguarding Internet of Things Devices.” IEEE Consumer Electronics Magazine 8 (2019): 28-34.
- Kotnis, Bhushan and Joy Kuri. “Percolation on networks with antagonistic and dependent interactions.” Physical review. E, Statistical, nonlinear, and soft matter physics 91 3 (2015): 032805 .
- Kotuliak, Martin, Simon Erni, Patrick Leu, Marc Roeschlin and Srdjan Capkun. “LTrack: Stealthy Tracking of Mobile Phones in LTE.” ArXiv abs/2106.05007 (2021): n. pag.
- Kotyan, Shashank, Danilo Vasconcellos Vargas and Moe Matsuki. “Representation Quality Of Neural Networks Links To Adversarial Attacks and Defences.” arXiv: Computer Vision and Pattern Recognition (2019): n. pag.
- Kuang, Da, P. Jeffrey Brantingham and A. Bertozzi. “Crime topic modeling.” Crime Science 6 (2017): 1-20.
- Kursuncu, Ugur, Manas Gaur, Carlos Castillo, Amanuel Alambo, Krishnaprasad Thirunarayan, Valerie L. Shalin, Dilshod Achilov, Ismailcem Budak Arpinar and A. Sheth. “Modeling Islamist Extremist Communications on Social Media using Contextual Dimensions.” Proceedings of the ACM on Human-Computer Interaction 3 (2019): 1 - 22.
- Ladisa, Piergiorgio, Henrik Plate, Matias Martinez and Olivier Barais. “Taxonomy of Attacks on Open-Source Software Supply Chains.” ArXiv abs/2204.04008 (2022): n. pag.
- Lakshminarayana, Subhash, Elena Veronica Belmega and H. Vincent Poor. “Moving-Target Defense Against Cyber-Physical Attacks in Power Grids via Game Theory.” IEEE Transactions on Smart Grid 12 (2021): 5244-5257.
- Lakshminarayana, Subhash, Elena Veronica Belmega and H. Vincent Poor. “Moving-Target Defense for Detecting Coordinated Cyber-Physical Attacks in Power Grids.” 2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm) (2019): 1-7.
- Lakshminarayana, Subhash, Jabir Shabbir Karachiwala, Sang-Yoon Chang, Girish Revadigar, Sristi Lakshmi Sravana Kumar, David K. Y. Yau and Yih-Chun Hu. “Signal Jamming Attacks Against Communication-Based Train Control: Attack Impact and Countermeasure.” Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks (2018): n. pag.
- Leavitt, Matthew L. and Ari S. Morcos. “Linking average- and worst-case perturbation robustness via class selectivity and dimensionality.” ArXiv abs/2010.07693 (2020): n. pag.

- Lee, Joon Sern, Gui Peng David Yam and Jin Hao Chan. “PhishGAN: Data Augmentation and Identification of Homoglpyh Attacks.” ArXiv abs/2006.13742 (2020): n. pag.
- Lenzen, Christoph and Julian Loss. “Optimal Clock Synchronization with Signatures.” ArXivabs/2203.02553 (2022): n. pag.
- Li, Jiani and Xenofon D. Koutsoukos. “Resilient Distributed Diffusion for Multi-task Estimation.” 2018 14th International Conference on Distributed Computing in Sensor Systems (DCOSS)(2018): 93-102.
- Li, Kaiya, Guangchun Luo, Yang Ye, Wei Li, Shihao Ji and Zhipeng Cai. “Adversarial Privacy-Preserving Graph Embedding Against Inference Attack.” IEEE Internet of Things Journal 8 (2021): 6904-6915.
- Li, Tao, Yingwen Wu, Sizhe Chen, Kun Fang and Xiaolin Huang. “Subspace Adversarial Training.” ArXiv abs/2111.12229 (2021): n. pag.
- Li, Xiaochen, Weiren Liu, Hanwen Feng, Kunzhe Huang, Yunpeng Hu, Jinfei Liu, Kui Ren and Zhan Qin. “DUMP: A Dummy-point-based Local Differential Privacy Enhancement Approach under the Shuffle Model.” (2021).
- Liaskos, Christos K., Vasileios Kotronis and Xenofontas A. Dimitropoulos. “A novel framework for modeling and mitigating distributed link flooding attacks.” IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications (2016): 1-9.
- Lin, Jian-Hong, Emiliano Marchese, Claudio J. Tessone and Tiziano Squartini. “The Weighted Bitcoin Lightning Network.” SSRN Electronic Journal (2022): n. pag.
- Ling, Chen, Utkucan Balci, Jeremy Blackburn and Gianluca Stringhini. “A First Look at Zoombombing.” 2021 IEEE Symposium on Security and Privacy (SP) (2021): 1452-1467.
- Liu, Ying, Andrey Garnaev and Wade Trappe. “Connectivity jamming game for physical layer attack in peer to peer networks.” Secur. Commun. Networks 9 (2016): 6080-6093.
- Loison, Ant’onio, Th’eo Combey and Hatem Hajri. “Probabilistic Jacobian-based Saliency Maps Attacks.” Mach. Learn. Knowl. Extr. 2 (2020): 558-578.
- Longo, Riccardo, Federico Pintore, Giancarlo Rinaldo and Massimiliano Sala. “On the security of the blockchain BIX protocol and certificates.” 2017 9th International Conference on Cyber Conflict (CyCon) (2017): 1-16.
- Low, Ian, William J. Buchanan, Richard Macfarlane and Owen Lo. “Wi-Fi Channel Saturation as a Mechanism to Improve Passive Capture of Bluetooth Through Channel Usage Restriction.” ArXivabs/2002.05126 (2020): n. pag.
- Lu, Jingyi and Daniel E. Quevedo. “A Jointly Optimal Design of Control and Scheduling in Networked Systems under Denial-of-Service Attacks.” (2021).
- Lu, Yang, Jianming Lian, Minghui Zhu and Ke Ma. “Transactive Energy System Deployment over Insecure Communication Links.” (2020).
- Lu, Yueyun, Chin-Yao Chang, Wei Zhang, Laurentiu Dan Marinovici and Antonio J. Conejo. “On resilience analysis and quantification for wide-area control of power systems.” 2016 IEEE 55th Conference on Decision and Control (CDC) (2016): 5799-5804.
- Luo, Yi, Haokun Mao and Qiong Li. “An Information-theoretical Secured Byzantine-fault Tolerance Consensus in Quantum Key Distribution Network.” ArXiv abs/2204.09832 (2022): n. pag.

- Luo, Zhiqing, Wei Wang, Jiang Xiao, Qianyi Huang, Tao Jiang and Q. Zhang. “Authenticating On-Body Backscatter by Exploiting Propagation Signatures.” Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 2 (2018): 1 - 22.
- Lyu, Bin, Dinh Thai Hoang, Shimin Gong, Dusit Tao Niyato and Dong In Kim. “IRS-Based Wireless Jamming Attacks: When Jammers Can Attack Without Power.” IEEE Wireless Communications Letters 9 (2020): 1663-1667.
- Ma, Qingyin and John Stachurski. “Dynamic Programming Deconstructed: Transformations of the Bellman Equation and Computational Efficiency.” Oper. Res. 69 (2021): 1591-1607.
- Mabodi, Kobra, Mehdi Yusefi, Shahram Zandiyan, Leili Irankhah and Reza Fotohi. “Multi-level trust-based intelligence schema for securing of internet of things (IoT) against security threats using cryptographic authentication.” The Journal of Supercomputing (2020): 1-26.
- Marco, Innocenzo De, Robert I. Woodward, G L Roberts, Taofiq K. Paraíso, Thomas Roger, Mirko Sanzaro, Marco Lucamarini, Zhiliang Yuan and Andrew J. Shields. “Real-time operation of a multi-rate, multi-protocol quantum key distribution transmitter.” (2021).
- Mars, Ayoub, Ahmad Abadleh and Wael Adi. “Operator and Manufacturer Independent D2D Private Link for Future 5G Networks.” IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (2019): 1-6.
- Mascaraque, Nerea, Kacper Januchta, Kristine F. Frederiksen, Randall E. Youngman, Mathieu Bauchy and Morten M. Smedskjaer. “Structural dependence of chemical durability in modified aluminoborate glasses.” Journal of the American Ceramic Society (2018): n. pag.
- McDaniel, Tyler, Jared M. Smith and Max Schuchard. “The Maestro Attack: Orchestrating Malicious Flows with BGP.” SecureComm (2020).
- McGinn, D., Douglas G. McIlwraith and Yike Guo. “Data from: Toward open data blockchain analytics: a Bitcoin perspective.” (2018).
- Meehan, Casey, Amrita Roy Chowdhury, Kamalika Chaudhuri and Somesh Jha. “A Shuffling Framework for Local Differential Privacy.” ArXiv abs/2106.06603 (2021): n. pag.
- Mensi, Neji, Danda B. Rawat and Elyes Balti. “PLS for V2I Communications Using Friendly Jammer and Double kappa-mu Shadowed Fading.” ICC 2021 - IEEE International Conference on Communications (2021): 1-6.
- Meyer, Philipp, Timo Häckel, Sandra Reider, Franz Korf and Thomas C. Schmidt. “Network Anomaly Detection in Cars: A Case for Time-Sensitive Stream Filtering and Policing.” ArXivabs/2112.11109 (2021): n. pag.
- Millar, Stuart. “Vulnerability Detection in Open Source Software: An Introduction.” ArXivabs/2203.16428 (2022): n. pag.
- Miller, Andrew K., Iddo Bentov, Surya Bakshi, Ranjit Kumaresan and Patrick McCorry. “Sprites and State Channels: Payment Networks that Go Faster Than Lightning.” Financial Cryptography(2019).
- Mirshghallah, Fatemehsadat, Mohammadkazem Taram, Praneeth Vepakomma, Abhishek Singh, Ramesh Raskar and Hadi Esmaeilzadeh. “Privacy in Deep Learning: A Survey.” ArXivabs/2004.12254 (2020): n. pag.

- Mirsky, Yisroel, Naor Kalbo, Yuval Elovici and Asaf Shabtai. “Vesper: Using Echo Analysis to Detect Man-in-the-Middle Attacks in LANs.” IEEE Transactions on Information Forensics and Security 14 (2019): 1638-1653.
- Misra, Saurabh, Mengxuan Tan, Mostafa Rezazad and Ngai-Man Cheung. “Early detection of Crossfire attacks using deep learning.” ArXiv abs/1801.00235 (2018): n. pag.
- Mitra, Aritra and Shreyas Sundaram. “Secure Distributed State Estimation of an LTI System Over Time-Varying Networks and Analog Erasure Channels.” 2018 Annual American Control Conference (ACC) (2018): 6578-6583.
- Moghadam, Rohollah and Hamidreza Modares. “Resilient Autonomous Control of Distributed Multiagent Systems in Contested Environments.” IEEE Transactions on Cybernetics 49 (2019): 3957-3967.
- Moreno-Sanchez, Pedro A., Navin Modi, Raghuvir Songhela, Aniket Kate and Sonia Fahmy. “Mind Your Credit: Assessing the Health of the Ripple Credit Network.” Proceedings of the 2018 World Wide Web Conference (2018): n. pag.
- Morgner, Philipp, Stephan Mattejat and Zinaida Benenson. “All Your Bulbs Are Belong to Us: Investigating the Current State of Security in Connected Lighting Systems.” ArXiv abs/1608.03732 (2016): n. pag.
- Moura, José M. F. and David Hutchison. “Resilience Enhancement at Edge Cloud Systems.” IEEE Access 10 (2022): 45190-45206.
- Moustafa, Nour, Marwa Keshk, Essam Soliman Debie and Helge Janicke. “Federated TON_IoT Windows Datasets for Evaluating AI-based Security Applications.” 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) (2020): 848-855.
- Mugisha, Salomon and Hai-Jun Zhou. “Identifying optimal targets of network attack by belief propagation.” Physical review. E 94 1-1 (2016): 012305 .
- Murakami, Takao and Kenta Takahashi. “Toward Evaluating Re-identification Risks in the Local Privacy Model.” Trans. Data Priv. 14 (2021): 79-116.
- Mururu, Girish, Chris Porter, Prithayan Barua and Santosh Pande. “Binary Debloating for Security via Demand Driven Loading.” ArXiv abs/1902.06570 (2019): n. pag.
- Nasr, Milad, Alireza Bahramali and Amir Houmansadr. “DeepCorr: Strong Flow Correlation Attacks on Tor Using Deep Learning.” Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (2018): n. pag.
- Neil, Lorenzo, Sudip Mittal and Anupam Joshi. “Mining Threat Intelligence about Open-Source Projects and Libraries from Code Repository Issues and Bug Reports.” 2018 IEEE International Conference on Intelligence and Security Informatics (ISI) (2018): 7-12.
- Neto, Helio N. Cunha, Ivana Dusparic, Diogo M. F. Mattos and Natalia Castro Fernandes. “FedSA: Accelerating Intrusion Detection in Collaborative Environments with Federated Simulated Annealing.” ArXiv abs/2205.11519 (2022): n. pag.
- Nguyen, Ho Dac Duy, Chi-Dung Phung, Stefano Secci, Benevid Felix Silva and Michele Nogueira Lima. “Can MPTCP secure Internet communications from man-in-the-middle attacks?” 2017 13th International Conference on Network and Service Management (CNSM) (2017): 1-7.
- Nguyen, Quang, Davide Cassi and Michele Bellingeri. “New nodes attack strategies for real complex weighted networks.” arXiv: Physics and Society (2020): n. pag.
- Nguyen, Quang, Tuan V. Vu, Hanh Duyen Dinh, Davide Cassi, Francesco Scotognella, Roberto Alfieri and Michele Bellingeri. “Modularity affects the robustness of scale-

free model and real-world social networks under betweenness and degree-based node attack." Applied Network Science 6 (2021): 1-21.
- Niu, Xiang, Alaa Moussawi, Gyorgy Korniss and Boleslaw K. Szymanski. "Evolution of threats in the global risk network." Applied Network Science 3 (2018): n. pag.
- Nogueira, Michele. "Anticipating Moves to Prevent Botnet Generated DDoS Flooding Attacks." arXiv: Networking and Internet Architecture (2016): n. pag.
- Nowroozi, Ehsan, Abhishek, Mohammadreza Mohammadi and Mauro Conti. "An Adversarial Attack Analysis on Malicious Advertisement URL Detection Framework." ArXiv abs/2204.13172 (2022): n. pag.
- Oh, ChangSeok, Sangho Lee, Wen Xu, Rohan Vora and Taesoo Kim. "Mitigating Low-volume DoS Attacks with Data-driven Resource Accounting." ArXiv abs/2205.00056 (2022): n. pag.
- Oliveira, Arthur de, Milad Siami and Eduardo Sontag. "Edge Selection in Bilinear Dynamical Networks." ArXiv abs/2009.03884 (2020): n. pag.
- Onibere, Mazino, Atif Ahmad and Sean B. Maynard. "Dynamic Information Security Management Capability: Strategising for Organisational Performance." ArXiv abs/2104.07141 (2021): n. pag.
- Oprisanu, Bristena, Christophe Dessimoz and Emiliano De Cristofaro. "How Much Does GenoGuard Really "Guard"?: An Empirical Analysis of Long-Term Security for Genomic Data." Proceedings of the 18th ACM Workshop on Privacy in the Electronic Society (2019): n. pag.
- Ortega, John E.. "Enhancing Networking Cipher Algorithms with Natural Language." ArXivabs/2206.10924 (2022): n. pag.
- Pagadala, Kalaharsha. "Detecting Phishing sites Without Visiting them." ArXiv abs/2205.05121 (2022): n. pag.
- Pan, Kaikai, Elyas Rakhshani and Peter Palensky. "False Data Injection Attacks on Hybrid AC/HVDC Interconnected Systems With Virtual Inertia—Vulnerability, Impact and Detection." IEEE Access 8 (2020): 141932-141945.
- Parkar, Nida, Bhavna Arora, Priti Rumao and Chandana A. Nighut. "Lighting Two Candles With One Flame: An Unaided Human Identification Protocol With Security Beyond Conventional Limit." (2019).
- Patel, Kartik, Nitin Jonathan Myers and Robert W. Heath. "Circulant Shift-based Beamforming for Secure Communication with Low-resolution Phased Arrays." (2021).
- Patrignani, Marco, Dominique Devriese and Frank Piessens. "On Modular and Fully-Abstract Compilation - Technical Appendix." ArXiv abs/1604.05044 (2016): n. pag.
- Patro, Badri N., Shivansh Pate and Vinay P. Namboodiri. "Robust Explanations for Visual Question Answering." 2020 IEEE Winter Conference on Applications of Computer Vision (WACV) (2020): 1566-1575.
- Pavur, James and Ivan Martinovic. "SOK: Building a Launchpad for Impactful Satellite Cyber-Security Research." ArXiv abs/2010.10872 (2020): n. pag.
- Pawlick, Jeffrey, Juntao Chen and Quanyan Zhu. "iSTRICT: An Interdependent Strategic Trust Mechanism for the Cloud-Enabled Internet of Controlled Things." IEEE Transactions on Information Forensics and Security 14 (2019): 1654-1669.
- Pazos-Revilla, Marbin, Mohamed Baza, Mahmoud Nabil, Ahmed B. T. Sherif, Mohamed Mahmoud and Waleed S. Alasmary. "Privacy-Preserving and Collusion-Resistant Charging Coordination Schemes for Smart Grid." ArXiv abs/1905.04666 (2019): n. pag.

- Perez, Ignacio A., Dana Vaknin Ben Porath, Cristian E. La Rocca, Sergey V. Buldyrev, Lidia A. Braunstein and Shlomo Havlin. “Cascading failures in isotropic and anisotropic spatial networks induced by localized attacks and overloads.” New Journal of Physics 24 (2022): n. pag.
- Petrova, Olga, Karel Durkota, Galina Alperovich, K. Horák, Michał Najman, Branislav Bosanský and V. Lisý. “Discovering Imperfectly Observable Adversarial Actions using Anomaly Detection.” AAMAS (2020).
- Phakathi, Thulani, Francis Lugayizi and Michael Esiefarienrhe. “Quality of Service-aware Security Framework for Mobile Ad hoc Networks using Optimized Link State Routing Protocol.” ArXivabs/2010.01852 (2020): n. pag.
- Piotrowska, Ania M., Jamie Hayes, Tariq Ehsan Elahi, Sebastian Meiser and George Danezis. “The Loopix Anonymity System.” ArXiv abs/1703.00536 (2017): n. pag.
- Plinio, Francesco Di and Ioannis Parissis. “Directional square functions and a sharp Meyer lemma.” arXiv: Classical Analysis and ODEs (2020): n. pag.
- Prasad, N., Navonil Chatterjee, Santanu Chattopadhyay and Indrajit Chakrabarti. “Runtime Mitigation of Packet Drop Attacks in Fault-tolerant Networks-on-Chip.” ArXiv abs/1908.00289 (2019): n. pag.
- Pu, Cunlai and Pang Wu. “Vulnerability Assessment of Power Grids Based on Both Topological and Electrical Properties.” ArXiv abs/1909.05789 (2019): n. pag.
- Pu, Cunlai, Kun Wang and Yongxiang Xia. “Robustness of Link Prediction Under Network Attacks.” IEEE Transactions on Circuits and Systems II: Express Briefs 67 (2020): 1472-1476.
- Puglisi, Silvia, David Rebollo-Monedero and Jordi Forné. “Potential Mass Surveillance and Privacy Violations in Proximity-Based Social Applications.” 2015 IEEE Trustcom/BigDataSE/ISPA 1 (2015): 1045-1052.
- Qian, Jianwei, Xiangyang Li, Yu Wang, Shaojie Tang, Taeho Jung and Yang Fan. “Social Network Deanonymization: More Adversarial Knowledge, More Users Re-Identified?” arXiv: Social and Information Networks (2017): n. pag.
- Qin, Jiahu, Menglin Li, Ling Shi and Yu Kang. “Optimal Denial-of-Service Attack Energy Management over an SINR-Based Network.” ArXiv abs/1810.02558 (2018): n. pag.
- Quan, Runai, Hu Hong, Wenxiang Xue, Honglei Quan, Wenyu Zhao, Xiao Xiang, Yuting Liu, Ming-Ming Cao, Tao Liu, Shougang Zhang and Ruifang Dong. “Implementation of field two-way quantum synchronization of distant clocks across a 7 km deployed fiber link.” Optics express 30 7 (2022): 10269-10279 .
- Quiring, Erwin, Dan Arp and Konrad Rieck. “Fraternal Twins: Unifying Attacks on Machine Learning and Digital Watermarking.” ArXiv abs/1703.05561 (2017): n. pag.
- Raj, Akash, Tram Truong Huu, Purnima Murali Mohan and Gurusamy Mohan. “Crossfire Attack Detection Using Deep Learning in Software Defined ITS Networks.” 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring) (2019): 1-6.
- Raman, Gururaghav, Bedoor K. AlShebli, Marcin Waniek, Talal Rahwan and Jimmy Chih-Hsien Peng. “How weaponizing disinformation can bring down a city’s power grid.” PLoS ONE 15 (2020): n. pag.
- Ramasubramanian, Bhaskar, Luyao Niu, Andrew Clark, Linda Bushnell and Radha Poovendran. “Privacy-Preserving Resilience of Cyber-Physical Systems to Adversaries.” 2020 59th IEEE Conference on Decision and Control (CDC) (2020): 3785-3792.

- Ravi, Nikhil and Anna Scaglione. “Detection and Isolation of Adversaries in Decentralized Optimization for Non-Strongly Convex Objectives.” ArXiv abs/1910.13020 (2019): n. pag.
- Remaud, Maxime and Jean-Pierre Tillich. “Time and Query Complexity Tradeoff for the Dihedral Coset Problem.” (2022).
- Ren, Xiaolong, Niels Gleinig, Dijana Tolic and Nino Antulov-Fantulin. “Underestimated cost of targeted attacks on complex networks.” Complex. 2018 (2018): 9826243:1-9826243:15.
- Reusch, Niklas, Silviu S. Craciunas and Paul Pop. “Dependability-Aware Routing and Scheduling for Time-Sensitive Networking.” ArXiv abs/2109.05883 (2022): n. pag.
- Rezaeifar, Shideh, Behrooz Razeghi, Olga Taran, Taras Holotyak and Slava Voloshynovskiy. “Reconstruction of Privacy-Sensitive Data from Protected Templates.” 2019 IEEE International Conference on Image Processing (ICIP) (2019): 1163-1167.
- Rezazad, Mostafa, Matthias R. Brust, Mohammad Akbari, Pascal Bouvry and Ngai-Man Cheung. “Detecting Target-Area Link-Flooding DDoS Attacks using Traffic Analysis and Supervised Learning.” ArXiv abs/1903.01550 (2018): n. pag.
- Rioul, Olivier. “Variations on a Theme by Massey.” IEEE Transactions on Information Theory 68 (2022): 2813-2828.
- Rizk, Elsa, Stefan Vlaski and Ali H. Sayed. “Privatized Graph Federated Learning.” ArXivabs/2203.07105 (2022): n. pag.
- Romano, Yaniv, Aviad Aberdam, Jeremias Sulam and Michael Elad. “Adversarial Noise Attacks of Deep Learning Architectures: Stability Analysis via Sparse-Modeled Signals.” Journal of Mathematical Imaging and Vision 62 (2019): 313-327.
- Roth, Kevin, Aurélien Lucchi, Sebastian Nowozin and Thomas Hofmann. “Adversarially Robust Training through Structured Gradient Regularisation.” ArXiv abs/1805.08736 (2018): n. pag.
- Roth, Kevin, Yannic Kilcher and Thomas Hofmann. “Adversarial Training is a Form of Data-dependent Operator Norm Regularization.” arXiv: Learning (2020): n. pag.
- Roy, Indradyumna, Abir De and Soumen Chakrabarti. “Adversarial Permutation Guided Node Representations for Link Prediction.” AAAI (2021).
- Ruge, Jan, Jiska Classen, Francesco Gringoli and Matthias Hollick. “Frankenstein: Advanced Wireless Fuzzing to Exploit New Bluetooth Escalation Targets.” ArXiv abs/2006.09809 (2020): n. pag.
- Saini, Shalini, Dhiral Panjwani and Nitesh Saxena. “Mobile Mental Health Apps: Alternative Intervention or Intrusion?” ArXiv abs/2206.10728 (2022): n. pag.
- Salamatian, Loqman, Frédérick Douzet, Kevin Limonier and Kave Salamatian. “The geopolitics behind the routes data travels: a case study of Iran.” J. Cybersecur. 7 (2021): n. pag.
- Sankaran, Ganesh Chennimala, Joaquín Chung and Rajkumar Kettimuthu. “La Résistance: Harnessing Heterogeneous Resources for Adaptive Resiliency in 6G Networks.” ArXivabs/2205.00821 (2022): n. pag.
- Sasaki, Takayuki, Christos Pappas, Taeho Lee, Torsten Hoefler and Adrian Perrig. “SDNsec: Forwarding Accountability for the SDN Data Plane.” 2016 25th International Conference on Computer Communication and Networks (ICCCN) (2016): 1-10.

- Sathwara, Snehal, Nitul Dutta and Emil Pricop. “IoT Forensic A digital investigation framework for IoT systems.” 2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI) (2018): 1-4.
- Savva, Giannis, Konstantinos Manousakis and Georgios Ellinas. “Network coding-based routing and spectrum allocation in elastic optical networks for enhanced physical layer security.” Photonic Network Communications (2020): 1 - 15.
- Scala, Antonio J. Di, Andrea Gangemi, Giuliano Romeo and Gabriele Vernetti. “Special subsets of addresses for blockchains using the secp256k1 curve.” ArXiv abs/2206.14107 (2022): n. pag.
- Schad, Jahan N.. “Mental Stress: Source of Neurological Degeneration; Case of MS.” Journal of Neurology and Stroke 1 (2014): n. pag.
- Schilling, Robert, Mario Werner and Stefan Mangard. “Securing conditional branches in the presence of fault attacks.” 2018 Design, Automation & Test in Europe Conference & Exhibition (DATE) (2018): 1586-1591.
- Schilling, Robert, Mario Werner, Pascal Nasahl and Stefan Mangard. “Pointing in the Right Direction - Securing Memory Accesses in a Faulty World.” Proceedings of the 34th Annual Computer Security Applications Conference (2018): n. pag.
- Schilling, Robert, Pascal Nasahl and Stefan Mangard. “FIPAC: Thwarting Fault- and Software-Induced Control-Flow Attacks with ARM Pointer Authentication.” COSADE (2022).
- Sciancalepore, Savio, Omar Adel Ibrahim, Gabriele Oligeri and Roberto Di Pietro. “PiNcH: An effective, efficient, and robust solution to drone detection via network traffic analysis.” Comput. Networks 168 (2020): n. pag.
- Sekatski, Pavel, Jean-Daniel Bancal, Xavier Valcarce, Ernest Y.-Z. Tan, Renato Renner and Nicolas Sangouard. “Device-independent quantum key distribution from generalized CHSH inequalities.” Quantum 5 (2021): 444.
- Senejohnny, Danial, Pietro Tesi and Claudio De Persis. “A Jamming-Resilient Algorithm for Self-Triggered Network Coordination.” IEEE Transactions on Control of Network Systems 5 (2018): 981-990.
- Seymour, John and Philip Tully. “Generative Models for Spear Phishing Posts on Social Media.” ArXiv abs/1802.05196 (2018): n. pag.
- Shafie, Ahmed El, Mohamed F. Marzban, Rakan C. Chabaan and Naofal Al-Dhahir. “An Artificial-Noise-Aided Secure Scheme for Hybrid Parallel PLC/Wireless OFDM Systems.” 2018 IEEE International Conference on Communications (ICC) (2018): 1-6.
- Shanthamallu, Uday Shankar, Jayaraman J. Thiagarajan and Andreas Spanias. “Uncertainty-Matching Graph Neural Networks to Defend Against Poisoning Attacks.” ArXiv abs/2009.14455 (2021): n. pag.
- Sharma, Kartik, Samidha Verma, Sourav Medya, Sayan Ranu and Arnab Bhattacharya. “Task and Model Agnostic Adversarial Attack on Graph Neural Networks.” ArXiv abs/2112.13267 (2021): n. pag.
- Sharma, Piyush Kumar, Devashish Gosain and Claudia Díaz. “On the Anonymity of Peer-To-Peer Network Anonymity Schemes Used by Cryptocurrencies.” ArXiv abs/2201.11860 (2022): n. pag.
- Sharma, Vishal, Ravinder Kumar, Wen-Huang Cheng, Mohammed Atiquzzaman, Kathiravan Srinivasan and Albert Y. Zomaya. “NHAD: Neuro-Fuzzy Based Horizontal Anomaly Detection in Online Social Networks.” IEEE Transactions on Knowledge and Data Engineering 30 (2018): 2171-2184.

- Sheikholeslami, Fatemeh, Swayambhoo Jain and Georgios B. Giannakis. “Minimum Uncertainty Based Detection of Adversaries in Deep Neural Networks.” 2020 Information Theory and Applications Workshop (ITA) (2020): 1-16.
- Shekhtman, Louis M. and Shlomo Havlin. “Percolation of hierarchical networks and networks of networks.” Physical Review E (2018): n. pag.
- Shekhtman, Louis M., Alon Sela and Shlomo Havlin. “Percolation framework reveals limits of privacy in Conspiracy, Dark Web, and Blockchain networks.” ArXiv abs/2007.05466 (2020): n. pag.
- Shen, Kaiwen, Chuhan Wang, Minglei Guo, Xiaofeng Zheng, Chaoyi Lu, Baojun Liu, Yuxuan Zhao, Shuang Hao, Haixin Duan, Qingfeng Pan and Min Yang. “Weak Links in Authentication Chains: A Large-scale Analysis of Email Sender Spoofing Attacks.” USENIX Security Symposium (2021).
- Shen, Wenlong, Yu Cheng, Bo Yin, Kecheng Liu and Xianghui Cao. “Diffie-Hellman in the Air: A Link Layer Approach for In-Band Wireless Pairing.” IEEE Transactions on Vehicular Technology 70 (2021): 11894-11907.
- Shi, Haoyue, Jiayuan Mao, Tete Xiao, Yuning Jiang and Jian Sun. “Learning Visually-Grounded Semantics from Contrastive Adversarial Samples.” COLING (2018).
- Shi, Lei, Qingchen Liu, Jinliang Shao and Yuhua Cheng. “Distributed Localisation in Wireless Sensor Networks Under Denial-of-Service Attacks.” IEEE Control Systems Letters 5 (2021): 493-498.
- Si, Weisheng, Balume Mburano, Wei Xing Zheng and Tie Qiu. “Measuring Network Robustness by Average Network Flow.” IEEE Transactions on Network Science and Engineering 9 (2022): 1697-1712.
- Smith, Matthew, Daniel Moser, Martin Strohmeier, Vincent Lenders and Ivan Martinovic. “Analyzing Privacy Breaches in the Aircraft Communications Addressing and Reporting System (ACARS).” ArXiv abs/1705.07065 (2017): n. pag.
- Smith, Matthew, Martin Strohmeier, Vincent Lenders and Ivan Martinovic. “Understanding realistic attacks on airborne collision avoidance systems.” Journal of Transportation Security 15 (2022): 87-118.
- Snyder, Peter, Soroush Karami, Benjamin Livshits and Hamed Haddadi. “Pool-Party: Exploiting Browser Resource Pools as Side-Channels for Web Tracking.” ArXiv abs/2112.06324 (2021): n. pag.
- Solat, Siamak. “Security of Electronic Payment Systems: A Comprehensive Survey.” ArXivabs/1701.04556 (2017): n. pag.
- Soltani, Ramin, Dennis L. Goeckel, Donald F. Towsley and Amir Houmansadr. “Fundamental Limits of Covert Bit Insertion in Packets.” 2018 56th Annual Allerton Conference on Communication, Control, and Computing (Allerton) (2018): 1065-1072.
- Song, Linhai and Xinyu Xing. “Fine-Grained Library Customisation.” ArXiv abs/1810.11128 (2018): n. pag.
- Srivastava, Brij Mohan Lal, Nathalie Vauquier, Md. Sahidullah, Aurélien Bellet, Marc Tommasi and Emmanuel Vincent. “Evaluating Voice Conversion-Based Privacy Protection against Informed Attackers.” ICASSP 2020 - 2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (2020): 2802-2806.
- Stepniak, Mateusz and Jakub Mielczarek. “Analysis of Multiple Overlapping Paths algorithms for Secure Key Exchange in Large-Scale Quantum Networks.” ArXiv abs/2205.03174 (2022): n. pag.

- Sun, Mingjie, Jian Tang, Huichen Li, Bo Li, Chaowei Xiao, Yao Chen and Dawn Xiaodong Song. “Data Poisoning Attack against Unsupervised Node Embedding Methods.” ArXiv abs/1810.12881 (2018): n. pag.
- Sundar, Bhuvanesh, Mattia Walschaers, Valentina Parigi and Lincoln D. Carr. “Response of quantum spin networks to attacks.” Journal of Physics: Complexity 2 (2021): n. pag.
- Sung, Keen, Brian Neil Levine and Mariya Zhivkova Zheleva. “ZipPhone: Protecting user location privacy from cellular service providers.” ArXiv abs/2002.04731 (2020): n. pag.
- Syverson, Paul F.. “Privacy-Protecting COVID-19 Exposure Notification Based on Cluster Events.” ArXiv abs/2201.00031 (2022): n. pag.
- Szalachowski, Pawel. “Blockchain-based TLS Notary Service.” ArXiv abs/1804.00875 (2018): n. pag.
- Taheri, Mahdi, Khashayar Khorasani, Iman Shames and Nader Meskin. “Cyber Attack and Machine Induced Fault Detection and Isolation Methodologies for Cyber-Physical Systems.” ArXivabs/2009.06196 (2020): n. pag.
- Taheri, Mahdi, Khashayar Khorasani, Iman Shames and Nader Meskin. “Mitigation and Resiliency of Multi-Agent Systems Subject to Malicious Cyber Attacks on Communication Links.” 2020 IEEE Conference on Control Technology and Applications (CCTA) (2020): 857-862.
- Taheri, Mahdi, Khashayar Khorasani, Iman Shames and Nader Meskin. “Undetectable Cyber Attacks on Communication Links in Multi-Agent Cyber-Physical Systems.” 2020 59th IEEE Conference on Decision and Control (CDC) (2020): 3764-3771.
- Talwar, Rohith, Nancy Amala, George Medina, Akshadeep Singh Jida and Mohammed E. Eltayeb. “Exploiting Multi-Path for Safeguarding mmWave Communications Against Randomly Located Eavesdroppers.” ArXiv abs/2010.00733 (2020): n. pag.
- Tang, Rui, Shuyu Jiang, Xingshu Chen, Wenxian Wang and Wei Wang. “Network structural perturbation against interlayer link prediction.” ArXiv abs/2205.09079 (2022): n. pag.
- Tedeschi, Pietro, Savio Sciancalepore and Roberto Di Pietro. “Satellite-Based Communications Security: A Survey of Threats, Solutions, and Research Challenges.” ArXiv abs/2112.11324 (2021): n. pag.
- Tharani, Jeyakumar Samantha and Nalin Asanka Gamagedara Arachchilage. “Understanding phishers’ strategies of mimicking uniform resource locators to leverage phishing attacks: A machine learning approach.” Security and Privacy 3 (2020): n. pag.
- Thiruvasagam, Prabhu Kaliyammal, Abhishek Chakraborty and C. Siva Ram Murthy. “Resilient and Latency-Aware Orchestration of Network Slices Using Multi-Connectivity in MEC-Enabled 5G Networks.” IEEE Transactions on Network and Service Management 18 (2021): 2502-2514.
- Threet, Zachariah, Christos Papadopoulos, William Luke Lambert, Proyash Podder, Spiros Thanasoulas, Alexander Afanasyev, Sheikh Ghafoor and Susmit Shannigrahi. “Securing Automotive Architectures with Named Data Networking.” ArXiv abs/2206.08278 (2022): n. pag.
- Tochner, Saar, Stefan Schmid and Aviv Zohar. “Hijacking Routes in Payment Channel Networks: A Predictability Tradeoff.” ArXiv abs/1909.06890 (2019): n. pag.
- Tople, Shruti, Amit Sharma and Aditya V. Nori. “Alleviating Privacy Attacks via Causal Learning.” ArXiv abs/1909.12732 (2020): n. pag.

- Torfi, Amirsina. “Resilient Feedback Controller Design For Linear Model of Power Grids.” ArXivabs/1807.06778 (2018): n. pag.
- Torre, Stephanie Rendón de la, Jaan Kalda, Robert Kitt and Jüri Engelbrecht. “On the topologic structure of economic complex networks: Empirical evidence from large scale payment network of Estonia.” Chaos Solitons & Fractals 90 (2016): 18-27.
- Torres, Wuilian and Antonio Rueda-Toicen. “Identification of Seed Cells in Multispectral Images for GrowCut Segmentation.” ArXiv abs/1801.05525 (2018): n. pag.
- Turner, H.C.M., Giulio Lovisotto, Simon Eberz and Ivan Martinovic. “I’m Hearing (Different) Voices: Anonymous Voices to Protect User Privacy.” ArXiv abs/2202.06278 (2022): n. pag.
- Ugrinovskii, Valery A. and Cédric Langbort. “Controller-jammer game models of Denial of Service in control systems operating over packet-dropping links.” Autom. 84 (2017): 128-141.
- Vaiwsri, Sirintra, Thilina Ranbaduge, Peter Christen and Kee Siong Ng. “Accurate and Efficient Suffix Tree Based Privacy-Preserving String Matching.” ArXiv abs/2104.03018 (2021): n. pag.
- Vaknin, Dana, Bnaya Gross, Sergey V. Buldyrev and Shlomo Havlin. “Spreading of localized attacks on spatial multiplex networks with a community structure.” arXiv: Physics and Society (2019): n. pag.
- Vaknin, Dana, Michael M. Danziger and Shlomo Havlin. “Spreading of localized attacks in spatial multiplex networks.” ArXiv abs/1704.00267 (2017): n. pag.
- Venkatakrishnan, Shaileshh Bojja, Giulia C. Fanti and Pramod Viswanath. “Dandelion: Redesigning the Bitcoin Network for Anonymity.” Proceedings of the 2017 ACM SIGMETRICS / International Conference on Measurement and Modeling of Computer Systems (2017): n. pag.
- Venkatesaramani, Rajagopal, Bradley A. Malin and Yevgeniy Vorobeychik. “Re-identification of Individuals in Genomic Datasets Using Public Face Images.” Science advances 7 47 (2021): eabg3296 .
- Walk, Nathan, S. J. Farajollah Hosseni, Jiao Geng, Oliver Thearle, Jing Yan Haw, Seiji C. Armstrong, Syed Muhamad Assad, Jirí Janousek, Timothy C. Ralph, Thomas Symul, Howard M. Wiseman and Ping Koy Lam. “Experimental demonstration of Gaussian protocols for one-sided device-independent quantum key distribution.” arXiv: Quantum Physics (2014): n. pag.
- Wan, Junpeng, Yanxiang Bi, Zhe Zhou and Zhou Li. “Volcano: Stateless Cache Side-channel Attack by Exploiting Mesh Interconnect.” ArXiv abs/2103.04533 (2021): n. pag.
- Wang, Dingding, Muhui Jiang, Rui Chang, Yajin Zhou, Baolei Hou, Xiapu Luo, L. Wu and Kui Ren. “A Measurement Study on the (In)security of End-of-Life (EoL) Embedded Devices.” ArXivabs/2105.14298 (2021): n. pag.
- Wang, Jianyu. “Bilateral Adversarial Training: Towards Fast Training of More Robust Models Against Adversarial Attacks.” 2019 IEEE/CVF International Conference on Computer Vision (ICCV)(2019): 6628-6637.
- Wang, Jue, Xuanxuan Wang, Ruifeng Gao, Che-Hao Lei, Wei Feng, Ning Ge, Shi Jin and Tony Q. S. Quek. “Physical Layer Security for UAV Communications in 5G and Beyond Networks.” ArXivabs/2105.11332 (2021): n. pag.

- Wang, Kai, Ilaria Vagniluca, Jie Zhang, Søren Forchhammer, Alessandro Zavatta, Jesper B. Christensen and Davide Bacco. “Round-Robin Differential Phase-Time-Shifting Protocol for Quantum Key Distribution: Theory and Experiment.” (2021).
- Wang, Lei, Pengcheng Xu, Zhaoyang Qu, Xiaoyong Bo, Yunchang Dong, Zhenming Zhang and Y. Li. “Coordinated Cyber-Attack Detection Model of Cyber-Physical Power System Based on the Operating State Data Link.” Frontiers in Energy Research (2021).
- Wang, Qingle, Chao-Hua Yu, Fei Gao, Haoyu Qi and Qiaoyan Wen. “Self-tallying quantum anonymous voting.” Physical Review A 94 (2016): 022333.
- Wang, Rong, Yu Mei, Xiangzhu Meng and Jianjun Ma. “Secrecy performance of terahertz wireless links in rain and snow.” Nano Commun. Networks 28 (2021): 100350.
- Wang, Xiaoyun, Joe Eaton, Cho-Jui Hsieh and Shyhtsun Felix Wu. “Attack Graph Convolutional Networks by Adding Fake Nodes.” ArXiv abs/1810.10751 (2018): n. pag.
- Wang, Xu, Wei Ni, Xuan Zha, Guangsheng Yu, Ren Ping Liu, Nektarios Georgalas and Andrew Reeves. “Capacity Analysis of Public Blockchain.” Comput. Commun. 177 (2021): 112-124.
- Wang, Yifan, Xin Liu, Mei Wang and Yuanjie Yu. “A hidden anti-jamming method based on deep reinforcement learning.” ArXiv abs/2012.12448 (2021): n. pag.
- Wang, Zhipeng, Stefanos Chaliasos, Kaihua Qin, Liyi Zhou, Lifeng Gao, Pascal Berrang, Benjamin Livshits and Arthur Gervais. “On How Zero-Knowledge Proof Blockchain Mixers Improve, and Worsen User Privacy.” ArXiv abs/2201.09035 (2022): n. pag.
- Wang, Zijie, Rongke Liu, Qirui Liu, Lincong Han and John S. Thompson. “Feasibility Study of UAV-Assisted Anti-Jamming Positioning.” IEEE Transactions on Vehicular Technology 70 (2021): 7718-7733.
- Wang, Ziqi and M. Loog. “Enhancing Classifier Conservativeness and Robustness by Polynomiality.” ArXiv abs/2203.12693 (2022): n. pag.
- Waniek, Marcin, Kai Zhou, Yevgeniy Vorobeychik, Esteban Moro Egido, Tomasz P. Michalak and Talal Rahwan. “Attack Tolerance of Link Prediction Algorithms: How to Hide Your Relations in a Social Network.” ArXiv abs/1809.00152 (2018): n. pag.
- Weber, Maurice, Nana Liu, Bo Li, Ce Zhang and Zhikuan Zhao. “Optimal provable robustness of quantum classification via quantum hypothesis testing.” npj Quantum Information 7 (2021): 1-12.
- Wei, Hongxin, Wei Feng, Yunfei Chen, Chengxiang Wang and Ning Ge. “Rethinking Blockchains in the Internet of Things Era from a Wireless Communication Perspective.” IEEE Network 34 (2020): 24-30.
- Wei, Na, Wen-Jie Xie and W.-X. Zhou. “Robustness of the international oil trade network under targeted attacks to economies.” Energy (2022): n. pag.
- Wiefling, Stephan, Tanvi Patil, Markus Durmuth and Luigi Lo Iacono. “Evaluation of Risk-Based Re-Authentication Methods.” ICT Systems Security and Privacy Protection 580 (2020): 280 - 294.
- Wilkens, Florian, Felix Ortmann, Steffen Haas, Matthias Vallentin and Mathias Fischer. “Multi-Stage Attack Detection via Kill Chain State Machines.” Proceedings of the 3rd Workshop on Cyber-Security Arms Race (2021): n. pag.
- Wilkinson, Kieran N., Panagiotis Papanastasiou, Carlo Ottaviani, Tobias Gehring and Stefano Pirandola. “Long-distance continuous-variable measurement-device-

independent quantum key distribution with postselection.” Physical Review Research (2020): n. pag.
- Wood, Trevor M., Vítor Basto Fernandes, Eerke A. Boiten and Iryna Yevseyeva. “Systematic Literature Review: Anti-Phishing Defences and Their Application to Before-the-click Phishing Email Detection.” ArXiv abs/2204.13054 (2022): n. pag.
- Wu, Hanzhou, Wei Wang, Jing Dong, Hongxia Wang and Lizhi Xiong. “The Cut and Dominating Set Problem in A Steganographer Network.” ArXiv abs/1802.09333 (2018): n. pag.
- Xiao, Yuan, Yinqian Zhang and Radu Teodorescu. “SPEECHMINER: A Framework for Investigating and Measuring Speculative Execution Vulnerabilities.” ArXiv abs/1912.00329 (2020): n. pag.
- Xu, J., Lingjie Duan and Rui Zhang. “Proactive Eavesdropping via Cognitive Jamming in Fading Channels.” IEEE Transactions on Wireless Communications 16 (2017): 2790-2806.
- Xu, J., Lingjie Duan and Rui Zhang. “Transmit Optimization for Symbol-Level Spoofing.” IEEE Transactions on Wireless Communications 17 (2018): 41-55.
- Xu, Jiarong, Junru Chen, Yang Yang, Yizhou Sun, Chunping Wang and Jiangang Lu. “Unsupervised Adversarially-Robust Representation Learning on Graphs.” ArXiv abs/2012.02486 (2022): n. pag.
- Xu, Jie, Lingjie Duan and Rui Zhang. “Surveillance and Intervention of Infrastructure-Free Mobile Communications: A New Wireless Security Paradigm.” IEEE Wireless Communications 24 (2017): 152-159.
- Xu, Kaidi, Sijia Liu, Gaoyuan Zhang, Mengshu Sun, Pu Zhao, Quanfu Fan, Chuang Gan and X. Lin. “Interpreting Adversarial Examples by Activation Promotion and Suppression.” ArXivabs/1904.02057 (2019): n. pag.
- Xu, Ziqi, Jingcheng Li, Yanjun Pan, Loukas Lazos, Ming Li and Nirnimesh Ghose. “PoF: Proof-of-Following for Vehicle Platoons.” ArXiv abs/2107.09863 (2022): n. pag.
- Xuan, Qi, Yalu Shan, Jinhuan Wang, Zhongyuan Ruan and Guanrong Chen. “Adversarial Attacks to Scale-Free Networks: Testing the Robustness of Physical Criteria.” ArXiv abs/2002.01249 (2020): n. pag.
- Ylianttila, M., Raimo Kantola, Andrei V. Gurtov, Lozenzo Mucchi, Ian J. Oppermann, Zheng Yan, Tri Nguyen, Fei Liu, Tharaka Mawanane Hewa, Madhusanka Liyanage, Ahmad Ijaz, Juha Partala, Robert Abbas, Artur Hecker, Sara Jayousi, Alessio Martinelli, Stefano Caputo, Jonathan Bechtold, Iván Morales, Andrei Stoica, Giuseppe Abreu, Shahriar Shahabuddin, Erdal Panayirci, Harald Haas, Tanesh Kumar, Basak Ozan Ozparlak and J. J. Roning. “6G White paper: Research challenges for Trust, Security and Privacy.” ArXiv abs/2004.11665 (2020): n. pag.
- Yoon, Minji, Bryan Hooi, Kijung Shin and Christos Faloutsos. “Fast and Accurate Anomaly Detection in Dynamic Graphs with a Two-Pronged Approach.” Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining (2019): n. pag.
- Yu, Shanqing, M. Zhao, Chenbo Fu, Huimin Huang, Xincheng Shu, Qi Xuan and Guanrong Chen. “Target Defense Against Link-Prediction-Based Attacks via Evolutionary Perturbations.” IEEE Transactions on Knowledge and Data Engineering 33 (2021): 754-767.
- Yuste, Javier and Sergio Pastrana. “Avaddon ransomware: an in-depth analysis and decryption of infected systems.” Comput. Secur. 109 (2021): 102388.

- Zahan, Nusrat, Laurie Ann Williams, Thomas Zimmermann, Patrice Godefroid, Brendan Murphy and Chandra Shekhar Maddila. “What are Weak Links in the npm Supply Chain?” 2022 IEEE/ACM 44th International Conference on Software Engineering: Software Engineering in Practice (ICSE-SEIP) (2022): 331-340.
- Zhang, Kai, Yu Wang, Hongyi Wang, Lifu Huang, Carl Yang and Lichao Sun. “Efficient Federated Learning on Knowledge Graphs via Privacy-preserving Relation Embedding Aggregation.” ArXivabs/2203.09553 (2022): n. pag.
- Zhang, Sixiao, Hongxu Chen, Xiangguo Sun, Yicong Li and Guandong Xu. “Unsupervised Graph Poisoning Attack via Contrastive Loss Back-propagation.” Proceedings of the ACM Web Conference 2022 (2022): n. pag.
- Zhang, Xingjian, Pei Zeng, Tian-Yu Ye, Hoi-Kwong Lo and Xiongfeng Ma. “Quantum Complementarity Approach to Device-Independent Security.” (2021).
- Zhao, Jun. “On Resilience and Connectivity of Secure Wireless Sensor Networks Under Node Capture Attacks.” IEEE Transactions on Information Forensics and Security 12 (2017): 557-571.
- Zhao, Jun. “Probabilistic Key Predistribution in Mobile Networks Resilient to Node-Capture Attacks.” IEEE Transactions on Information Theory 63 (2017): 6714-6734.
- Zhao, Kangfei, Yu Rong, Jeffrey Xu Yu, Junzhou Huang and Hao Zhang. “Graph Ordering: Towards the Optimal by Learning.” WISE (2021).
- Zhao, Yimeng, Samantha Lo, Ellen Witte Zegura, Mostafa H. Ammar and Niky Riga. “Virtual network migration on the GENI wide-area SDN-enabled infrastructure.” 2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (2017): 265-270.
- Zheng, Kexian, Ying Liu, Yang Wang and Wei Wang. “k-core percolation on interdependent and interconnected multiplex networks.” Europhysics Letters 133 (2021): n. pag.
- Zheng, Wenzhe, Zhiyu He, Jianping He, Chengcheng Zhao and Chongrong Fang. “Resilient Average Consensus: A Detection and Compensation Approach.” ArXiv abs/2202.10814 (2022): n. pag.
- Zheng-Xun, Jiang and Tsay Ren-Song. “A Double-Linked Blockchain Approach Based on Proof-of-Refundable-Tax Consensus Algorithm.” (2020).
- Zhong, Changtao and Nishanth R. Sastry. “Systems Applications of Social Networks.” ACM Computing Surveys (CSUR) 50 (2017): 1 - 42.
- Zhou, Bo, Yuqian Lv, Yongchao Mao, Jinhuan Wang, Shanqing Yu and Qi Xuan. “The Robustness of Graph k-Shell Structure Under Adversarial Attacks.” IEEE Transactions on Circuits and Systems II: Express Briefs 69 (2022): 1797-1801.
- Zhou, Dong and Amir Bashan. “Dependency-based targeted attacks in interdependent networks.” Physical review. E 102 2-1 (2020): 022301 .
- Zhou, Hongyi, Toshihiko Sasaki and Masato Koashi. “Numerical Method for Finite-size Security Analysis of Quantum Key Distribution.” (2021).
- Zhou, Kai, Tomasz P. Michalak and Yevgeniy Vorobeychik. “Adversarial Robustness of Similarity-Based Link Prediction.” 2019 IEEE International Conference on Data Mining (ICDM) (2019): 926-935.
- Zhou, Kai, Tomasz P. Michalak, Marcin Waniek, Talal Rahwan and Yevgeniy Vorobeychik. “Attacking Similarity-Based Link Prediction in Social Networks.” AAMAS (2019).

- Zhou, Pan, Lin Cheng and Dapeng Oliver Wu. “Near Optimal Adaptive Shortest Path Routing with Stochastic Links States under Adversarial Attack.” ArXiv abs/1610.03348 (2016): n. pag.
- Zhu, Junhao, Yalu Shan, Jinhuan Wang, Shanqing Yu, Guanrong Chen and Qi Xuan. “DeepInsight: Interpretability Assisting Detection of Adversarial Samples on Graphs.” ArXiv abs/2106.09501 (2021): n. pag.
- Zhu, R., Tao Shu and Huirong Fu. “Statistical Inference Attack Against PHY-layer Key Extraction and Countermeasures.” Wirel. Networks 27 (2021): 4853-4873.
- Zhu, Yanzi, Ying Ju, Bolun Wang, Jenna Cryan, Ben Y. Zhao and Haitao Zheng. “Wireless Side-Lobe Eavesdropping Attacks.” ArXiv abs/1810.10157 (2018): n. pag.
- Zhu, Yanzi, Zhujun Xiao, Yuxin Chen, Zhijing Li, Max Liu, Ben Y. Zhao and Haitao Zheng. “Et Tu Alexa? When Commodity WiFi Devices Turn into Adversarial Motion Sensors.” Proceedings 2020 Network and Distributed System Security Symposium (2020): n. pag.
- Zhuang, Quntao, Zheshen Zhang and Jeffrey H. Shapiro. “High-order encoding schemes for floodlight quantum key distribution.” Physical Review A (2018): n. pag.
- Zhuang, Quntao, Zheshen Zhang, Justin Dove, Franco N. C. Wong and Jeffrey H. Shapiro. “Floodlight quantum key distribution: A practical route to gigabit-per-second secret-key rates.” Physical Review A 94 (2016): 012322.
- Zia, R. K. P., Weibin Zhang, Mohammadmehdi Ezzatabadipour and Kevin E. Bassler. “Exact results for the extreme Thouless effect in a model of network dynamics.” EPL (Europhysics Letters)(2019): n. pag.
- Zou, Xu, Qinkai Zheng, Yuxiao Dong, Xin Guan, Evgeny Kharlamov, Jialiang Lu and Jie Tang. “TDGIA: Effective Injection Attacks on Graph Neural Networks.” Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery & Data Mining (2021).

Annex V: Inference

- Aalmoes, Jan, Vasisht Duddu and Antoine Boutet. “Dikaios: Privacy Auditing of Algorithmic Fairness via Attribute Inference Attacks.” ArXiv abs/2202.02242 (2022): n. pag.
- Abad, Gorka, Servio Paguada, Stjepan Picek, V’ictor Julio Ram’irez-Dur’an and Aitor Urbieta. “Client-Wise Targeted Backdoor in Federated Learning.” ArXiv abs/2203.08689 (2022): n. pag.
- Abdelnabi, Sahar and Mario Fritz. “Adversarial Watermarking Transformer: Towards Tracing Text Provenance with Data Hiding.” 2021 IEEE Symposium on Security and Privacy (SP) (2021): 121-140.
- Abdulsamad, Hany, Tim Dorau, Boris Belousov, Jia-Jie Zhu and Jan Peters. “Distributionally Robust Trajectory Optimization Under Uncertain Dynamics via Relative-Entropy Trust Regions.” ArXiv abs/2103.15388 (2021): n. pag.
- Acharya, Jayadev, Ziteng Sun and Huanyu Zhang. “Robust Testing and Estimation under Manipulation Attacks.” ICML (2021).
- Adeyemo, Adewale, Faiq Khalid, Tolulope A. Odetola and Syed Rafay Hasan. “Security Analysis of Capsule Network Inference using Horizontal Collaboration.” 2021 IEEE International Midwest Symposium on Circuits and Systems (MWSCAS) (2021): 1074-1077.
- Agarwal, Vibhor, Sagar Joglekar, Anthony Peter Young and Nisha Chetana Sastry. “GraphNLI: A Graph-based Natural Language Inference Model for Polarity Prediction in Online Debates.” Proceedings of the ACM Web Conference 2022 (2022): n. pag.
- Aggarwal, Abhinav, Shiva Prasad Kasiviswanathan, Zekun Xu, Oluwaseyi Feyisetan and Nathanael Teissier. “Label Inference Attacks from Log-loss Scores.” ArXiv abs/2105.08266 (2021): n. pag.
- Aggarwal, Abhinav, Shiva Prasad Kasiviswanathan, Zekun Xu, Oluwaseyi Feyisetan and Nathanael Teissier. “Reconstructing Test Labels from Noisy Loss Functions.” AISTATS (2022).

- Aggarwal, Abhinav, Zekun Xu, Oluwaseyi Feyisetan and Nathanael Teissier. “On Primes, Log-Loss Scores and (No) Privacy.” ArXiv abs/2009.08559 (2020): n. pag.
- Aghakhani, H., Dongyu Meng, Yu-xiang Wang, Christopher Kruegel and Giovanni Vigna. “Bullseye Polytope: A Scalable Clean-Label Poisoning Attack with Improved Transferability.” 2021 IEEE European Symposium on Security and Privacy (EuroS&P) (2021): 159-178.
- Aghdaie, Poorya, Baaria Chaudhary, Sobhan Soleymani, Jeremy M. Dawson and Nasser M. Nasrabadi. “Morph Detection Enhanced by Structured Group Sparsity.” 2022 IEEE/CVF Winter Conference on Applications of Computer Vision Workshops (WACVW) (2022): 311-320.
- Ahuja, Nilesh A., Ibrahima J. Ndiour, Trushant Kalyanpur and Omesh Tickoo. “Probabilistic Modeling of Deep Features for Out-of-Distribution and Adversarial Detection.” ArXivabs/1909.11786 (2019): n. pag.
- Alam, Mohammad Mahmudul, Edward Raff, Tim Oates and James Holt. “Deploying Convolutional Networks on Untrusted Platforms Using 2D Holographic Reduced Representations.” ICML (2022).
- Albert, Kendra, Jonathon W. Penney, Bruce Schneier and Ram Shankar Siva Kumar. “Politics of Adversarial Machine Learning.” ArXiv abs/2002.05648 (2020): n. pag.
- Aldahdooh, Ahmed, Wassim Hamidouche and Olivier D’eforges. “Revisiting model’s uncertainty and confidences for adversarial example detection.” Applied Intelligence (2022): n. pag.
- Ali, Hassan, Surya Nepal, Salil S. Kanhere and Sanjay Kumar Jha. “HaS-Nets: A Heal and Select Mechanism to Defend DNNs Against Backdoor Attacks for Data Collection Scenarios.” ArXivabs/2012.07474 (2020): n. pag.
- Almseidin, Mohammad and Szilveszter Kovács. “Intrusion Detection Mechanism Using Fuzzy Rule Interpolation.” ArXiv abs/1904.08790 (2019): n. pag.
- Almseidin, Mohammad, Jamil Al-Sawwa and Mouhammd Alkasassbeh. “Anomaly-based Intrusion Detection System Using Fuzzy Logic.” 2021 International Conference on Information Technology (ICIT) (2021): 290-295.
- Aloufi, Ranya, Hamed Haddadi and David Boyle. “Privacy-preserving Voice Analysis via Disentangled Representations.” Proceedings of the 2020 ACM SIGSAC Conference on Cloud Computing Security Workshop (2020): n. pag.
- Alrahis, Lilas, Satwik Patnaik, Muhammad Abdullah Hanif, Muhammad Shafique and Ozgur Sinanoglu. “UNTANGLE: Unlocking Routing and Logic Obfuscation Using Graph Neural Networks-based Link Prediction.” 2021 IEEE/ACM International Conference On Computer Aided Design (ICCAD) (2021): 1-9.
- Alserr, Nour Almadhoun, Gül Kale, Onur Mutlu, Oznur Tastan and Erman Ayday. “Near-Optimal Privacy-Utility Tradeoff in Genomic Studies Using Selective SNP Hiding.” ArXiv abs/2106.05211 (2021): n. pag.
- Al-Shaer, Rawan, Jonathan M. Spring and Eliana Christou. “Learning the Associations of MITRE ATT & CK Adversarial Techniques.” 2020 IEEE Conference on Communications and Network Security (CNS) (2020): 1-9.
- Alvar, Saeed Ranjbar, Lanjun Wang, Jiangbo Pei and Yong Zhang. “Membership Privacy Protection for Image Translation Models via Adversarial Knowledge Distillation.” ArXiv abs/2203.05212 (2022): n. pag.
- Alvari, Hamidreza, Elham Shaabani and Paulo Shakarian. “Early Identification of Pathogenic Social Media Accounts.” 2018 IEEE International Conference on Intelligence and Security Informatics (ISI) (2018): 169-174.

- Alvari, Hamidreza. “Causal Inference for Early Detection of Pathogenic Social Media Accounts.” ArXiv abs/1806.09787 (2018): n. pag.
- Alvim, Mário S., Konstantinos Chatzikokolakis, Yusuke Kawamoto and Catuscia Palamidessi. “A Game-Theoretic Approach to Information-Flow Control via Protocol Composition.” Entropy 20 (2018): n. pag.
- Alvim, Mário S., Konstantinos Chatzikokolakis, Yusuke Kawamoto and Catuscia Palamidessi. “Leakage and Protocol Composition in a Game-Theoretic Perspective.” POST (2018).
- An, Qi A., Ruijiang Li, Lin Gu, Hao Zhang, Qingyu Chen, Zhiyong Lu, Fei Wang and Yingying Zhu. “A Privacy-Preserving Unsupervised Domain Adaptation Framework for Clinical Text Analysis.” ArXivabs/2201.07317 (2022): n. pag.
- Anderson, Blake, Andrew Chi, Scott Dunlop and David A. McGrew. “Limitless HTTP in an HTTPS World: Inferring the Semantics of the HTTPS Protocol without Decryption.” Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy (2019): n. pag.
- André, Étienne and Aleksander Kryukov. “Parametric non-interference in timed automata.” 2020 25th International Conference on Engineering of Complex Computer Systems (ICECCS) (2020): 37-42.
- Andreev, Mikhail, Avraham Klausner, Trishita Tiwari, Ari Trachtenberg and Arkady Yerukhimovich. “Nothing But Net: Invading Android User Privacy Using Only Network Access Patterns.” ArXivabs/1807.02719 (2018): n. pag.
- Anirudh, Rushil, Jayaraman J. Thiagarajan, Bhavya Kailkhura and Timo Bremer. “MimicGAN: Corruption-Mimicking for Blind Image Recovery & Adversarial Defense.” ArXiv abs/1811.08484 (2018): n. pag.
- Aprilpyone, Maungmaung and Hitoshi Kiya. “Transfer Learning-Based Model Protection With Secret Key.” 2021 IEEE International Conference on Image Processing (ICIP) (2021): 3877-3881.
- Apruzzese, Giovanni, Rodion Vladimirov, A.T. Tastemirova and Pavel Laskov. “Wild Networks: Exposure of 5G Network Infrastructures to Adversarial Examples.” ArXiv abs/2207.01531 (2022): n. pag.
- Apthorpe, Noah J., Danny Yuxing Huang, Dillon Reisman, Arvind Narayanan and Nick Feamster. “Keeping the Smart Home Private with Smart(er) IoT Traffic Shaping.” Proceedings on Privacy Enhancing Technologies 2019 (2019): 128 - 148.
- Arashloo, Shervin Rahimzadeh. “Unknown Face Presentation Attack Detection via Localised Learning of Multiple Kernels.” ArXiv abs/2204.10675 (2022): n. pag.
- Arisoy, Cagri, Anuradha Mandal and Nitesh Saxena. “Human Brains Can’t Detect Fake News: A Neuro-Cognitive Study of Textual Disinformation Susceptibility.” ArXiv abs/2207.08376 (2022): n. pag.
- Arnab, Anurag, Ondrej Miksik and Philip H. S. Torr. “On the Robustness of Semantic Segmentation Models to Adversarial Attacks.” 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition (2018): 888-897.
- Atanasova, Pepa, Dustin Wright and Isabelle Augenstein. “Generating Label Cohesive and Well-Formed Adversarial Claims.” ArXiv abs/2009.08205 (2020): n. pag.
- Atrey, Akanksha, Prashant J. Shenoy and David Jensen. “Preserving Privacy in Personalized Models for Distributed Mobile Services.” 2021 IEEE 41st International Conference on Distributed Computing Systems (ICDCS) (2021): 875-886.
- Awais, Muhammad, Fahad Shamshad and Sung-Ho Bae. “Towards an Adversarially Robust Normalisation Approach.” ArXiv abs/2006.11007 (2020): n. pag.

- Ayoz, Kerem, Erman Ayday and A. Ercument Cicek. “Genome Reconstruction Attacks Against Genomic Data-Sharing Beacons.” Proceedings on Privacy Enhancing Technologies 2021 (2021): 28 - 48.
- Baccour, Emna, Aiman Erbad, Amr M. Mohamed, Mounir Hamdi and Mohsen Guizani. “DistPrivacy: Privacy-Aware Distributed Deep Neural Networks in IoT surveillance systems.” GLOBECOM 2020 - 2020 IEEE Global Communications Conference (2020): 1-6.
- Backes, Michael, Mathias Humbert, Jun Pang and Yang Zhang. “walk2friends: Inferring Social Links from Mobility Profiles.” Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (2017): n. pag.
- Bae, Ho, Jaehee Jang, Dahuin Jung, Hyemi Jang, Heonseok Ha and Sungroh Yoon. “Security and Privacy Issues in Deep Learning.” ArXiv abs/1807.11655 (2018): n. pag.
- Baek, Kyungjune and Hyunjung Shim. “Commonality in Natural Images Rescues GANs: Pretraining GANs with Generic and Privacy-free Synthetic Data.” ArXiv abs/2204.04950 (2022): n. pag.
- Bagdasaryan, Eugene and Vitaly Shmatikov. “Blind Backdoors in Deep Learning Models.” ArXivabs/2005.03823 (2021): n. pag.
- Bagmar, Aadesh, Shishira R. Maiya, Shruti Bidwalka and Amol Deshpande. “Membership Inference Attacks on Lottery Ticket Networks.” ArXiv abs/2108.03506 (2021): n. pag.
- Bai, Jiawang, Baoyuan Wu, Yong Zhang, Y. Li, Zhifeng Li and Shutao Xia. “Targeted Attack against Deep Neural Networks via Flipping Limited Weight Bits.” ArXiv abs/2102.10496 (2021): n. pag.
- Bakopoulou, Evita, Jiang Zhang, Justin Ley, Konstantinos Psounis and Athina Markopoulou. “Location Leakage in Federated Signal Maps.” ArXiv abs/2112.03452 (2021): n. pag.
- Banerjee, Sarbartha, Shijia Wei, Prakash Ramrakhyani and Mohit Tiwari. “Bandwidth Utilization Side-Channel on ML Inference Accelerators.” ArXiv abs/2110.07157 (2021): n. pag.
- Bao, Rongzhou, Jiayi Wang and Hai Zhao. “Defending Pre-trained Language Models from Adversarial Word Substitution Without Performance Sacrifice.” FINDINGS (2021).
- Barman, Ludovic and Jean-Pierre Hubaux. “Every Byte Matters: Traffic Analysis of Bluetooth Wearable Devices.” (2021).
- Barman, Ludovic, Italo Dacosta, Mahdi Zamani, Ennan Zhai, Apostolos Pyrgelis, Bryan Ford, Joan Feigenbaum and Jean-Pierre Hubaux. “PriFi: Low-Latency Anonymity for Organizational Networks.” Proceedings on Privacy Enhancing Technologies 2020 (2020): 24 - 47.
- Bar-On, Y., Ron Sender, Avi I. Flamholz, Rob Phillips and Ron Milo. “A quantitative compendium of COVID-19 epidemiology.” arXiv: Other Quantitative Biology (2020): n. pag.
- Beigi, Ghazaleh, Ahmadreza Mosallanezhad, Ruocheng Guo, Hamidreza Alvari, Alexander Nou and Huan Liu. “Privacy-Aware Recommendation with Private-Attribute Protection using Adversarial Learning.” Proceedings of the 13th International Conference on Web Search and Data Mining(2020): n. pag.
- Bensalem, Mounir, Sandeep Kumar Singh and Admela Jukan. “On Detecting and Preventing Jamming Attacks with Machine Learning in Optical Networks.” 2019 IEEE Global Communications Conference (GLOBECOM) (2019): 1-6.

- Bentley, Jason, Daniel Gibney, Gary Hoppenworth and Sumit Kumar Jha. “Quantifying Membership Inference Vulnerability via Generalization Gap and Other Model Metrics.” ArXiv abs/2009.05669 (2020): n. pag.
- Bernau, Daniel, Jonas Robl and Florian Kerschbaum. “Assessing Differentially Private Variational Autoencoders under Membership Inference.” ArXiv abs/2204.07877 (2022): n. pag.
- Bernau, Daniel, Philip-William Grassal, Jonas Robl and Florian Kerschbaum. “Assessing differentially private deep learning with Membership Inference.” ArXiv abs/1912.11328 (2019): n. pag.
- Bhardwaj, Peru, John D. Kelleher, Luca Costabello and Declan O’Sullivan. “Poisoning Knowledge Graph Embeddings via Relation Inference Patterns.” ArXiv abs/2111.06345 (2021): n. pag.
- Bielik, Pavol and Martin T. Vechev. “Adversarial Robustness for Code.” ICML (2020).
- Biskup, Joachim, Cornelia Tadros and Jaouad Zarouali. “Confidentiality enforcement by hybrid control of information flows.” ArXiv abs/1707.08482 (2017): n. pag.
- Bitton, Joanna, Maya Pavlova and I. Evtimov. “Adversarial Text Normalization.” ArXivabs/2206.04137 (2022): n. pag.
- Blaabjerg, Jeppe Fredsgaard and Aslan Askarov. “Towards Language-Based Mitigation of Traffic Analysis Attacks.” 2021 IEEE 34th Computer Security Foundations Symposium (CSF) (2021): 1-15.
- Blaas, Arno and Stephen J. Roberts. “The Effect of Prior Lipschitz Continuity on the Adversarial Robustness of Bayesian Neural Networks.” ArXiv abs/2101.02689 (2021): n. pag.
- Borji, Ali. “Adversarial examples are useful too!” ArXiv abs/2005.06107 (2020): n. pag.
- Borji, Ali. “Shape Defense Against Adversarial Attacks.” (2020).
- Bortolussi, Luca, Ginevra Carbone, Luca Laurenti, Andrea Patané, Guido Sanguinetti and Matthew Wicker. “On the Robustness of Bayesian Neural Networks to Adversarial Attacks.” (2022).
- Boskov, Novak, Mihailo Isakov and Michel A. Kinsy. “Drndalo: Lightweight Control Flow Obfuscation Through Minimal Processor/Compiler Co-Design.” ArXiv abs/1912.01560 (2019): n. pag.
- Boutet, Antoine, Thomas LeBrun, Jan Aalmoes and Adrien Baud. “MixNN: Protection of Federated Learning Against Inference Attacks by Mixing Neural Network Layers.” ArXiv abs/2109.12550 (2021): n. pag.
- Boutros, Andrew, Mathew Hall, Nicolas Papernot and Vaughn Betz. “Neighbors From Hell: Voltage Attacks Against Deep Learning Accelerators on Multi-Tenant FPGAs.” 2020 International Conference on Field-Programmable Technology (ICFPT) (2020): 103-111.
- Brasser, Ferdinand, Srdjan Capkun, Alexandra Dmitrienko, Tommaso Frassetto, Kari Kostiainen, Urs Müller and Ahmad-Reza Sadeghi. “DR.SGX: Hardening SGX Enclaves against Cache Attacks with Data Location Randomization.” ArXiv abs/1709.09917 (2019): n. pag.
- Breier, Jakub, Xiaolu Hou, Martín Ochoa and Jesus Solano. “FooBaR: Fault Fooling Backdoor Attack on Neural Network Training.” ArXiv abs/2109.11249 (2022): n. pag.
- Büchel, Julian, Fynn Faber and Dylan Richard Muir. “Network insensitivity to parameter noise via adversarial regularization.” ArXiv abs/2106.05009 (2021): n. pag.

- Buriachok, Volodymyr, Volodymyr Yu. Sokolov and Mahyar Taj Dini. “Research of Caller ID Spoofing Launch, Detection, and Defense.” ArXiv abs/2004.00318 (2020): n. pag.
- Bushart, Jonas and Christian Rossow. “Padding Ain't Enough: Assessing the Privacy Guarantees of Encrypted DNS.” ArXiv abs/1907.01317 (2020): n. pag.
- Byrenheid, Martin, Stefanie Roos and Thorsten Strufe. “Topology Inference of Networks utilizing Rooted Spanning Tree Embeddings.” 23rd International Conference on Distributed Computing and Networking (2022): n. pag.
- Byun, Junyoung, Hyojun Go and Changick Kim. “On the Effectiveness of Small Input Noise for Defending Against Query-based Black-Box Attacks.” 2022 IEEE/CVF Winter Conference on Applications of Computer Vision (WACV) (2022): 3819-3828.
- Cai, Danwei, Zexin Cai and Ming Li. “Identifying Source Speakers for Voice Conversion based Spoofing Attacks on Speaker Verification Systems.” ArXiv abs/2206.09103 (2022): n. pag.
- Cai, Shuowei, Di Chai, Liu Yang, Junxue Zhang, Yilun Jin, Leye Wang, Kun Guo and Kai Chen. “Secure Forward Aggregation for Vertical Federated Neural Networks.” ArXiv abs/2207.00165 (2022): n. pag.
- Camburu, Oana-Maria, Brendan Shillingford, Pasquale Minervini, Thomas Lukasiewicz and Phil Blunsom. “Make Up Your Mind! Adversarial Generation of Inconsistent Natural Language Explanations.” ACL (2020).
- Cao, Phuong. “On Preempting Advanced Persistent Threats Using Probabilistic Graphical Models.” ArXiv abs/1903.08826 (2019): n. pag.
- Cao, Yang, Yonghui Xiao, Li Xiong and Liquan Bai. “PriSTE: From Location Privacy to Spatiotemporal Event Privacy.” 2019 IEEE 35th International Conference on Data Engineering (ICDE) (2019): 1606-1609.
- Carannante, Giuseppina, Dimah Dera, Ghulam Rasool, Nidhal Carla Bouaynaya and Lyudmila S. Mihaylova. “Robust Learning via Ensemble Density Propagation in Deep Neural Networks.” 2020 IEEE 30th International Workshop on Machine Learning for Signal Processing (MLSP) (2020): 1-6.
- Carbone, Ginevra, Matthew Wicker, Luca Laurenti, Andrea Patané, Luca Bortolussi and Guido Sanguinetti. “Robustness of Bayesian Neural Networks to Gradient-Based Attacks.” ArXivabs/2002.04359 (2020): n. pag.
- Cardaioli, Matteo, Mauro Conti, Kiran S. Balagani and Paolo Gasti. “Your PIN Sounds Good! On The Feasibility of PIN Inference Through Audio Leakage.” ArXiv abs/1905.08742 (2019): n. pag.
- Cardaioli, Matteo, Stefano Cecconello, Mauro Conti, Simone Milani, Stjepan Picek and Eugen Saraci. “Hand Me Your PIN! Inferring ATM PINs of Users Typing with a Covered Hand.” ArXivabs/2110.08113 (2021): n. pag.
- Carlini, Nicholas, Steve Chien, Milad Nasr, Shuang Song, A. Terzis and Florian Tramèr. “Membership Inference Attacks From First Principles.” ArXiv abs/2112.03570 (2021): n. pag.
- Ceccato, Mariano, Paolo Tonella, Cataldo Basile, Bart Coppens, Bjorn De Sutter, Paolo Falcarin and Marco Torchiano. “How Professional Hackers Understand Protected Code while Performing Attack Tasks.” 2017 IEEE/ACM 25th International Conference on Program Comprehension (ICPC)(2017): 154-164.
- Cemgil, Ali Taylan, Sumedh Ghaisas, Krishnamurthy Dvijotham, Sven Gowal and Pushmeet Kohli. “The Autoencoding Variational Autoencoder.” ArXiv abs/2012.03715 (2020): n. pag.

- Cennamo, Alessandro, Ido Freeman and Anton Kummert. “A Statistical Defense Approach for Detecting Adversarial Examples.” Proceedings of the 2020 International Conference on Pattern Recognition and Intelligent Systems (2019): n. pag.
- Champion, Pierre, Denis Jouvet and Anthony Larcher. “Evaluating X-Vector-Based Speaker Anonymization Under White-Box Assessment.” SPECOM (2021).
- Chan, Alvin, Yi Tay, Y. Ong and Aston Zhang. “Poison Attacks against Text Datasets with Conditional Adversarially Regularized Autoencoder.” FINDINGS (2020).
- Chandrasekaran, Varun, Suman Banerjee, Diego Perino and Nicolas Kourtellis. “Hierarchical Federated Learning with Privacy.” ArXiv abs/2206.05209 (2022): n. pag.
- Chandy, Sarin E., Amin Rasekh, Zachary A. Barker and M. Ehsan Shafiee. “Cyberattack Detection using Deep Generative Models with Variational Inference.” ArXiv abs/1805.12511 (2019): n. pag.
- Chang, Hong and R. Shokri. “On the Privacy Risks of Algorithmic Fairness.” 2021 IEEE European Symposium on Security and Privacy (EuroS&P) (2021): 292-303.
- Chang, Hong, Virat Shejwalkar, R. Shokri and Amir Houmansadr. “Cronus: Robust and Heterogeneous Collaborative Learning with Black-Box Knowledge Transfer.” ArXivabs/1912.11279 (2019): n. pag.
- Chase, Melissa, Esha Ghosh and Saeed Mahloujifar. “Property Inference From Poisoning.” IACR Cryptol. ePrint Arch. 2021 (2021): 99.
- Chattopadhyay, Nandish, Lionell Yip En Zhi, Bryan Tan Bing Xing and Anupam Chattopadhyay. “Spatially Correlated Patterns in Adversarial Images.” ArXiv abs/2011.10794 (2020): n. pag.
- Chattopadhyay, Sudipta, Moritz Beck, Ahmed Rezine and Andreas Zeller. “Quantifying the Information Leak in Cache Attacks through Symbolic Execution.” ArXiv abs/1611.04426 (2016): n. pag.
- Chawla, Nikhil, Arvind Singh, Monodeep Kar and S. Mukhopadhyay. “Application Inference using Machine Learning based Side Channel Analysis.” 2019 International Joint Conference on Neural Networks (IJCNN) (2019): 1-8.
- Chen, Bryant, Wilka Carvalho, Nathalie Baracaldo, Heiko Ludwig, Ben Edwards, Taesung Lee, Ian Molloy and B. Srivastava. “Detecting Backdoor Attacks on Deep Neural Networks by Activation Clustering.” ArXiv abs/1811.03728 (2019): n. pag.
- Chen, Chen, Xuanli He, Lingjuan Lyu and Fangzhao Wu. “Killing One Bird with Two Stones: Model Extraction and Attribute Inference Attacks against BERT-based APIs.” (2021).
- Chen, Chien-Ying, Sibin Mohan, Rodolfo Pellizzoni and Rakesh B. Bobba. “On Scheduler Side-Channels in Dynamic-Priority Real-Time Systems.” ArXiv abs/2001.06519 (2020): n. pag.
- Chen, Dingfan, Ning Yu and Mario Fritz. “RelaxLoss: Defending Membership Inference Attacks without Losing Utility.” (2022).
- Chen, Dingfan, Ning Yu, Yang Zhang and Mario Fritz. “GAN-Leaks: A Taxonomy of Membership Inference Attacks against Generative Models.” Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (2020): n. pag.
- Chen, Jiaxin and Yi Fang. “Deep Cross-modality Adaptation via Semantics Preserving Adversarial Learning for Sketch-based 3D Shape Retrieval.” ECCV (2018).
- Chen, Jiyang, Tomasz Kloda, Ayoosh Bansal, Rohan Tabish, Chien-Ying Chen, Bo Liu, Sibin Mohan, Marco Caccamo and Lui Raymond Sha. “SchedGuard: Protecting against Schedule Leaks Using Linux Containers.” 2021 IEEE 27th Real-Time and Embedded Technology and Applications Symposium (RTAS) (2021): 14-26.

- Chen, Kongyang, Yao Huang and Yiwen Wang. “Machine unlearning via GAN.” ArXivabs/2111.11869 (2021): n. pag.
- Chen, Li-Wei and Nils Thuerey. “Towards high-accuracy deep learning inference of compressible turbulent flows over aerofoils.” ArXiv abs/2109.02183 (2021): n. pag.
- Chen, Michelle and Olga Ohrimenko. “Protecting Global Properties of Datasets with Distribution Privacy Mechanisms.” ArXiv abs/2207.08367 (2022): n. pag.
- Chen, Min, Zhikun Zhang, Tianhao Wang, Michael Backes, Mathias Humbert and Yang Zhang. “When Machine Unlearning Jeopardizes Privacy.” Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (2021): n. pag.
- Chen, Qingrong, Chong Xiang, Minhui Xue, Bo Li, Nikita Borisov, Dali Kaafar and Haojin Zhu. “Differentially Private Data Generative Models.” ArXiv abs/1812.02274 (2018): n. pag.
- Chen, Xiyuan, Xingyu Li, Yi Zhou and Tianming Yang. “DDDM: a Brain-Inspired Framework for Robust Classification.” ArXiv abs/2205.10117 (2022): n. pag.
- Chen, Xuxi, Tianlong Chen, Zhenyu (Allen) Zhang and Zhangyang Wang. “You are caught stealing my winning lottery ticket! Making a lottery ticket claim its ownership.” NeurIPS (2021).
- Chen, Yongxin, Tryphon T. Georgiou and Michele Pavon. “Stochastic Control Liaisons: Richard Sinkhorn Meets Gaspard Monge on a Schrödinger Bridge.” SIAM Rev. 63 (2021): 249-313.
- Chen, Yuan, Soummya Kar and José M. F. Moura. “The Internet of Things: Secure Distributed Inference.” IEEE Signal Processing Magazine 35 (2018): 64-75.
- Chen, Yufei, Chao Shen, Cong Wang and Yang Zhang. “Teacher Model Fingerprinting Attacks Against Transfer Learning.” ArXiv abs/2106.12478 (2021): n. pag.
- Chen, Zhaoyu, Bo Li, Jianghe Xu, Shuang Wu, Shouhong Ding and Wenqiang Zhang. “Towards Practical Certifiable Patch Defense with Vision Transformer.” ArXiv abs/2203.08519 (2022): n. pag.
- Chen, Zhuotong, Qianxiao Li and Zheng Zhang. “Self-Healing Robust Neural Networks via Closed-Loop Control.” ArXiv abs/2206.12963 (2022): n. pag.
- Cheng, Peng, Ibrahim Ethem Bagci, Utz Roedig and Jeff Yan. “SonarSnoop: active acoustic side-channel attacks.” International Journal of Information Security 19 (2019): 213-228.
- Cheng, Sheng, Yi Ren and Yezhou Yang. “SSR-GNNs: Stroke-based Sketch Representation with Graph Neural Networks.” ArXiv abs/2204.13153 (2022): n. pag.
- Chettri, Bhusan, Emmanouil Benetos and Bob L. Sturm. “Dataset Artefacts in Anti-Spoofing Systems: A Case Study on the ASVspoof 2017 Benchmark.” IEEE/ACM Transactions on Audio, Speech, and Language Processing 28 (2020): 3018-3028.
- Chi, Haotian, Qiang Zeng, Xiaojiang Du and Lannan Luo. “PFirewall: Semantics-Aware Customizable Data Flow Control for Home Automation Systems.” ArXiv abs/1910.07987 (2019): n. pag.
- Chi, Haotian, Qiang Zeng, Xiaojiang Du and Lannan Luo. “PFirewall: Semantics-Aware Customizable Data Flow Control for Smart Home Privacy Protection.” ArXiv abs/2101.10522 (2021): n. pag.
- Chi, Jianfeng, Emmanuel Owusu, Xuwang Yin, Tong Yu, William Chan, Patrick Tague and Yuan Tian. “Privacy Partitioning: Protecting User Data During the Deep Learning Inference Phase.” ArXivabs/1812.02863 (2018): n. pag.

- Chien, Tiffany and Jugal Kumar Kalita. “Adversarial Analysis of Natural Language Inference Systems.” 2020 IEEE 14th International Conference on Semantic Computing (ICSC) (2020): 1-8.
- Cho, Won Ik, Sangwhan Moon, Jong In Kim, Seokhwan Kim and Nam Soo Kim. “StyleKQC: A Style-Variant Paraphrase Corpus for Korean Questions and Commands.” ArXiv abs/2103.13439 (2021): n. pag.
- Choi, Taejun, Guangdong Bai, Ryan Kok Leong Ko, Naipeng Dong, Wenlu Zhang and Shunyao Wang. “An Analytics Framework for Heuristic Inference Attacks against Industrial Control Systems.” 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) (2020): 827-835.
- Choquette-Choo, Christopher A., Florian Tramèr, Nicholas Carlini and Nicolas Papernot. “Label-Only Membership Inference Attacks.” ICML (2021).
- Chou, Edward, Thao Nguyen, Josh Beal, Albert Haque and Li Fei-Fei. “A Fully Private Pipeline for Deep Learning on Electronic Health Records.” ArXiv abs/1811.09951 (2018): n. pag.
- Chourasia, Rishav, Batnyam Enkhtaivan, Kunihiro Ito, Junki Mori, Isamu Teranishi and Hikaru Tsuchida. “Knowledge Cross-Distillation for Membership Privacy.” Proceedings on Privacy Enhancing Technologies 2022 (2022): 362 - 377.
- Chowdhury, Amrita Roy, Bolin Ding, Somesh Jha, Weiran Liu and Jingren Zhou. “Strengthening Order Preserving Encryption with Differential Privacy.” (2020).
- Chowdhuryy, Md Hafizul Islam and Fan Yao. “Leaking Secrets through Modern Branch Predictor in the Speculative World.” ArXiv abs/2107.09833 (2021): n. pag.
- Chundawat, Vikram S, Ayush K Tarun, Murari Mandal and Mohan S. Kankanhalli. “Zero-Shot Machine Unlearning.” ArXiv abs/2201.05629 (2022): n. pag.
- Cohen, Gilad and Raja Giryes. “Membership Inference Attack Using Self Influence Functions.” ArXiv abs/2205.13680 (2022): n. pag.
- Comiter, Marcus Z., Surat Teerapittayanon and H. T. Kung. “CheckNet: Secure Inference on Untrusted Devices.” ArXiv abs/1906.07148 (2019): n. pag.
- Creţu, Ana-Maria, Florent Guépin and Yves-Alexandre de Montjoye. “Dataset correlation inference attacks against machine learning models.” ArXiv abs/2112.08806 (2021): n. pag.
- Cui, Shujie, Xiangfu Song, Muhammad Rizwan Asghar, Steven D. Galbraith and Giovanni Russello. “Privacy-preserving Searchable Databases with Controllable Leakage.” ArXiv abs/1909.11624 (2019): n. pag.
- Cui, Yufei, Wuguannan Yao, Qiao Li, Antoni B. Chan and Chun Jason Xue. “Accelerating Monte Carlo Bayesian Inference via Approximating Predictive Uncertainty over Simplex.” ArXivabs/1905.12194 (2019): n. pag.
- Cunningham, Teddy, Graham Cormode and Hakan Ferhatosmanoğlu. “Privacy-Preserving Synthetic Location Data in the Real World.” 17th International Symposium on Spatial and Temporal Databases (2021): n. pag.
- Dai, Tianxiang and Haya Shulman. “SMap: Internet-wide Scanning for Ingress Filtering.” ArXivabs/2003.05813 (2020): n. pag.
- Daluwatta, Wathsara, Ravindu De Silva, Sanduni Kariyawasam, Mohamed Nabeel, Charitha Elvitigala, Kasun De Zoysa and Chamath Keppitiyagama. “CGraph: Graph Based Extensible Predictive Domain Threat Intelligence Platform.” ArXiv abs/2202.07883 (2022): n. pag.

- Dam, Khanh-Huu-The, Charles-Henry Bertrand Van Ouytsel and Axel Legay. “Symbolic analysis meets federated learning to enhance malware identifier.” ArXiv abs/2204.14159 (2022): n. pag.
- Datta, Siddhartha and Nigel Shadbolt. “Hiding Behind Backdoors: Self-Obfuscation Against Generative Models.” ArXiv abs/2201.09774 (2022): n. pag.
- Datta, Siddhartha, Giulio Lovisotto, Ivan Martinovic and Nigel Shadbolt. “Widen The Backdoor To Let More Attackers In.” ArXiv abs/2110.04571 (2021): n. pag.
- Däubener, Sina and Asja Fischer. “How Sampling Impacts the Robustness of Stochastic Neural Networks.” ArXiv abs/2204.10839 (2022): n. pag.
- Däubener, Sina and Asja Fischer. “Investigating maximum likelihood based training of infinite mixtures for uncertainty quantification.” ArXiv abs/2008.03209 (2020): n. pag.
- Davaslioglu, Kemal and Yalin Evren Sagduyu. “Trojan Attacks on Wireless Signal Classification with Adversarial Machine Learning.” 2019 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN) (2019): 1-6.
- Dawson, Glenn, Muhammad Umer and Robi Polikar. “Contributor-Aware Defenses Against Adversarial Backdoor Attacks.” ArXiv abs/2206.03583 (2022): n. pag.
- Delaney, Anne Marie, Eoin Brophy and Tomas E. Ward. “Synthesis of Realistic ECG using Generative Adversarial Networks.” ArXiv abs/1909.09150 (2019): n. pag.
- Derakhshan, Farzaneh, Stephanie Balzer and Limin Jia. “Session Logical Relations for Noninterference.” 2021 36th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)(2021): 1-14.
- Dessouky, Ghada, Tommaso Frassetto and Ahmad-Reza Sadeghi. “HybCache: Hybrid Side-Channel-Resilient Caches for Trusted Execution Environments.” ArXiv abs/1909.09599 (2020): n. pag.
- Dhir, Neil, Henrique Hoeltgebaum, Niall M. Adams, Mark Briers, Anthony Burke and Paul Jones. “Prospective Artificial Intelligence Approaches for Active Cyber Defence.” ArXiv abs/2104.09981 (2021): n. pag.
- Ding, Jiayu, Siyuan Wang, Qin Chen and Zhongyu Wei. “Reasoning Chain Based Adversarial Attack for Multi-hop Question Answering.” ArXiv abs/2112.09658 (2021): n. pag.
- Dixit, Siddharth, Meghna Chaudhary and Niteesh Sahni. “Network Learning Approaches to study World Happiness.” ArXiv abs/2007.09181 (2020): n. pag.
- Dong, Caiqin, Jian Weng, Yao Tong, Jianan Liu, Anjia Yang, Yudan Cheng and Shun Hu. “Fusion: Efficient and Secure Inference Resilient to Malicious Server and Curious Clients.” ArXivabs/2205.03040 (2022): n. pag.
- Dong, Shuaike, Zhou Li, Di Tang, Jiongyi Chen, Menghan Sun and Kehuan Zhang. “Your Smart Home Can’t Keep a Secret: Towards Automated Fingerprinting of IoT Traffic.” Proceedings of the 15th ACM Asia Conference on Computer and Communications Security (2020): n. pag.
- Dong, Tian, Bo Zhao and Lingjuan Lyu. “Privacy for Free: How does Dataset Condensation Help Privacy?” ICML (2022).
- Dong, Xinhsuai, Anh Tuan Luu, Min Lin, Shuicheng Yan and Hanwang Zhang. “How Should Pre-Trained Language Models Be Fine-Tuned Towards Adversarial Robustness?” NeurIPS (2021).
- Dong, Xinshuai, Anh Tuan Luu, Rongrong Ji and Hong Liu. “Towards Robustness Against Natural Language Word Substitutions.” ArXiv abs/2107.13541 (2021): n. pag.
- Dong, Yinpeng, Xiao Yang, Zhijie Deng, Tianyu Pang, Zihao Xiao, Hang Su and Jun Zhu. “Black-box Detection of Backdoor Attacks with Limited Information and

Data." 2021 IEEE/CVF International Conference on Computer Vision (ICCV) (2021): 16462-16471.
- Doostmohammadian, Mohammadreza, Themistoklis Charalambous, Miadreza Shafie-khah, Nader Meskin and Usman A. Khan. "Simultaneous Distributed Estimation and Attack Detection/Isolation in Social Networks: Structural Observability, Kronecker-Product Network, and Chi-Square Detector." 2021 IEEE International Conference on Autonomous Systems (ICAS) (2021): 1-5.
- Dou, Yongqiang, Haocheng Yang, Maolin Yang, Yanyan Xu and Dengfeng Ke. "Dynamically Mitigating Data Discrepancy with Balanced Focal Loss for Replay Attack Detection." 2020 25th International Conference on Pattern Recognition (ICPR) (2021): 4115-4122.
- Doumanidis, Constantine, Prashant Hari Narayan Rajput, Michail Maniatakos New York University Abu Dhabi and Nyu Tandon School of Engineering. "ICSML: Industrial Control Systems Machine Learning Inference Framework natively executing on IEC 61131-3 compliant devices." (2022).
- Du, Haitao and Shanchieh Jay Yang. "Probabilistic Modeling and Inference for Obfuscated Cyber Attack Sequences." ArXiv abs/1809.01562 (2018): n. pag.
- Du, Jiawei, Hu Zhang, Joey Tianyi Zhou, Yi Yang and Jiashi Feng. "Query-efficient Meta Attack to Deep Neural Networks." ArXiv abs/1906.02398 (2020): n. pag.
- Duan, Shijin, Shaolei Ren and Xiaolin Xu. "HDLock: Exploiting Privileged Encoding to Protect Hyperdimensional Computing Models against IP Stealing." ArXiv abs/2203.09681 (2022): n. pag.
- Duan, Xiaoming, Zhe Xu, Rui Yan and Ufuk Topcu. "Privacy-Utility Trade-Offs Against Limited Adversaries." ArXiv abs/2106.14643 (2021): n. pag.
- Dubey, Anuj, Rosario Cammarota and Aydin Aysu. "BoMaNet: Boolean Masking of an Entire Neural Network." 2020 IEEE/ACM International Conference On Computer Aided Design (ICCAD) (2020): 1-9.
- Dubey, Anuj, Rosario Cammarota and Aydin Aysu. "MaskedNet: The First Hardware Inference Engine Aiming Power Side-Channel Protection." 2020 IEEE International Symposium on Hardware Oriented Security and Trust (HOST) (2020): 197-208.
- Duddu, Vasisht and D. Vijay Rao. "Quantifying (Hyper) Parameter Leakage in Machine Learning." 2020 IEEE Sixth International Conference on Multimedia Big Data (BigMM) (2020): 239-244.
- Duddu, Vasisht, Antoine Boutet and Virat Shejwalkar. "GECKO: Reconciling Privacy, Accuracy and Efficiency in Embedded Deep Learning." ArXiv abs/2010.00912 (2020): n. pag.
- Duddu, Vasisht, Antoine Boutet and Virat Shejwalkar. "Quantifying Privacy Leakage in Graph Embedding." MobiQuitous 2020 - 17th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (2020): n. pag.
- Duddu, Vasisht, Debasis Samanta, D. Vijay Rao and Valentina Emilia Balas. "Stealing Neural Networks via Timing Side Channels." ArXiv abs/1812.11720 (2018): n. pag.
- Duddu, Vasisht, Sebastian Szyller and N. Asokan. "SHAPr: An Efficient and Versatile Membership Privacy Risk Metric for Machine Learning." ArXiv abs/2112.02230 (2021): n. pag.
- Dumont, Mathieu, Pierre-Alain Moellic, Raphael Andreoni Camponogara Viera, Jean-Max Dutertre and Rémi Bernhard. "An Overview of Laser Injection against Embedded Neural Network Models." 2021 IEEE 7th World Forum on Internet of Things (WF-IoT) (2021): 616-621.

- Dupuy, Christophe, Radhika Arava, Rahul Gupta and Anna Rumshisky. “An Efficient DP-SGD Mechanism for Large Scale NLP Models.” ICASSP (2022).
- Dutta, Sankha Baran, Hoda Naghibijouybari, Arjun Gupta, Nael CSE and ECE Abu-Ghazaleh, Andrés Márquez and Kevin J. Barker. “Spy in the GPU-box: Covert and Side Channel Attacks on Multi-GPU Systems.” ArXiv abs/2203.15981 (2022): n. pag.
- Dziedzic, Adam, Nikita Dhawan, Muhammad Ahmad Kaleem, Jonas Guan and Nicolas Papernot. “On the Difficulty of Defending Self-Supervised Learning against Model Extraction.” ICML (2022).
- Elinas, Pantelis, Edwin V. Bonilla and Louis C. Tiao. “Variational Inference for Graph Convolutional Networks in the Absence of Graph Data and Adversarial Settings.” arXiv: Learning (2020): n. pag.
- Emmery, Chris, ‘Akos K’ad’ar and Grzegorz Chrupała. “Adversarial Stylometry in the Wild: Transferable Lexical Substitution Attacks on Author Profiling.” EACL (2021).
- Erdogan, Ege, Alptekin Kupcu and A. Ercument Cicek. “UnSplit: Data-Oblivious Model Inversion, Model Stealing, and Label Inference Attacks Against Split Learning.” ArXiv abs/2108.09033 (2021): n. pag.
- Fachkha, Claude. “Security Monitoring of the Cyber Space.” ArXiv abs/1608.01468 (2016): n. pag.
- Fan, Cheng, Ziao Li and Wei Wei. “Gradient-guided Unsupervised Text Style Transfer via Contrastive Learning.” ArXiv abs/2202.00469 (2022): n. pag.
- Fan, Lixin, Kam Woh Ng and Chee Seng Chan. “Rethinking Deep Neural Network Ownership Verification: Embedding Passports to Defeat Ambiguity Attacks.” ArXiv abs/1909.07830 (2019): n. pag.
- Fandinno, Jorge and Luis Fariñas del Cerro. “Abstract argumentation and answer set programming: two faces of Nelson’s logic.” ArXiv abs/2203.14405 (2022): n. pag.
- Fang, Meiling, Fadi Boutros, Arjan Kuijper and Naser Damer. “Partial Attack Supervision and Regional Weighted Inference for Masked Face Presentation Attack Detection.” 2021 16th IEEE International Conference on Automatic Face and Gesture Recognition (FG 2021) (2021): 1-8.
- Farokhi, Farhad and Mohamed Ali Kâafar. “Modelling and Quantifying Membership Information Leakage in Machine Learning.” ArXiv abs/2001.10648 (2020): n. pag.
- Farrukh, Habiba, Tinghan Yang, Hanwen Xu, Yuxuan Yin, He Wang and Z. Berkay Celik. “S3: Side-Channel Attack on Stylus Pencil through Sensors.” Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. 5 (2021): 8:1-8:25.
- Fauvelle, Jean-Philippe, A. Dey and Sylvain Navers. “Protection d’un système d’information par une intelligence artificielle : une approche en trois phases basée sur l’analyse UEBA des comportements pour détecter un scénario hostile.” (2019).
- Felps, Daniel, Amelia D. Schwickerath, Joyce D. Williams, Trung N. Vuong, Alan Briggs, M. Hunt, Evan Sakmar, David D. Saranchak and Tyler Shumaker. “Bootstrap Aggregation for Point-based Generalized Membership Inference Attacks.” ArXiv abs/2011.08738 (2020): n. pag.
- Felps, Daniel, Amelia D. Schwickerath, Joyce D. Williams, Trung N. Vuong, Alan Briggs, M. Hunt, Evan Sakmar, David D. Saranchak and Tyler Shumaker. “Class Clown: Data Redaction in Machine Unlearning at Enterprise Scale.” ICORES (2021).
- Feng, Tiantian, Hanieh Hashemi, Rajat Hebbar, Murali Annavaram and Shrikanth S. Narayanan. “Attribute Inference Attack of Speech Emotion Recognition in Federated Learning Settings.” ArXivabs/2112.13416 (2021): n. pag.

- Feng, Tiantian, Raghuveer Peri and Shrikanth S. Narayanan. “User-Level Differential Privacy against Attribute Inference Attack of Speech Emotion Recognition in Federated Learning.” ArXivabs/2204.02500 (2022): n. pag.
- Feng, Xuewei, Chuanpu Fu, Qi Li, Kun Sun and Ke Xu. “Off-Path TCP Exploits of the Mixed IPID Assignment.” Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (2020): n. pag.
- Franci, Adriano, Maxime Cordy, Martin Gubri, Mike Papadakis and Yves Le Traon. “Influence-Driven Data Poisoning in Graph-Based Semi-Supervised Classifiers.” 2022 IEEE/ACM 1st International Conference on AI Engineering – Software Engineering for AI (CAIN) (2022): 77-87.
- Francis, Paul L.. “A Note on the Misinterpretation of the US Census Re-identification Attack.” ArXivabs/2202.04872 (2022): n. pag.
- Francis, Sreya, Irene Tenison and Irina Rish. “Towards Causal Federated Learning For Enhanced Robustness and Privacy.” ArXiv abs/2104.06557 (2021): n. pag.
- Frank, Mario, Tiffany Hwu, Sakshi Jain, Robert T. Knight, Ivan Martinovic, Prateek Mittal, Daniele Perito and Dawn Xiaodong Song. “Subliminal Probing for Private Information via EEG-Based BCI Devices.” ArXiv abs/1312.6052 (2013): n. pag.
- Franzoni, Federico, Xavier Salleras and Vanesa Daza. “AToM: Active topology monitoring for the bitcoin peer-to-peer network.” Peer-to-Peer Networking and Applications 15 (2022): 408-425.
- Gadotti, Andrea, Florimond Houssiau, Luc Rocher, Benjamin Livshits and Yves-Alexandre de Montjoye. “When the Signal is in the Noise: Exploiting Diffix’s Sticky Noise.” USENIX Security Symposium (2019).
- Gal, Yarin and Lewis Smith. “Sufficient Conditions for Idealised Models to Have No Adversarial Examples: a Theoretical and Empirical Study with Bayesian Neural Networks.” arXiv: Machine Learning (2018): n. pag.
- Galinkin, Erick. “The Influence of Dropout on Membership Inference in Differentially Private Models.” ArXiv abs/2103.09008 (2021): n. pag.
- Galinkin, Erick. “Who’s Afraid of Thomas Bayes?” ArXiv abs/2107.14601 (2021): n. pag.
- Gálvez, Rafa, Veelasha Moonsamy and Claudia Díaz. “Less is More: A privacy-respecting Android malware classifier using federated learning.” Proceedings on Privacy Enhancing Technologies2021 (2021): 96 - 116.
- Gan, Yiming, Yuxian Qiu, Jingwen Leng, Minyi Guo and Yuhao Zhu. “Ptolemy: Architecture Support for Robust Deep Learning.” 2020 53rd Annual IEEE/ACM International Symposium on Microarchitecture (MICRO) (2020): 241-255.
- Gao, Ji, Sanjam Garg, Mohammad Mahmoody and Prashant Nalini Vasudevan. “Deletion Inference, Reconstruction, and Compliance in Machine (Un)Learning.” ArXiv abs/2202.03460 (2022): n. pag.
- Gao, Pengfei, Hongyi Xie, Fu Song and Taolue Chen. “A Hybrid Approach to Formal Verification of Higher-Order Masked Arithmetic Programs.” ACM Transactions on Software Engineering and Methodology (TOSEM) 30 (2021): 1 - 42.
- Gao, Pengfei, Hongyi Xie, Jun Zhang, Fu Song and Taolue Chen. “Quantitative Verification of Masked Arithmetic Programs against Side-Channel Attacks.” TACAS (2019).
- Gao, Yue, Ilia Shumailov, Kassem Fawaz and Nicolas Papernot. “On the Limitations of Stochastic Pre-processing Defenses.” ArXiv abs/2206.09491 (2022): n. pag.

- Garcia, Washington, Joseph I. Choi, Suman Kalyan Adari, Somesh Jha and Kevin R. B. Butler. “Explainable Black-Box Attacks Against Model-based Authentication.” ArXiv abs/1810.00024 (2018): n. pag.
- Gazzari, Matthias, Annemarie Mattmann, Max Maass and Matthias Hollick. “My(o) Armband Leaks Passwords.” Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 5 (2021): 1 - 24.
- Geiping, Jonas, Liam Fowl, Gowthami Somepalli, Micah Goldblum, Michael Moeller and Tom Goldstein. “What Doesn’t Kill You Makes You Robust(er): How to Adversarially Train against Data Poisoning.” (2021).
- Geng, Jiahui, Yongli Mou, Feifei Li, Qing Li, Oya Deniz Beyan, Stefan Decker and Chunming Rong. “Towards General Deep Leakage in Federated Learning.” ArXiv abs/2110.09074 (2021): n. pag.
- Genkin, Daniel, Mihir Pattani, R. Schuster and Eran Tromer. “Synesthesia: Detecting Screen Content via Remote Acoustic Side Channels.” 2019 IEEE Symposium on Security and Privacy (SP)(2019): 853-869.
- Giaconi, Giulio, Deniz Gunduz and H. Vincent Poor. “Privacy-Aware Smart Metering: Progress and Challenges.” IEEE Signal Processing Magazine 35 (2018): 59-78.
- Giudice, Oliver, Luca Guarnera and Sebastiano Battiato. “Fighting Deepfakes by Detecting GAN DCT Anomalies.” Journal of Imaging 7 (2021): n. pag.
- Gokhale, Tejas, Abhishek Chaudhary, Pratyay Banerjee, Chitta Baral and Yezhou Yang. “Semantically Distributed Robust Optimization for Vision-and-Language Inference.” FINDINGS(2022).
- Goldsteen, Abigail, Gilad Ezov and Ariel Farkash. “Reducing Risk of Model Inversion Using Privacy-Guided Training.” ArXiv abs/2006.15877 (2020): n. pag.
- Goldsteen, Abigail, Gilad Ezov, Ron Shmelkin, Micha Moffie and Ariel Farkash. “Anonymizing Machine Learning Models.” DPM/CBT@ESORICS (2021).
- Gomrokchi, Maziar, Susan Amin, Hossein Aboutalebi, Alexander Wong and Doina Precup. “Where Did You Learn That From? Surprising Effectiveness of Membership Inference Attacks Against Temporally Correlated Data in Deep Reinforcement Learning.” ArXiv abs/2109.03975 (2021): n. pag.
- Gong, Neil Zhenqiang and Bin Liu. “You Are Who You Know and How You Behave: Attribute Inference Attacks via Users’ Social Friends and Behaviors.” ArXiv abs/1606.05893 (2016): n. pag.
- Graves, Laura, Vineel Nagisetty and Vijay Ganesh. “Amnesiac Machine Learning.” AAAI (2021).
- Grizou, Jonathan. “IFTT-PIN: A PIN-Entry Method Leveraging the Self-Calibration Paradigm.” ArXivabs/2205.09534 (2022): n. pag.
- Grosse, Kathrin, David Pfaff, Michael Thomas Smith and Michael Backes. “How Wrong Am I? - Studying Adversarial Examples and their Impact on Uncertainty in Gaussian Process Machine Learning Models.” ArXiv abs/1711.06598 (2017): n. pag.
- Grosse, Kathrin, Michael Thomas Smith and Michael Backes. “Killing Four Birds with one Gaussian Process: The Relation between different Test-Time Attacks.” 2020 25th International Conference on Pattern Recognition (ICPR) (2021): 4696-4703.
- Grosso, Ganesh Del, Georg Pichler and Pablo Piantanida. “Privacy-Preserving Synthetic Smart Meters Data.” 2021 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT) (2021): 1-5.

- Grosso, Ganesh Del, Georg Pichler, Catuscia Palamidessi and Pablo Piantanida. “Bounding Information Leakage in Machine Learning.” ArXiv abs/2105.03875 (2021): n. pag.
- Grover, Karan, Shruti Tople, Shweta Shinde, Ranjita Bhagwan and Ramachandran Ramjee. “Privado: Practical and Secure DNN Inference with Enclaves.” arXiv: Cryptography and Security(2018): n. pag.
- Guan, Jiyang, Zhuozhuo Tu, Ran He and Dacheng Tao. “Few-shot Backdoor Defense Using Shapley Estimation.” ArXiv abs/2112.14889 (2021): n. pag.
- Gui, Tao, Xiao Wang, Qi Zhang, Qin Liu, Yicheng Zou, Xin Zhou, Rui Zheng, Chong Zhang, Qinzhuo Wu, Jiacheng Ye, Zexiong Pang, Yongxin Zhang, Zhengyan Li, Ruotian Ma, Zichu Fei, Ruijian Cai, Jun Zhao, Xinwu Hu, Zhiheng Yan, Yiding Tan, Yuan Hu, Qiyuan Bian, Zhihua Liu, Bolin Zhu, Shan Qin, Xiaoyu Xing, Jinlan Fu, Yue Zhang, Minlong Peng, Xiaoqing Zheng, Yaqian Zhou, Zhongyu Wei, Xipeng Qiu and Xuanjing Huang. “TextFlint: Unified Multilingual Robustness Evaluation Toolkit for Natural Language Processing.” ACL (2021).
- Gülmezoglu, Berk, Andreas Zankl, M. Caner Tol, Saad Islam, Thomas Eisenbarth and Berk Sunar. “Undermining User Privacy on Mobile Devices Using AI.” Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security (2019): n. pag.
- Gülmezoglu, Berk, Andreas Zankl, Thomas Eisenbarth and Berk Sunar. “PerfWeb: How to Violate Web Privacy with Hardware Performance Events.” ArXiv abs/1705.04437 (2017): n. pag.
- Guo, Chuan, Brian Karrer, Kamalika Chaudhuri and Laurens van der Maaten. “Bounding Training Data Reconstruction in Private (Deep) Learning.” ICML (2022).
- Guo, Jianxiong and Weili Wu. “Differential Privacy-Based Online Allocations towards Integrating Blockchain and Edge Computing.” ArXiv abs/2101.02834 (2021): n. pag.
- Guo, Jianxiong, Xingjian Ding and Weijia Jia. “Combinatorial Resources Auction in Decentralized Edge-Thing Systems Using Blockchain and Differential Privacy.” ArXiv abs/2108.05567 (2022): n. pag.
- Guo, Pengxin, Yuancheng Xu, Baijiong Lin and Yu Zhang. “Multi-Task Adversarial Attack.” ArXivabs/2011.09824 (2020): n. pag.
- Gupta, Umang, Dmitris Stripelis, Pradeep K. Lam, Paul M. Thompson, J. Ambite and Greg Ver Steeg. “Membership Inference Attacks on Deep Regression Models for Neuroimaging.” MIDL(2021).
- Gurulingan, Naresh, E. Arani and Bahram Zonooz. “UniNet: A Unified Scene Understanding Network and Exploring Multi-Task Relationships through the Lens of Adversarial Attacks.” 2021 IEEE/CVF International Conference on Computer Vision Workshops (ICCVW) (2021): 2239-2248.
- Hafeez, Khadija, Donna OShea and Mubashir Husain Rehmani. “E-DPNCT: An Enhanced Attack Resilient Differential Privacy Model For Smart Grids Using Split Noise Cancellation.” ArXivabs/2110.11091 (2021): n. pag.
- Haghani, Naveen, Julian Yarkony and Amelia Regan. “Family Column Generation: A Principled Stabilized Column Generation Approach.” ArXiv abs/2103.15234 (2021): n. pag.
- Hamidouche, Mounia, Reda Bellafqira, Gwénolé Quellec and Gouenou Coatrieux. “White-box Membership Attack Against Machine Learning Based Retinopathy Classification.” ArXivabs/2206.03584 (2022): n. pag.

- Hamm, Jihun. “Minimax Filter: Learning to Preserve Privacy from Inference Attacks.” J. Mach. Learn. Res. 18 (2017): 129:1-129:31.
- Han, Jesse Michael. “Enhancing SAT solvers with glue variable predictions.” ArXivabs/2007.02559 (2020): n. pag.
- Han, Xiao, Leye Wang, Junjie Wu and Yuncong Yang. “Large-Scale Privacy-Preserving Network Embedding against Private Link Inference Attacks.” ArXiv abs/2205.14440 (2022): n. pag.
- Han, Xiao, Yuncong Yang and Junjie Wu. “HyObscure: Hybrid Obscuring for Privacy-Preserving Data Publishing.” ArXiv abs/2112.07850 (2021): n. pag.
- Hanzlik, Lucjan, Yang Zhang, Kathrin Grosse, A. Salem, Maximilian Augustin, Michael Backes and Mario Fritz. “MLCapsule: Guarded Offline Deployment of Machine Learning as a Service.” 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW) (2021): 3295-3304.
- Harsha, Benjamin, Robert Morton, Jeremiah Blocki, John A. Springer and Melissa Jane Dark. “Bicycle Attacks Considered Harmful: Quantifying the Damage of Widespread Password Length Leakage.” Comput. Secur. 100 (2021): 102068.
- Hashemi, Hanieh, Yongqin Wang and Murali Annavaram. “DarKnight: An Accelerated Framework for Privacy and Integrity Preserving Deep Learning Using Trusted Hardware.” MICRO-54: 54th Annual IEEE/ACM International Symposium on Microarchitecture (2021): n. pag.
- Hassanzadeh, Parisa and Robert E. Tillman. “Generative Models with Information-Theoretic Protection Against Membership Inference Attacks.” ArXiv abs/2206.00071 (2022): n. pag.
- Haydari, Ammar, H. Michael Zhang, Chen-Nee Chuah, Jane MacFarlane and Sean Peisert. “Adaptive Differential Privacy Mechanism for Aggregated Mobility Dataset.” ArXivabs/2112.08487 (2021): n. pag.
- Hayes, Jamie and George Danezis. “k-fingerprinting: A Robust Scalable Website Fingerprinting Technique.” USENIX Security Symposium (2016).
- Hayes, Jamie and Olga Ohrimenko. “Contamination Attacks and Mitigation in Multi-Party Machine Learning.” NeurIPS (2018).
- Hayes, Jamie, Luca Melis, George Danezis and Emiliano De Cristofaro. “LOGAN: Membership Inference Attacks Against Generative Models.” Proceedings on Privacy Enhancing Technologies2019 (2019): 133 - 152.
- He, Chen, Kan Ming, Yongwei Wang and Z. Jane Wang. “A Deep Learning Based Attack for The Chaos-based Image Encryption.” ArXiv abs/1907.12245 (2019): n. pag.
- He, Jianping, Yushan Li, Lingbin Cai and Xinping Guan. “I Can Read Your Mind: Control Mechanism Secrecy of Networked Dynamical Systems under Inference Attacks.” ArXivabs/2205.03556 (2022): n. pag.
- He, Xinlei and Yang Zhang. “Quantifying and Mitigating Privacy Risks of Contrastive Learning.” Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security(2021): n. pag.
- He, Xinlei, Jinyuan Jia, Michael Backes, Neil Zhenqiang Gong and Yang Zhang. “Stealing Links from Graph Neural Networks.” ArXiv abs/2005.02131 (2021): n. pag.
- He, Xinlei, Rui Wen, Yixin Wu, Michael Backes, Yun Shen and Yang Zhang. “Node-Level Membership Inference Attacks Against Graph Neural Networks.” ArXiv abs/2102.05429 (2021): n. pag.

- He, Yang, Shadi Rahimian, Bernt Schiele and Mario Fritz. “Segmentations-Leak: Membership Inference Attacks and Defenses in Semantic Image Segmentation.” ECCV (2020).
- He, Ziwen, Wei Wang, Jing Dong and Tieniu Tan. “Transferable Sparse Adversarial Attack.” ArXivabs/2105.14727 (2021): n. pag.
- Hecht, Pedro. “Algebraic Extension Ring Framework for Non-Commutative Asymmetric Cryptography.” ArXiv abs/2002.08343 (2020): n. pag.
- Hemberg, Erik and Una-May O’Reilly. “Using a Collated Cybersecurity Dataset for Machine Learning and Artificial Intelligence.” ArXiv abs/2108.02618 (2021): n. pag.
- Heo, Geon and Steven Euijong Whang. “Redactor: Targeted Disinformation Generation using Probabilistic Decision Boundaries.” ArXiv abs/2202.02902 (2022): n. pag.
- Hidano, Seira, Yusuke Kawamoto and Takao Murakami. “TransMIA: Membership Inference Attacks Using Transfer Shadow Training.” 2021 International Joint Conference on Neural Networks (IJCNN) (2021): 1-10.
- Hilprecht, Benjamin, Martin Härterich and Daniel Bernau. “Reconstruction and Membership Inference Attacks against Generative Models.” ArXiv abs/1906.03006 (2019): n. pag.
- Hintersdorf, Dominik, Lukas Struppek and Kristian Kersting. “To Trust or Not To Trust Prediction Scores for Membership Inference Attacks.” Proceedings of the Thirty-First International Joint Conference on Artificial Intelligence (2022): n. pag.
- Hisamoto, Sorami, Matt Post and Kevin Duh. “Membership Inference Attacks on Sequence-to-Sequence Models: Is My Data In Your Machine Translation System?” Transactions of the Association for Computational Linguistics 8 (2020): 49-63.
- Ho, Grant, Mayank Dhiman, Devdatta Akhawe, Vern Paxson, Stefan Savage, Geoffrey M. Voelker and David A. Wagner. “Hopper: Modeling and Detecting Lateral Movement (Extended Report).” ArXiv abs/2105.13442 (2021): n. pag.
- Hoang, Nguyen Phong. “Towards an Autonomous System Monitor for Mitigating Correlation Attacks in the Tor Network.” ArXiv abs/1610.02065 (2016): n. pag.
- Hoang, Thi-Nu and Dae Hoe Kim. “Detecting In-vehicle Intrusion via Semi-supervised Learning-based Convolutional Adversarial Autoencoders.” ArXiv abs/2204.01193 (2022): n. pag.
- Hong, Chi, Jiyue Huang and Lydia Yiyu Chen. “MEGA: Model Stealing via Collaborative Generator-Substitute Networks.” ArXiv abs/2202.00008 (2022): n. pag.
- Hong, Sanghyun, Michael Davinroy, Yigitcan Kaya, Dana Dachman-Soled and Tudor Dumitras. “How to 0wn NAS in Your Spare Time.” ArXiv abs/2002.06776 (2020): n. pag.
- Hong, Sanghyun, Michael Panaitescu-Liess, Yigitcan Kaya and Tudor Dumitras. “Qu-ANTI-zation: Exploiting Quantization Artifacts for Achieving Adversarial Outcomes.” ArXiv abs/2110.13541 (2021): n. pag.
- Hong, Sanghyun, Yigitcan Kaya, Ionut-Vlad Modoranu and Tudor Dumitras. “A Panda? No, It’s a Sloth: Slowdown Attacks on Adaptive Multi-Exit Neural Network Inference.” ArXiv abs/2010.02432 (2021): n. pag.
- Hoskins, Jeremy G., Cameron Musco, Christopher Musco and Charalampos E. Tsourakakis. “Learning Networks from Random Walk-Based Node Similarities.” ArXiv abs/1801.07386 (2018): n. pag.

- Hossain, Md Tamjid, Shahriar Badsha, Hung La, Haoting Shen, Shafkat Islam, Ibrahim Khalil and X. Yi. “Adversarial Analysis of the Differentially-Private Federated Learning in Cyber-Physical Critical Infrastructures.” ArXiv abs/2204.02654 (2022): n. pag.
- Hsieh, I-Chung and Cheng-te Li. “NetFense: Adversarial Defenses against Privacy Attacks on Neural Networks for Graph Data.” ArXiv abs/2106.11865 (2021): n. pag.
- Hsiung, Lei, Yun-Yun Tsai, Pin-Yu Chen and Tsung-Yi Ho. “CARBEN: Composite Adversarial Robustness Benchmark.” Proceedings of the Thirty-First International Joint Conference on Artificial Intelligence (2022): n. pag.
- Hu, Aoting, Renjie Xie, Zhigang Lu, Aiqun Hu and Minhui Xue. “TableGAN-MCA: Evaluating Membership Collisions of GAN-Synthesized Tabular Data Releasing.” Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (2021): n. pag.
- Hu, Guangneng and Qiang Yang. “PrivNet: Safeguarding Private Attributes in Transfer Learning for Recommendation.” ArXiv abs/2010.08187 (2020): n. pag.
- Hu, Hongsheng, Zoran A. Salcic, Gillian Dobbie and Xuyun Zhang. “Membership Inference Attacks on Machine Learning: A Survey.” ACM Computing Surveys (CSUR) (2022): n. pag.
- Hu, Hongsheng, Zoran A. Salcic, Gillian Dobbie, Jinjun Chen, Lichao Sun and Xuyun Zhang. “Membership Inference via Backdooring.” ArXiv abs/2206.04823 (2022): n. pag.
- Hu, Hongsheng, Zoran A. Salcic, Lichao Sun, G. Dobbie and Xuyun Zhang. “Source Inference Attacks in Federated Learning.” 2021 IEEE International Conference on Data Mining (ICDM)(2021): 1102-1107.
- Hu, Minghao, Yuxing Peng, Furu Wei, Zhen Huang, Dongsheng Li, Nan Yang and M. Zhou. “Attention-Guided Answer Distillation for Machine Reading Comprehension.” EMNLP (2018).
- Hu, Rui, Yanmin Gong and Yuanxiong Guo. “Federated Learning with Sparsified Model Perturbation: Improving Accuracy under Client-Level Differential Privacy.” ArXiv abs/2202.07178 (2022): n. pag.
- Hu, Ting-Kuei, Tianlong Chen, Haotao Wang and Zhangyang Wang. “Triple Wins: Boosting Accuracy, Robustness and Efficiency Together by Enabling Input-Adaptive Inference.” ArXivabs/2002.10025 (2020): n. pag.
- Huang, Chong, Peter Kairouz, Xiao Chen, L. Sankar and Ram Rajagopal. “Context-Aware Generative Adversarial Privacy.” Entropy 19 (2017): 656.
- Huang, Hongwei, Weiqi Luo, Guoqiang Zeng, Jian Weng, Yue Zhang and Anjia Yang. “DAMIA: Leveraging Domain Adaptation as a Defense against Membership Inference Attacks.” ArXivabs/2005.08016 (2020): n. pag.
- Huang, Shanshi, Hongwu Jiang and Shimeng Yu. “Mitigating Adversarial Attack for Compute-in-Memory Accelerator Utilizing On-chip Finetune.” 2021 IEEE 10th Non-Volatile Memory Systems and Applications Symposium (NVMSA) (2021): 1-6.
- Huang, Shanshi, Xiaochen Peng, Hongwu Jiang, Yandong Luo and Shimeng Yu. “New Security Challenges on Machine Learning Inference Engine: Chip Cloning and Model Reverse Engineering.” arXiv: Signal Processing (2020): n. pag.
- Huang, Shanshi, Xiaochen Peng, Hongwu Jiang, Yandong Luo and Shimeng Yu. “New Security Challenges on Machine Learning Inference Engine: Chip Cloning and Model Reverse Engineering.” arXiv: Signal Processing (2020): n. pag.

- Huang, Wen, Shijie Zhou and Yongjian Liao. “Unexpected Information Leakage of Differential Privacy Due to the Linear Property of Queries.” IEEE Transactions on Information Forensics and Security 16 (2021): 3123-3137.
- Huang, Yong, Wei Wang, Tao Jiang and Qian Zhang. “Detecting Colluding Sybil Attackers in Robotic Networks Using Backscatters.” IEEE/ACM Transactions on Networking 29 (2021): 793-804.
- Huang, Yudi, Ting He, Nilanjan Ray Chaudhuri and Thomas F. La Porta. “Verifiable Failure Localization in Smart Grid under Cyber-Physical Attacks.” ArXiv abs/2101.07129 (2021): n. pag.
- Huang, Yuheng and Yuanchun Li. “Zero-Shot Certified Defense against Adversarial Patches with Vision Transformers.” ArXiv abs/2111.10481 (2021): n. pag.
- Huang, Yujia, James Gornet, Sihui Dai, Zhiding Yu, Tan Nguyen, Doris Y. Tsao and Anima Anandkumar. “Neural Networks with Recurrent Generative Feedback.” ArXiv abs/2007.09200 (2020): n. pag.
- Huang, Yujin and Chunyang Chen. “Smart App Attack: Hacking Deep Learning Models in Android Apps.” IEEE Transactions on Information Forensics and Security 17 (2022): 1827-1840.
- Hui, Bo, Yuchen Yang, Haolin Yuan, Philippe Burlina, Neil Zhenqiang Gong and Yinzhi Cao. “Practical Blind Membership Inference Attack via Differential Comparisons.” ArXivabs/2101.01341 (2021): n. pag.
- Humphries, Thomas, Simon Oya, Lindsey Tulloch, Matthew Rafuse, Ian Goldberg, U. Hengartner and Florian Kerschbaum. “Investigating Membership Inference Attacks under Data Dependencies.” (2020).
- Hussenot, L’eonard, Matthieu Geist and Olivier Pietquin. “CopyCAT: : Taking Control of Neural Policies with Constant Attacks.” AAMAS (2020).
- Hwang, Uiwon, Jaewoo Park, Hyemi Jang, Sungroh Yoon and Nam Ik Cho. “PuVAE: A Variational Autoencoder to Purify Adversarial Examples.” IEEE Access 7 (2019): 126582-126593.
- Hyland, Stephanie L. and Shruti Tople. “An Empirical Study on the Intrinsic Privacy of SGD.” arXiv: Learning (2019): n. pag.
- Ibitoye, Olakunle, Ashraf Matrawy and M. Omair Shafiq. “A GAN-based Approach for Mitigating Inference Attacks in Smart Home Environment.” ArXiv abs/2011.06725 (2020): n. pag.
- Ibrahem, Mohamed I., Mohamed Mahmoud, Mostafa M. Fouda, Fawaz Alsolami, Waleed S. Alasmary and Xuemin Shen. “Privacy Preserving and Efficient Data Collection Scheme for AMI Networks Using Deep Learning.” IEEE Internet of Things Journal 8 (2021): 17131-17146.
- Indrusiak, Leandro Soares, James Harbin and Martha Johanna Sepúlveda. “Side-channel attack resilience through route randomisation in secure real-time Networks-on-Chip.” 2017 12th International Symposium on Reconfigurable Communication-centric Systems-on-Chip (ReCoSoC)(2017): 1-8.
- Islam, Md. Amirul, Matthew Kowal, Konstantinos G. Derpanis and Neil D. B. Bruce. “Feature Binding with Category-Dependant MixUp for Semantic Segmentation and Adversarial Robustness.” arXiv: Computer Vision and Pattern Recognition (2020): n. pag.
- Islam, Md. Amirul, Matthew Kowal, Konstantinos G. Derpanis and Neil D. B. Bruce. “SegMix: Co-occurrence Driven Mixup for Semantic Segmentation and Adversarial Robustness.” ArXivabs/2108.09929 (2021): n. pag.

- Islam, Md. Shohidul, Ihsen Alouani and Khaled N. Khasawneh. “Stochastic-HMDs: Adversarial Resilient Hardware Malware Detectors through Voltage Over-scaling.” ArXiv abs/2103.06936 (2021): n. pag.
- Izmailov, Rauf, Peter Lin, Chris Mesterharm and Samyadeep Basu. “Privacy Leakage Avoidance with Switching Ensembles.” MILCOM 2021 - 2021 IEEE Military Communications Conference (MILCOM) (2021): 981-986.
- Jaeckle, Florian and M. Pawan Kumar. “Generating Adversarial Examples with Graph Neural Networks.” UAI (2021).
- Jagannatha, Abhyuday N., Bhanu Pratap Singh Rawat and Hong Yu. “Membership Inference Attack Susceptibility of Clinical Language Models.” ArXiv abs/2104.08305 (2021): n. pag.
- Jagielski, Matthew, Giorgio Severi, Niklas Pousette Harger and Alina Oprea. “Subpopulation Data Poisoning Attacks.” Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (2021): n. pag.
- Jagielski, Matthew, Stanley Wu, Alina Oprea, Jonathan Ullman and Roxana Geambasu. “How to Combine Membership-Inference Attacks on Multiple Updated Models.” ArXiv abs/2205.06369 (2022): n. pag.
- Jakubik, Johannes, Michael Vossing, Dominik Bar, Nicolas Prollochs and Stefan Feuerriegel. “Online Emotions During the Storming of the U.S. Capitol: Evidence from the Social Media Network Parler.” ArXiv abs/2204.04245 (2022): n. pag.
- Jarin, Ismat and Birhanu Eshete. “DP-UTIL: Comprehensive Utility Analysis of Differential Privacy in Machine Learning.” Proceedings of the Twelfth ACM Conference on Data and Application Security and Privacy (2022): n. pag.
- Jarin, Ismat and Birhanu Eshete. “MIAShield: Defending Membership Inference Attacks via Preemptive Exclusion of Members.” ArXiv abs/2203.00915 (2022): n. pag.
- Jarin, Ismat and Birhanu Eshete. “PRICURE: Privacy-Preserving Collaborative Inference in a Multi-Party Setting.” Proceedings of the 2021 ACM Workshop on Security and Privacy Analytics (2021): n. pag.
- Javaheripi, Mojan and Farinaz Koushanfar. “HASHTAG: Hash Signatures for Online Detection of Fault-Injection Attacks on Deep Neural Networks.” 2021 IEEE/ACM International Conference On Computer Aided Design (ICCAD) (2021): 1-9.
- Javaheripi, Mojan, Mohammad Samragh, Gregory Fields, Tara Javidi and Farinaz Koushanfar. “CleaNN: Accelerated Trojan Shield for Embedded Neural Networks.” 2020 IEEE/ACM International Conference On Computer Aided Design (ICCAD) (2020): 1-9.
- Jayaraman, Bargav and David E. Evans. “Evaluating Differentially Private Machine Learning in Practice.” USENIX Security Symposium (2019).
- Jayaraman, Bargav, Lingxiao Wang, David E. Evans and Quanquan Gu. “Revisiting Membership Inference Under Realistic Assumptions.” Proceedings on Privacy Enhancing Technologies 2021 (2021): 348 - 368.
- Jeddi, Ahmadreza, Mohammad Javad Shafiee, Michelle Karg, Christian Scharfenberger and Alexander Wong. “Learn2Perturb: An End-to-End Feature Perturbation Learning to Improve Adversarial Robustness.” 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2020): 1238-1247.
- Jegorova, Marija, Chaitanya Kaul, Charlie Mayor, Alison Q. O’Neil, Alexander Weir, Roderick Murray-Smith and Sotirios A. Tsaftaris. “Survey: Leakage and Privacy at Inference Time.” ArXivabs/2107.01614 (2021): n. pag.

- Jeong, Seong Hoon, Boosun Jeon, Boheung Chung and Huy Kang Kim. “Convolutional Neural Network-based Intrusion Detection System for AVTP Streams in Automotive Ethernet-based Networks.” Veh. Commun. 29 (2021): 100338.
- Jha, Nandan Kumar, Sparsh Mittal, Binod Kumar and Govardhan Mattela. “DeepPeep: Exploiting Design Ramifications to Decipher the Architecture of Compact DNNs.” ArXiv abs/2007.15248 (2020): n. pag.
- Jha, Sumit Kumar, Susmit Jha, Rickard Ewetz, Sunny Raj, Alvaro Velasquez, Laura L. Pullum and Ananthram Swami. “An Extension of Fano’s Inequality for Characterizing Model Susceptibility to Membership Inference Attacks.” ArXiv abs/2009.08097 (2020): n. pag.
- Ji, Nan, YanFei Feng, Haidong Xie, Xueshuang Xiang and Naijin Liu. “Adversarial YOLO: Defense Human Detection Patch Attacks via Detecting Adversarial Patches.” ArXiv abs/2103.08860 (2021): n. pag.
- Ji, Shouling, Haiqin Weng, Yiming Wu, Pan Zhou, Qinming He, Raheem A. Beyah and Ting Wang. “FDI: Quantifying Feature-based Data Inferability.” ArXiv abs/1902.00714 (2019): n. pag.
- Ji, Tianxi, Erman Ayday, Emre Yilmaz and Pan Li. “Privacy-Preserving Database Fingerprinting.” (2021).
- Ji, Yujie, Xinyang Zhang, Shouling Ji, Xiapu Luo and Ting Wang. “Model-Reuse Attacks on Deep Learning Systems.” Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (2018): n. pag.
- Jia, Hengrui, Christopher A. Choquette-Choo and Nicolas Papernot. “Entangled Watermarks as a Defense against Model Extraction.” ArXiv abs/2002.12200 (2021): n. pag.
- Jia, Jinyuan and Neil Zhenqiang Gong. “AttriGuard: A Practical Defense Against Attribute Inference Attacks via Adversarial Machine Learning.” USENIX Security Symposium (2018).
- Jia, Jinyuan and Neil Zhenqiang Gong. “Defending against Machine Learning based Inference Attacks via Adversarial Examples: Opportunities and Challenges.” Adaptive Autonomous Secure Cyber Systems (2020).
- Jia, Jinyuan, Ahmed Salem, Michael Backes, Yang Zhang and Neil Zhenqiang Gong. “MemGuard: Defending against Black-Box Membership Inference Attacks via Adversarial Examples.” Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security(2019): n. pag.
- Jiang, Yuzhou, Emre Yilmaz and Erman Ayday. “Differentially Private Fingerprinting for Location Trajectories.” ArXiv abs/2204.04792 (2022): n. pag.
- Jin, Charles, Melinda Sun and Martin C. Rinard. “Provable Guarantees against Data Poisoning Using Self-Expansion and Compatibility.” ArXiv abs/2105.03692 (2021): n. pag.
- Jin, Hongyu and Panos Papadimitratos. “Resilient Privacy Protection for Location-Based Services through Decentralization.” ACM Transactions on Privacy and Security (TOPS) 22 (2019): 1 - 36.
- Jin, Kaidi, Tianwei Zhang, Chao Shen, Yufei Chen, Ming Fan, Chenhao Lin and Ting Liu. “A Unified Framework for Analyzing and Detecting Malicious Examples of DNN Models.” ArXivabs/2006.14871 (2020): n. pag.
- Joe, Byunggill, Sung Ju Hwang and Insik Shin. “Learning to Disentangle Robust and Vulnerable Features for Adversarial Detection.” ArXiv abs/1909.04311 (2019): n. pag.

- John, Tara Merin, Syed Kamran Haider, Hamza Omar and Marten Van Dijk. “Connecting the Dots: Privacy Leakage via Write-Access Patterns to the Main Memory.” IEEE Transactions on Dependable and Secure Computing 17 (2020): 436-442.
- Jordon, James, Daniel Jarrett, Jinsung Yoon, Tavian Barnes, Paul W. G. Elbers, Patrick J. Thoral, Ari Ercole, Cui-cui Zhang, Danielle Belgrave and Mihaela van der Schaar. “Hide-and-Seek Privacy Challenge.” ArXiv abs/2007.12087 (2020): n. pag.
- Joshi, Ameya, Gauri Jagatap and Chinmay Hegde. “Adversarial Token Attacks on Vision Transformers.” ArXiv abs/2110.04337 (2021): n. pag.
- Joshi, Sonal, Saurabh Kataria, Jesús Villalba and Najim Dehak. “AdvEst: Adversarial Perturbation Estimation to Classify and Detect Adversarial Attacks against Speaker Identification.” ArXiv abs/2204.03848 (2022): n. pag.
- Jourdan, Théo, Antoine Boutet and Carole Frindel. “Privacy Assessment of Federated Learning Using Private Personalized Layers.” 2021 IEEE 31st International Workshop on Machine Learning for Signal Processing (MLSP) (2021): 1-6.
- Jung, Woosub, Yizhou Feng, Sabbir Ahmed Khan, Chunsheng Xin, Danella Zhao and Gang Zhou. “DeepAuditor: Distributed Online Intrusion Detection System for IoT devices via Power Side-channel Auditing.” ArXiv abs/2106.12753 (2022): n. pag.
- Kanovich, Max I., Tajana Ban Kirigin, Vivek Nigam, Andre Scedrov and Carolyn L. Talcott. “Time, computational complexity, and probability in the analysis of distance-bounding protocols.” ArXivabs/1702.03504 (2017): n. pag.
- Kao, Hsuan-Kai and Li Su. “Temporally Guided Music-to-Body-Movement Generation.” Proceedings of the 28th ACM International Conference on Multimedia (2020): n. pag.
- Kato, Fumiyuki, Yang Cao and Masatoshi Yoshikawa. “OLIVE: Oblivious and Differentially Private Federated Learning on Trusted Execution Environment.” ArXiv abs/2202.07165 (2022): n. pag.
- Kaya, Yigitcan, Sanghyun Hong and Tudor Dumitras. “On the Effectiveness of Regularization Against Membership Inference Attacks.” ArXiv abs/2006.05336 (2020): n. pag.
- Kaya, Yigitcan, Sanghyun Hong and Tudor Dumitras. “Shallow-Deep Networks: Understanding and Mitigating Network Overthinking.” ICML (2019).
- Kerkouche, Raouf, Gergely Ács and Claude Castelluccia. “Federated Learning in Adversarial Settings.” ArXiv abs/2010.07808 (2020): n. pag.
- Kerkouche, Raouf, Gergely Ács, Claude Castelluccia and Pierre Genevès. “Compression Boosts Differentially Private Federated Learning.” 2021 IEEE European Symposium on Security and Privacy (EuroS&P) (2021): 304-318.
- Kesarwani, Manish, Akshar Kaul, Stefano Braghin, Naoise Holohan and Spiros Antonatos. “Secure k-Anonymisation over Encrypted Databases.” 2021 IEEE 14th International Conference on Cloud Computing (CLOUD) (2021): 20-30.
- Khabarlak, Kostiantyn and Larysa Koriashkina. “Minimizing Perceived Image Quality Loss Through Adversarial Attack Scoping.” ArXiv abs/1904.10390 (2019): n. pag.
- Khalid, Faiq, Muhammad Abdullah Hanif, Semeen Rehman and Muhammad Akmal Shafique. “Security for Machine Learning-Based Systems: Attacks and Challenges During Training and Inference.” 2018 International Conference on Frontiers of Information Technology (FIT) (2018): 327-332.
- Khalid, Faiq, Muhammad Abdullah Hanif, Semeen Rehman, Junaid Qadir and Muhammad Akmal Shafique. “FAdeML: Understanding the Impact of Pre-Processing

Noise Filtering on Adversarial Machine Learning." 2019 Design, Automation & Test in Europe Conference & Exhibition (DATE)(2019): 902-907.
- Khalid, Faiq, Muhammad Abdullah Hanif, Semeen Rehman, Rehan Ahmed and Muhammad Akmal Shafique. "TrISec: Training Data-Unaware Imperceptible Security Attacks on Deep Neural Networks." 2019 IEEE 25th International Symposium on On-Line Testing and Robust System Design (IOLTS) (2019): 188-193.
- Khan, Latif Ullah, Walid Saad, Zhu Han and Choong Seon Hong. "Dispersed Federated Learning: Vision, Taxonomy, and Future Directions." IEEE Wireless Communications 28 (2021): 192-198.
- Kharitonov, Eugene, Marco Baroni and Dieuwke Hupkes. "How BPE Affects Memorization in Transformers." ArXiv abs/2110.02782 (2021): n. pag.
- Khasawneh, Khaled N., Esmaeil Mohammadian Koruyeh, Chengyu Song, Dmitry Evtyushkin, Dmitry V. Ponomarev and Nael B. Abu-Ghazaleh. "SafeSpec: Banishing the Spectre of a Meltdown with Leakage-Free Speculation." 2019 56th ACM/IEEE Design Automation Conference (DAC)(2019): 1-6.
- Khodaei, Mohammad Javad and Panagiotis Papadimitratos. "Cooperative Location Privacy in Vehicular Networks: Why Simple Mix Zones are Not Enough." IEEE Internet of Things Journal 8 (2021): 7985-8004.
- Khowaja, Sunder Ali, Ik Hyun Lee, Kapal Dev, Muhammad Aslam Jarwar and Nawab Muhammad Faseeh Qureshi. "Get Your Foes Fooled: Proximal Gradient Split Learning for Defense Against Model Inversion Attacks on IoMT Data." IEEE Transactions on Network Science and Engineering(2022): n. pag.
- Kido, Hiroyuki and Bei Shui Liao. "A Bayesian Approach to Direct and Inverse Abstract Argumentation Problems." ArXiv abs/1909.04319 (2019): n. pag.
- Kilbertus, Niki, Giambattista Parascandolo and Bernhard Schölkopf. "Generalization in anti-causal learning." ArXiv abs/1812.00524 (2018): n. pag.
- Kim, Young-Eun, Woo-Jeoung Nam, K. Min and Seong-Whan Lee. "Style-Guided Domain Adaptation for Face Presentation Attack Detection." ArXiv abs/2203.14565 (2022): n. pag.
- Kiourti, Panagiota, Wenchao Li, Anirban Roy, Karan Sikka and Susmit Jha. "MISA: Online Defense of Trojaned Models using Misattributions." Annual Computer Security Applications Conference(2021): n. pag.
- Kiritani, Taro and Koji Ono. "Recurrent Attention Model with Log-Polar Mapping is Robust against Adversarial Attacks." ArXiv abs/2002.05388 (2020): n. pag.
- Klein, Amit. "Cross Layer Attacks and How to Use Them (for DNS Cache Poisoning, Device Tracking and More)." 2021 IEEE Symposium on Security and Privacy (SP) (2021): 1179-1196.
- Knight, Georgie, Alexander P. Kartun-Giles, Orestis Georgiou and Carl P. Dettmann. "Counting Geodesic Paths in 1-D VANETs." IEEE Wireless Communications Letters 6 (2017): 110-113.
- Koda, Yusuke, Koji Yamamoto, Takayuki Nishio and Masahiro Morikura. "Differentially Private AirComp Federated Learning with Power Adaptation Harnessing Receiver Noise." GLOBECOM 2020 - 2020 IEEE Global Communications Conference (2020): 1-6.
- Koffas, Stefanos, Jing Xu, Mauro Conti and Stjepan Picek. "Can You Hear It?: Backdoor Attacks via Ultrasonic Triggers." Proceedings of the 2022 ACM Workshop on Wireless Security and Machine Learning (2022): n. pag.

- Kolluri, Aashish, Teodora Baluta, Bryan Hooi and Prateek Saxena. “LPGNet: Link Private Graph Networks for Node Classification.” ArXiv abs/2205.03105 (2022): n. pag.
- Krenc, Thomas, Robert Beverly and Georgios Smaragdakis. “AS-level BGP community usage classification.” Proceedings of the 21st ACM Internet Measurement Conference (2021): n. pag.
- Krishna, Kalpesh, Gaurav Singh Tomar, Ankur P. Parikh, Nicolas Papernot and Mohit Iyyer. “Thieves on Sesame Street! Model Extraction of BERT-based APIs.” ArXiv abs/1910.12366 (2020): n. pag.
- Krishna, Satyapriya, Rahul Gupta and Christophe Dupuy. “ADePT: Auto-encoder based Differentially Private Text Transformation.” EACL (2021).
- Kronenberger, Jan and Anselm Haselhoff. “Dependency Decomposition and a Reject Option for Explainable Models.” ArXiv abs/2012.06523 (2020): n. pag.
- Kulkarni, Vaibhav, Natasa Tagasovska, Thibault Vatter and Benoît Garbinato. “Generative Models for Simulating Mobility Trajectories.” ArXiv abs/1811.12801 (2018): n. pag.
- Kulynych, Bogdan, Mohammad Yaghini, Giovanni Cherubin, Michael Veale and Carmela Troncoso. “Disparate Vulnerability to Membership Inference Attacks.” Proceedings on Privacy Enhancing Technologies 2022 (2021): 460 - 480.
- Kumar, Aounon, Alexander Levine and Soheil Feizi. “Policy Smoothing for Provably Robust Reinforcement Learning.” ArXiv abs/2106.11420 (2021): n. pag.
- Kumar, Ram Shankar Siva, Jonathon W. Penney, Bruce Schneier and Kendra Albert. “Legal Risks of Adversarial Machine Learning Research.” ArXiv abs/2006.16179 (2020): n. pag.
- Kumaraswamy, Deepak, Shyam Murthy and Srinivas Vivek. “Revisiting Driver Anonymity in ORide.” SAC (2021).
- Kunar, Aditya, Robert Birke, Zilong Zhao and Lydia Yiyu Chen. “DTGAN: Differential Private Training for Tabular GANs.” ArXiv abs/2107.02521 (2021): n. pag.
- Kunar, Aditya. “Effective and Privacy preserving Tabular Data Synthesizing.” ArXivabs/2108.10064 (2021): n. pag.
- Kuzina, Anna, Max Welling and Jakub M. Tomczak. “Defending Variational Autoencoders from Adversarial Attacks with MCMC.” ArXiv abs/2203.09940 (2022): n. pag.
- Kyatham, Vinay, P. PrathoshA., Deepak Mishra, Tarun Kumar Yadav and Dheeraj Mundhra. “Variational Inference with Latent Space Quantization for Adversarial Resilience.” 2020 25th International Conference on Pattern Recognition (ICPR) (2021): 9593-9600.
- Lai, Zihang, Senthil Purushwalkam and Abhinav Kumar Gupta. “The Functional Correspondence Problem.” ArXiv (2021): n. pag.
- Lakshminarayana, Subhash, Saurav Sthapit and Carsten Maple. “Data-Driven Detection and Identification of IoT-Enabled Load-Altering Attacks in Power Grids.” ArXiv abs/2110.00667 (2022): n. pag.
- Lam, Maximilian, Gu-Yeon Wei, David M. Brooks, Vijay Janapa Reddi and Michael Mitzenmacher. “Gradient Disaggregation: Breaking Privacy in Federated Learning by Reconstructing the User Participant Matrix.” ArXiv abs/2106.06089 (2021): n. pag.

- Lampesberger, Harald. “An Incremental Learner for Language-Based Anomaly Detection in XML.” 2016 IEEE Security and Privacy Workshops (SPW) (2016): 156-170.
- Law, Andrew Chung Chee, Chester Leung, Rishabh Poddar, Raluca A. Popa, Chenyu Shi, Octavian Sima, Chaofan Yu, Xingmeng Zhang and Wenting Zheng. “Secure Collaborative Training and Inference for XGBoost.” Proceedings of the 2020 Workshop on Privacy-Preserving Machine Learning in Practice (2020): n. pag.
- Le, Thai and tql. “Socialbots on Fire: Modeling Adversarial Behaviors of Socialbots via Multi-Agent Hierarchical Reinforcement Learning.” Proceedings of the ACM Web Conference 2022 (2022): n. pag.
- Learning-Aided Physical Layer Attacks Against Multicarrier Communications in IoT.” IEEE Transactions on Cognitive Communications and Networking 7 (2021): 239-254
- Lechner, Mathias, Alexander Amini, Daniela Rus and Thomas A. Henzinger. “Revisiting the Adversarial Robustness-Accuracy Tradeoff in Robot Learning.” ArXiv abs/2204.07373 (2022): n. pag.
- Lee, Sangho, Ming-Wei Shih, Prasun Gera, Taesoo Kim, Hyesoon Kim and Marcus Peinado. “Inferring Fine-grained Control Flow Inside SGX Enclaves with Branch Shadowing.” USENIX Security Symposium (2017).
- Leino, Klas and Matt Fredrikson. “Stolen Memories: Leveraging Model Memorization for Calibrated White-Box Membership Inference.” ArXiv abs/1906.11798 (2020): n. pag.
- Levin, Owen, Zihang Meng, Vikas Singh and Xiaojin Zhu. “Fooling Computer Vision into Inferring the Wrong Body Mass Index.” ArXiv abs/1905.06916 (2019): n. pag.
- Li, Ang, Jiayi Guo, Huanrui Yang, Flora Dilys Salim and Yiran Chen. “DeepObfuscator: Obfuscating Intermediate Representations with Privacy-Preserving Adversarial Learning on Smartphones.” Proceedings of the International Conference on Internet-of-Things Design and Implementation(2021): n. pag.
- Li, Ang, Yixiao Duan, Huanrui Yang, Yiran Chen and Jianlei Yang. “TIPRDC: Task-Independent Privacy-Respecting Data Crowdsourcing Framework for Deep Learning with Anonymized Intermediate Representations.” Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining (2020): n. pag.
- Li, Chau Yi and Andrea Cavallaro. “Training privacy-preserving video analytics pipelines by suppressing features that reveal information about private attributes.” ICASSP (2022).
- Li, Guo Wei, Shahbaz Rezaei and Xin Liu. “User-Level Membership Inference Attack against Metric Embedding Learning.” ArXiv abs/2203.02077 (2022): n. pag.
- Li, Guyue, Hai-fen Yang, Junqing Zhang, Hongzhi Liu and Aiqun Hu. “Fast and Secure Key Generation with Channel Obfuscation in Slowly Varying Environments.” IEEE INFOCOM 2022 - IEEE Conference on Computer Communications (2022): 1-10.
- Li, Haocheng, Satwik Patnaik, Abhrajit Sengupta, Haoyu Yang, Johann Knechtel, Bei Yu, Evangeline F. Y. Young and Ozgur Sinanoglu. “Attacking Split Manufacturing from a Deep Learning Perspective.” 2019 56th ACM/IEEE Design Automation Conference (DAC) (2019): 1-6.
- Li, Haofeng, Yirui Zeng, Guanbin Li, Liang Lin and Yizhou Yu. “Online Alternate Generator Against Adversarial Attacks.” IEEE Transactions on Image Processing 29 (2020): 9305-9315.

- Li, Haoran, Yangqiu Song and Lixin Fan. “You Don’t Know My Favorite Color: Preventing Dialogue Representations from Revealing Speakers’ Private Personas.” ArXiv abs/2205.10228 (2022): n. pag.
- Li, Jiacheng, Ninghui Li and Bruno Ribeiro. “Membership Inference Attacks and Defenses in Classification Models.” Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy (2021): n. pag.
- Li, Jiangnan, Yingyuan Yang, Jinyuan Sun, Kevin L. Tomsovic and Hairong Qi. “Towards Adversarial-Resilient Deep Neural Networks for False Data Injection Attack Detection in Power Grids.” ArXiv abs/2102.09057 (2021): n. pag.
- Li, Jingqi, Ximing Chen, Sérgio Daniel Pequito, George J. Pappas and Victor M. Preciado. “Resilient Structural Stabilizability of Undirected Networks.” 2019 American Control Conference (ACC) (2019): 5173-5178.
- Li, Jingtao, Adnan Siraj Rakin, Xing Chen, Zhezhi He, Deliang Fan and Chaitali Chakrabarti. “ResSFL: A Resistance Transfer Framework for Defending Model Inversion Attack in Split Federated Learning.” ArXiv abs/2205.04007 (2022): n. pag.
- Li, Jingtao, Adnan Siraj Rakin, Zhezhi He, Deliang Fan and Chaitali Chakrabarti. “RADAR: Run-time Adversarial Weight Attack Detection and Accuracy Recovery.” 2021 Design, Automation & Test in Europe Conference & Exhibition (DATE) (2021): 790-795.
- Li, Jingwei, Patrick P. C. Lee, Chufeng Tan, Chuan Qin and Xiaosong Zhang. “Information Leakage in Encrypted Deduplication via Frequency Analysis.” 2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) (2017): 1-12.
- Li, Kaiya, Guangchun Luo, Yang Ye, Wei Li, Shihao Ji and Zhipeng Cai. “Adversarial Privacy-Preserving Graph Embedding Against Inference Attack.” IEEE Internet of Things Journal 8 (2021): 6904-6915.
- Li, Linyang, Demin Song, Jiehang Zeng, Ruotian Ma and Xipeng Qiu. “Rebuild and Ensemble: Exploring Defense Against Text Adversaries.” ArXiv abs/2203.14207 (2022): n. pag.
- Li, Renjue, Pengfei Yang, Cheng-Chao Huang, Youcheng Sun, Bai Xue and Lijun Zhang. “Towards Practical Robustness Analysis for DNNs based on PAC-Model Learning.” 2022 IEEE/ACM 44th International Conference on Software Engineering (ICSE) (2022): 2189-2201.
- Li, Shuai, Huajun Guo and Nicholas Hopper. “Measuring Information Leakage in Website Fingerprinting Attacks and Defenses.” Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (2018): n. pag.
- Li, Shuhao, Yajie Wang, Yuanzhang Li and Yu-an Tan. “l-Leaks: Membership Inference Attacks with Logits.” ArXiv abs/2205.06469 (2022): n. pag.
- Li, Tianyang, Anastasios Kyrillidis, L. Liu and Constantine Caramanis. “Approximate Newton-based statistical inference using only stochastic gradients.” ArXiv abs/1805.08920 (2018): n. pag.
- Li, Timmy, Yi Huang, James Evans and Ishanu Chattopadhyay. “Long-range Event-level Prediction and Response Simulation for Urban Crime and Global Terrorism with Granger Networks.” ArXivabs/1911.05647 (2019): n. pag.
- Li, Xi, Zhen Xiang, David J. Miller and George Kesidis. “Test-Time Detection of Backdoor Triggers for Poisoned Deep Neural Networks.” ICASSP (2022).

- Li, Xiaoguang, Hui Li, Haonan Yan, Zelei Cheng, Wenhai Sun and Hui Zhu. “Mitigating Query-Flooding Parameter Duplication Attack on Regression Models with High-Dimensional Gaussian Mechanism.” ArXiv abs/2002.02061 (2020): n. pag.
- Li, Xiaoxiao, Yangsibo Huang, Binghui Peng, Zhao Song and K. Li. “MixCon: Adjusting the Separability of Data Representations for Harder Data Recovery.” ArXiv abs/2010.11463 (2020): n. pag.
- Li, Xingyu and Bogdan I. Epureanu. “Analysis of Fleet Modularity in an Artificial Intelligence-Based Attacker-Defender Game.” ArXiv abs/1811.03742 (2018): n. pag.
- Li, Yuchen, Yifan Bao, Liyao Xiang, Junhan Liu, Cen Chen, Li Wang and Xinbing Wang. “Privacy Threats Analysis to Secure Federated Learning.” ArXiv abs/2106.13076 (2021): n. pag.
- Li, Zhe, Wieland Brendel, Edgar Y. Walker, Erick Cobos, Taliah Muhammad, Jacob Reimer, Matthias Bethge, Fabian H Sinz, Xaq Pitkow and Andreas Savas Tolias. “Learning From Brains How to Regularize Machines.” NeurIPS (2019).
- Li, Zhenbang, Yaya Shi, Jin Gao, Shaoru Wang, Bing Li, Pengpeng Liang and Weiming Hu. “A Simple and Strong Baseline for Universal Targeted Attacks on Siamese Visual Tracking.” IEEE Transactions on Circuits and Systems for Video Technology 32 (2022): 3880-3894.
- Li, Zheng and Yang Zhang. “Membership Leakage in Label-Only Exposures.” Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (2021): n. pag.
- Li, Zhengpin, Zheng Wei, Xiaojun Mao and Jian Wang. “One-Bit Matrix Completion with Differential Privacy.” ArXiv abs/2110.00719 (2021): n. pag.
- Li, Zhi, Haoliang Li, Xin Luo, Yongjian Hu, Kwok-Yan Lam and Alex Chichung Kot. “Asymmetric Modality Translation For Face Presentation Attack Detection.” ArXiv abs/2110.09108 (2021): n. pag.
- Liang, Zhicong, Bao Wang, Quanquan Gu, S. Osher and Yuan Yao. “Differentially Private Federated Learning with Laplacian Smoothing.” (2020).
- Liao, Peiyuan, Han Zhao, Keyulu Xu, T. Jaakkola, Geoffrey J. Gordon, Stefanie Jegelka and Ruslan Salakhutdinov. “Information Obfuscation of Graph Neural Networks.” ICML (2021).
- Liew, Seng Pei and Tsubasa Takahashi. “FaceLeaks: Inference Attacks against Transfer Learning Models via Black-box Queries.” ArXiv abs/2010.14023 (2020): n. pag.
- Lim, John, Jan-Michael Frahm and Fabian Monrose. “Leveraging Disentangled Representations to Improve Vision-Based Keystroke Inference Attacks Under Low Data Constraints.” Proceedings of the Twelfth ACM Conference on Data and Application Security and Privacy (2022): n. pag.
- Lim, John, True Price, Fabian Monrose and Jan-Michael Frahm. “Revisiting the Threat Space for Vision-based Keystroke Inference Attacks.” ECCV Workshops (2020).
- Lin, Wei-An, Yogesh Balaji, Pouya Samangouei and Rama Chellappa. “Invert and Defend: Model-based Approximate Inversion of Generative Adversarial Networks for Secure Inference.” ArXivabs/1911.10291 (2019): n. pag.
- Lin, Zinan, Vyas Sekar and Giulia C. Fanti. “On the Privacy Properties of GAN-generated Samples.” ArXiv abs/2206.01349 (2021): n. pag.
- Liu, Chen, Abhishek Chakraborty, Nikhil Chawla and Neer Roggel. “Frequency Throttling Side-Channel Attack.” ArXiv abs/2206.07012 (2022): n. pag.

- Liu, Depeng, Lutan Zhao, Pengfei Yang, Bow-Yaw Wang, Rui Hou, Lijun Zhang and Naijun Zhan. “Defensive Design of Saturating Counters Based on Differential Privacy.” ArXiv abs/2206.00279 (2022): n. pag.
- Liu, Guanxiong, Issa M. Khalil, Abdallah Khreishah and Nhathai Phan. “A Synergetic Attack against Neural Network Classifiers combining Backdoor and Adversarial Examples.” 2021 IEEE International Conference on Big Data (Big Data) (2021): 834-846.
- Liu, Hongbin, Jinyuan Jia, Wenjie Qu and Neil Zhenqiang Gong. “EncoderMI: Membership Inference against Pre-trained Encoders in Contrastive Learning.” Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (2021): n. pag.
- Liu, Jiaxiang, Simon Oya and Florian Kerschbaum. “Generalization Techniques Empirically Outperform Differential Privacy against Membership Inference.” ArXiv abs/2110.05524 (2021): n. pag.
- Liu, Junlin and Xinchen Lyu. “Clustering Label Inference Attack against Practical Split Learning.” ArXiv abs/2203.05222 (2022): n. pag.
- Liu, Kang, Benjamin Tan, Gaurav Rajavendra Reddy, Siddharth Garg, Yiorgos Makris and Ramesh Karri. “Bias Busters: Robustifying DL-Based Lithographic Hotspot Detectors Against Backdooring Attacks.” IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 40 (2021): 2077-2089.
- Liu, Kin Sum, Chaowei Xiao, Bo Li and Jie Gao. “Performing Co-membership Attacks Against Deep Generative Models.” 2019 IEEE International Conference on Data Mining (ICDM) (2019): 459-467.
- Liu, Qun, Supratik Mukhopadhyay, Maria-Ximena Bastidas-Rodríguez, Xing Fu, Sushant P Sahu, David Burk and Manas Ranjan Gartia. “A One-Shot Learning Framework for Assessment of Fibrillar Collagen from Second Harmonic Generation Images of an Infarcted Myocardium.” 2020 IEEE 17th International Symposium on Biomedical Imaging (ISBI) (2020): 839-843.
- Liu, Tianyu, Xin Zheng, Xiaoan Ding, Baobao Chang and Zhifang Sui. “An Empirical Study on Model-agnostic Debiasing Strategies for Robust Natural Language Inference.” CONLL (2020).
- Liu, Wenqing, Miaojing Shi, Teddy Furon and Li Li. “Defending Adversarial Examples via DNN Bottleneck Reinforcement.” Proceedings of the 28th ACM International Conference on Multimedia(2020): n. pag.
- Liu, Y., Xinghua Zhu, Jianzong Wang and Jing Xiao. “A Quantitative Metric for Privacy Leakage in Federated Learning.” ICASSP 2021 - 2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (2021): 3065-3069.
- Liu, Yang, Tianyuan Zou, Yan Kang, Wenhan Liu, Yuanqin He, Zhi-qian Yi and Qian Yang. “Batch Label Inference and Replacement Attacks in Black-Boxed Vertical Federated Learning.” (2021).
- Liu, Yi, Jia-Jie Peng, Jiawen Kang, Abdullah M. Iliyasu, Dusit Tao Niyato and Ahmed Abd El-latif. “A Secure Federated Learning Framework for 5G Networks.” IEEE Wireless Communications 27 (2020): 24-31.
- Liu, Yugeng, Rui Wen, Xinlei He, A. Salem, Zhikun Zhang, Michael Backes, Emiliano De Cristofaro, Mario Fritz and Yang Zhang. “ML-Doctor: Holistic Risk Assessment of Inference Attacks Against Machine Learning Models.” ArXiv abs/2102.02551 (2021): n. pag.

- Liu, Ziqi, Alex Smola, Kyle Soska, Yu-Xiang Wang and Qinghua Zheng. “Attributing Hacks.” ArXivabs/1611.03021 (2017): n. pag.
- Lomnitz, M., Nina Lopatina, Paul Gamble, Zigfried Hampel-Arias, Lucas Tindall, Felipe A. Mejia and Maria Alejandra Barrios. “Reducing audio membership inference attack accuracy to chance: 4 defenses.” ArXiv abs/1911.01888 (2019): n. pag.
- Long, Yunhui, Vincent Bindschaedler and Carl A. Gunter. “Towards Measuring Membership Privacy.” ArXiv abs/1712.09136 (2017): n. pag.
- Long, Yunhui, Vincent Bindschaedler, Lei Wang, Diyue Bu, Xiaofeng Wang, Haixu Tang, Carl A. Gunter and Kai Chen. “Understanding Membership Inferences on Well-Generalized Learning Models.” ArXiv abs/1802.04889 (2018): n. pag.
- Lorenz, Peter, Paula Harder, Dominik Strassel, Margret Keuper and Janis Keuper. “Detecting AutoAttack Perturbations in the Frequency Domain.” ArXiv abs/2111.08785 (2021): n. pag.
- Lu, Chris Xiaoxuan, Bowen Du, Hongkai Wen, Sen Wang, A. Markham, Ivan Martinovic, Yiran Shen and Agathoniki Trigoni. “Snoopy: Sniffing Your Smartwatch Passwords via Deep Sequence Learning.” ArXiv abs/1912.04836 (2017): n. pag.
- Lu, Hanlin, Changchang Liu, Ting He, Shiqiang Wang and Kevin S. Chan. “Sharing Models or Coresets: A Study based on Membership Inference Attack.” ArXiv abs/2007.02977 (2020): n. pag.
- Lu, Tianhan, Bor-Yuh Evan Chang and Ashutosh Trivedi. “Selectively-Amortized Resource Bounding (Extended Version).” (2021).
- Lu, Zhigang and Hong Shen. “Differentially Private k-Means Clustering with Guaranteed Convergence.” ArXiv abs/2002.01043 (2020): n. pag.
- Lu, Zhigang, Hassan Jameel Asghar, Mohamed Ali Kâafar, Darren Webb and Peter Dickinson. “A Differentially Private Framework for Deep Learning With Convexified Loss Functions.” IEEE Transactions on Information Forensics and Security 17 (2022): 2151-2165.
- Luo, Xinjian and Xiangqi Zhu. “Exploiting Defenses against GAN-Based Feature Inference Attacks in Federated Learning.” ArXiv abs/2004.12571 (2020): n. pag.
- Luo, Xinjian, Yuncheng Wu, Xiaokui Xiao and Beng Chin Ooi. “Feature Inference Attack on Model Predictions in Vertical Federated Learning.” 2021 IEEE 37th International Conference on Data Engineering (ICDE) (2021): 181-192.
- Lyu, L., Han Yu, Xingjun Ma, Lichao Sun, Jun Zhao, Qiang Yang and Philip S. Yu. “Privacy and Robustness in Federated Learning: Attacks and Defenses.” ArXiv abs/2012.06337 (2020): n. pag.
- Ma, Hua, Huming Qiu, Yansong Gao, Zhi Zhang, Alsharif Abuadbba, Minhui Xue, Anmin Fu, Zhang Jiliang, Said F. Al-Sarawi and Derek Abbott. “Quantization Backdoors to Deep Learning Commercial Frameworks.” (2021).
- Ma, Hua, Qun Li, Yifeng Zheng, Zhi Xuan Zhang, Xiaoning Liu, Yan Gao, Said F. Al-Sarawi and Derek Abbott. “MUD-PQFed: Towards Malicious User Detection in Privacy-Preserving Quantized Federated Learning.” (2022).
- Madge, James Henry, Giovanni Colavizza, James Hetherington, Weisi Guo and Alan Wilson. “Assessing Simulations of Imperial Dynamics and Conflict in the Ancient World.” Cliodynamics: The Journal of Quantitative History and Cultural Evolution (2019): n. pag.
- Maergner, Paul, Vinaychandran Pondenkandath, Michele Alberti, Marcus Liwicki, Kaspar Riesen, Rolf Ingold and Andreas Fischer. “Offline Signature Verification by Combining Graph Edit Distance and Triplet Networks.” S+SSPR (2018).

- Mahajan, Divyat, Shruti Tople and Amit Sharma. “The Connection between Out-of-Distribution Generalization and Privacy of ML Models.” ArXiv abs/2110.03369 (2021): n. pag.
- Mahawaga Arachchige, Pathum Chamikara, Dongxin Liu, Seyit Ahmet Çamtepe, Surya Nepal, Marthie Grobler, Peter Bertók and Ibrahim Khalil. “Local Differential Privacy for Federated Learning in Industrial Settings.” ArXiv abs/2202.06053 (2022): n. pag.
- Mahawaga Arachchige, Pathum Chamikara, Peter Bertók, Ibrahim Khalil, D. Liu and Seyit Ahmet Çamtepe. “Privacy Preserving Distributed Machine Learning with Federated Learning.” Comput. Commun. 171 (2021): 112-125.
- Mahawaga Arachchige, Pathum Chamikara, Peter Bertók, Ibrahim Khalil, D. Liu and Seyit Ahmet Çamtepe. “Privacy Preserving Face Recognition Utilizing Differential Privacy.” Comput. Secur. 97 (2020): 101951.
- Mahloujifar, Saeed, Alexandre Sablayrolles, Graham Cormode and Somesh Jha. “Optimal Membership Inference Bounds for Adaptive Composition of Sampled Gaussian Mechanisms.” ArXiv abs/2204.06106 (2022): n. pag.
- Mahloujifar, Saeed, Huseyin A. Inan, Melissa Chase, Esha Ghosh and Marcello Hasegawa. “Membership Inference on Word Embedding and Beyond.” ArXiv abs/2106.11384 (2021): n. pag.
- Maia, Henrique Teles, Chang Xiao, Dingzeyu Li, Eitan Grinspun and Changxi Zheng. “Can one hear the shape of a neural network?: Snooping the GPU via Magnetic Side Channel.” ArXivabs/2109.07395 (2021): n. pag.
- Maini, Pratyush. “Dataset Inference: Ownership Resolution in Machine Learning.” ArXivabs/2104.10706 (2021): n. pag.
- Maiti, Anindya and Murtuza Jadliwala. “Light Ears: Information Leakage via Smart Lights.” arXiv: Cryptography and Security (2018): n. pag.
- Maiti, Anindya, Murtuza Jadliwala, Jibo He and Igor Bilogrevic. “Side-Channel Inference Attacks on Mobile Keypads Using Smartwatches.” IEEE Transactions on Mobile Computing 17 (2018): 2180-2194.
- Maiti, Anindya, Ryan Heard, Mohd Sabra and Murtuza Jadliwala. “Towards Inferring Mechanical Lock Combinations using Wrist-Wearables as a Side-Channel.” Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks (2018): n. pag.
- Maity, Subha, Songkai Xue, Mikhail Yurochkin and Yuekai Sun. “Statistical inference for individual fairness.” ArXiv abs/2103.16714 (2021): n. pag.
- Majumdar, Saikat, Mohammad Hossein Samavatian, Kristin Barber and Radu Teodorescu. “Using Undervolting as an on-Device Defense Against Adversarial Machine Learning Attacks.” 2021 IEEE International Symposium on Hardware Oriented Security and Trust (HOST) (2021): 158-169.
- Malek, Mani, Ilya Mironov, Karthik Prasad, Igor Shilov and Florian Tramèr. “Antipodes of Label Differential Privacy: PATE and ALIBI.” NeurIPS (2021).
- Malekzadeh, M., Anastasia Borovykh and Deniz Gunduz. “Honest-but-Curious Nets: Sensitive Attributes of Private Inputs Can Be Secretly Coded into the Classifiers’ Outputs.” Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (2021): n. pag.
- Mao, Chengzhi, Mia Chiquer, Hao Wang, Junfeng Yang and Carl Vondrick. “Adversarial Attacks are Reversible with Natural Supervision.” 2021 IEEE/CVF International Conference on Computer Vision (ICCV) (2021): 641-651.

- Mao, Xiaofeng, YueFeng Chen, Yuhong Li, Yuan He and Hui Xue. “GAP++: Learning to generate target-conditioned adversarial examples.” ArXiv abs/2006.05097 (2020): n. pag.
- Mao, Xiaofeng, YueFeng Chen, Yuhong Li, Yuan He and Hui Xue. “Learning to Characterize Adversarial Subspaces.” ICASSP 2020 - 2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (2020): 2438-2442.
- Mathai, Alex, Shreya Khare, Srikanth G. Tamilselvam and Senthil Mani. “Adversarial Black-Box Attacks On Text Classifiers Using Multi-Objective Genetic Optimization Guided By Deep Networks.” ArXiv abs/2011.03901 (2020): n. pag.
- Mathew, Alwyn, Aditya Patra and Jimson Mathew. “Monocular Depth Estimators: Vulnerabilities and Attacks.” ArXiv abs/2005.14302 (2020): n. pag.
- Mathews, Sherin M. and Samuel A. Assefa. “Federated Learning: Balancing the Thin Line Between Data Intelligence and Privacy.” ArXiv abs/2204.13697 (2022): n. pag.
- Matovu, Richard, Isaac Griswold-Steiner and Abdul Serwadda. “Kinetic Song Comprehension: Deciphering Personal Listening Habits via Phone Vibrations.” ArXiv abs/1909.09123 (2019): n. pag.
- Matta, Vincenzo, Mario Di Mauro and Maurizio Longo. “DDoS Attacks With Randomized Traffic Innovation: Botnet Identification Challenges and Strategies.” IEEE Transactions on Information Forensics and Security 12 (2017): 1844-1859.
- Matthews, Isaac, S. Soudjani and Aad van Moorsel. “Stochastic Simulation Techniques for Inference and Sensitivity Analysis of Bayesian Attack Graphs.” SciSec (2021).
- Maungmaung, AprilPyone and Hitoshi Kiya. “A protection method of trained CNN model with a secret key from unauthorized access.” APSIPA Transactions on Signal and Information Processing 10 (2021): n. pag.
- Mavroudis, Vasilios and Jamie Hayes. “Adaptive Traffic Fingerprinting: Large-scale Inference under Realistic Assumptions.” ArXiv abs/2010.10294 (2020): n. pag.
- Meehan, Casey, Amrita Roy Chowdhury, Kamalika Chaudhuri and Somesh Jha. “A Shuffling Framework for Local Differential Privacy.” ArXiv abs/2106.06603 (2021): n. pag.
- Mehnaz, Shagufta, Ninghui Li and Elisa Bertino. “Black-box Model Inversion Attribute Inference Attacks on Classification Models.” ArXiv abs/2012.03404 (2020): n. pag.
- Mehnaz, Shagufta, Sayanton Vhaduri Dibbo, Ehsanul Kabir, Ninghui Li and Elisa Bertino. “Are Your Sensitive Attributes Private? Novel Model Inversion Attribute Inference Attacks on Classification Models.” ArXiv abs/2201.09370 (2022): n. pag.
- Mehrnezhad, Maryam, Ehsan Toreini, Siamak Fayyaz Shahandashti and Feng Hao. “Stealing PINs via mobile sensors: actual risk versus user perception.” International Journal of Information Security 17 (2017): 291 - 313.
- Melis, Luca, Congzheng Song, Emiliano De Cristofaro and Vitaly Shmatikov. “Exploiting Unintended Feature Leakage in Collaborative Learning.” 2019 IEEE Symposium on Security and Privacy (SP) (2019): 691-706.
- Merkel, Cory E.. “Enhancing Adversarial Attacks on Single-Layer NVM Crossbar-Based Neural Networks with Power Consumption Information.” ArXiv abs/2207.02764 (2022): n. pag.
- Merlo, Ettore, Mira Marhaba, Foutse Khomh, Houssem Ben Braiek and Giuliano Antoniol. “Models of Computational Profiles to Study the Likelihood of DNN Metamorphic Test Cases.” ArXivabs/2107.13491 (2021): n. pag.

- Metzen, Jan Hendrik and Maksym Yatsura. “Efficient Certified Defenses Against Patch Attacks on Image Classifiers.” ArXiv abs/2102.04154 (2021): n. pag.
- Metzner, Claus. “Inferring long-range interactions between immune and tumor cells -- pitfalls and (partial) solutions.” arXiv: Quantitative Methods (2019): n. pag.
- Miehling, Erik, Roy Dong, Cédric Langbort and Tamer Başar. “Strategic Inference with a Single Private Sample.” 2019 IEEE 58th Conference on Decision and Control (CDC) (2019): 2188-2193.
- Milajerdi, Sadegh M., Birhanu Eshete, Rigel Gjomemo and Venkat Venkatakrishnan. “ProPatrol: Attack Investigation via Extracted High-Level Tasks.” ArXiv abs/1810.05711 (2018): n. pag.
- Mireshghallah, Fatemehsadat, Archit Uniyal, Tianhao Wang, David Evans and Taylor Berg-Kirkpatrick. “Memorization in NLP Fine-tuning Methods.” ArXiv abs/2205.12506 (2022): n. pag.
- Mireshghallah, Fatemehsadat, Kartik Goyal, Archit Uniyal, Taylor Berg-Kirkpatrick and R. Shokri. “Quantifying Privacy Risks of Masked Language Models Using Membership Inference Attacks.” ArXiv abs/2203.03929 (2022): n. pag.
- Mireshghallah, FatemehSadat, Mohammadkazem Taram, Prakash Ramrakhyani, Dean M. Tullsen and Hadi Esmaeilzadeh. “Shredder: Learning Noise Distributions to Protect Inference Privacy.” Proceedings of the Twenty-Fifth International Conference on Architectural Support for Programming Languages and Operating Systems (2020): n. pag.
- Mirshghallah, Fatemehsadat, Mohammadkazem Taram, Praneeth Vepakomma, Abhishek Singh, Ramesh Raskar and Hadi Esmaeilzadeh. “Privacy in Deep Learning: A Survey.” ArXivabs/2004.12254 (2020): n. pag.
- Mo, Fan, Ali Shahin Shamsabadi, Kleomenis Katevas, Andrea Cavallaro and Hamed Haddadi. “Poster: Towards Characterizing and Limiting Information Exposure in DNN Layers.” Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (2019): n. pag.
- Mo, Fan, Ali Shahin Shamsabadi, Kleomenis Katevas, Soteris Demetriou, Ilias Leontiadis, Andrea Cavallaro and Hamed Haddadi. “DarkneTZ: towards model privacy at the edge using trusted execution environments.” Proceedings of the 18th International Conference on Mobile Systems, Applications, and Services (2020): n. pag.
- Mo, Fan, Anastasia Borovykh, M. Malekzadeh, Hamed Haddadi and Soteris Demetriou. “Layer-wise Characterization of Latent Information Leakage in Federated Learning.” ArXivabs/2010.08762 (2020): n. pag.
- Mo, Fan, Hamed Haddadi, Kleomenis Katevas, Eduard Marin, Diego Perino and Nicolas Kourtellis. “PPFL: privacy-preserving federated learning with trusted execution environments.” Proceedings of the 19th Annual International Conference on Mobile Systems, Applications, and Services (2021): n. pag.
- Mohammed, Hawzhin, Tolulope A. Odetola and Syed Rafay Hasan. “How Secure is Distributed Convolutional Neural Network on IoT Edge Devices?” ArXiv abs/2006.09276 (2020): n. pag.
- Moini, Shayan, Shanquan Tian, Daniel E. Holcomb, Jakub Szefer and Russell Tessier. “Power Side-Channel Attacks on BNN Accelerators in Remote FPGAs.” IEEE Journal on Emerging and Selected Topics in Circuits and Systems 11 (2021): 357-370.

- Moitra, Abhishek and Priyadarshini Panda. “Exposing the Robustness and Vulnerability of Hybrid 8T-6T SRAM Memory Architectures to Adversarial Attacks in Deep Neural Networks.” ArXivabs/2011.13392 (2020): n. pag.
- Montanari, Arthur Noronha, Chao Duan, Luis Antonio Aguirre and Adilson E. Motter. “Functional observability and target state estimation in large-scale networks.” Proceedings of the National Academy of Sciences of the United States of America 119 (2021): n. pag.
- Mopuri, Konda Reddy, Aditya Ganeshan and R. Venkatesh Babu. “Generalizable Data-Free Objective for Crafting Universal Adversarial Perturbations.” IEEE Transactions on Pattern Analysis and Machine Intelligence 41 (2019): 2452-2465.
- Moradibaad, Amir and Ramin Jalilian Mashhoud. “Use Dimensionality Reduction and SVM Methods to Increase the Penetration Rate of Computer Networks.” ArXiv abs/1812.03173 (2019): n. pag.
- Morbitzer, Mathias, Manuel Huber and Julian Horsch. “Extracting Secrets from Encrypted Virtual Machines.” Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy (2019): n. pag.
- Mousouliotis, Panagiotis G. and Loukas P. Petrou. “Software-Defined FPGA Accelerator Design for Mobile Deep Learning Applications.” ARC (2019).
- Mu, Bingxu, Zhenxing Niu, Le Wang, Xueyang Wang, Rong Jin and Gang Hua. “Adversarial Fine-tuning for Backdoor Defense: Connecting Backdoor Attacks to Adversarial Attacks.” (2022).
- Mühlhauser, Michael, Henning Pridöhl and Dominik Herrmann. “How Private is Android’s Private DNS Setting? Identifying Apps by Encrypted DNS Traffic.” The 16th International Conference on Availability, Reliability and Security (2021): n. pag.
- Mukherjee, Sumit, Yixi Xu, Anusua Trivedi, Nabajyoti Patowary and Juan M. Lavista Ferres. “privGAN: Protecting GANs from membership inference attacks at low cost to utility.” Proceedings on Privacy Enhancing Technologies 2021 (2021): 142 - 163.
- Muñoz-González, Luis, Daniele Sgandurra, Andrea Paudice and Emil C. Lupu. “Efficient Attack Graph Analysis through Approximate Inference.” ACM Transactions on Privacy and Security (TOPS) 20 (2017): 1 - 30.
- Muñoz-González, Luis, Daniele Sgandurra, Martín Barrère and Emil C. Lupu. “Exact Inference Techniques for the Analysis of Bayesian Attack Graphs.” IEEE Transactions on Dependable and Secure Computing 16 (2019): 231-244.
- Murakami, Takao and Kenta Takahashi. “Toward Evaluating Re-identification Risks in the Local Privacy Model.” Trans. Data Priv. 14 (2021): 79-116.
- Murakami, Takao, Hiromi Arai, Koki Hamada, Takuma Hatano, Makoto Iguchi, Hiroaki Kikuchi, Atsushi Kuromasa, Hiroshi Nakagawa, Yuichi Nakamura, Kenshiro Nishiyama, Ryo Nojima, Hidenobu Oguri, Chiemi Watanabe, Akira Yamada, Takayasu Yamaguchi and Yuji Yamaoka. “Designing a Location Trace Anonymization Contest.” ArXiv abs/2107.10407 (2021): n. pag.
- Murakonda, Sasi Kumar and R. Shokri. “ML Privacy Meter: Aiding Regulatory Compliance by Quantifying the Privacy Risks of Machine Learning.” ArXiv abs/2007.09339 (2020): n. pag.
- Murakonda, Sasi Kumar, R. Shokri and George Theodorakopoulos. “Quantifying the Privacy Risks of Learning High-Dimensional Graphical Models.” AISTATS (2021).
- Mustafa, Aquib and Hamidreza Modares. “Secure Event-Triggered Distributed Kalman Filters for State Estimation.” ArXiv abs/1901.06746 (2019): n. pag.

- Nagaraja, Shishir and Ryan Shah. “Clicktok: click fraud detection using traffic analysis.” Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks(2019): n. pag.
- Nandy, Jay, Sudipan Saha, Wynne Hsu, Mong Li Lee and Xiaoxiang Zhu. “Adversarially Trained Models with Test-Time Covariate Shift Adaptation.” (2021).
- Narain, Sashank and Guevara Noubir. “Mitigating Location Privacy Attacks on Mobile Devices using Dynamic App Sandboxing.” Proceedings on Privacy Enhancing Technologies 2019 (2019): 66 - 87.
- Naseer, Muzammal, Salman Hameed Khan and Fatih Murat Porikli. “Local Gradients Smoothing: Defense Against Localized Adversarial Attacks.” 2019 IEEE Winter Conference on Applications of Computer Vision (WACV) (2019): 1300-1307.
- Naseri, Mohammad, Jamie Hayes and Emiliano De Cristofaro. “Local and Central Differential Privacy for Robustness and Privacy in Federated Learning.” Proceedings 2022 Network and Distributed System Security Symposium (2022): n. pag.
- Nasr, Milad, R. Shokri and Amir Houmansadr. “Comprehensive Privacy Analysis of Deep Learning: Passive and Active White-box Inference Attacks against Centralized and Federated Learning.” 2019 IEEE Symposium on Security and Privacy (SP) (2019): 739-753.
- Nasr, Milad, R. Shokri and Amir Houmansadr. “Machine Learning with Membership Privacy using Adversarial Regularization.” Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (2018): n. pag.
- Naveiro, Roi. “Adversarial attacks against Bayesian forecasting dynamic models.” ArXivabs/2110.10783 (2021): n. pag.
- Nawrocki, Marcin, Mattijs Jonker, Thomas C. Schmidt and Matthias Wählisch. “The far side of DNS amplification: tracing the DDoS attack ecosystem from the internet core.” Proceedings of the 21st ACM Internet Measurement Conference (2021): n. pag.
- Nazarovs, Jurijs, Jack W. Stokes, Melissa J. M. Turcotte, Justin Carroll and Itai Grady. “Radial Spike and Slab Bayesian Neural Networks for Sparse Data in Ransomware Attacks.” ArXivabs/2205.14759 (2022): n. pag.
- Nemcovsky, Yaniv, Evgenii Zheltonozhskii, Chaim Baskin, Brian Chmiel, Alexander M. Bronstein and Avi Mendelson. “Smoothed Inference for Adversarially-Trained Models.” ArXivabs/1911.07198 (2019): n. pag.
- Nemcovsky, Yaniv, Matan Yaakoby, Alexander M. Bronstein and Chaim Baskin. “Physical Passive Patch Adversarial Attacks on Visual Odometry Systems.” ArXiv abs/2207.05729 (2022): n. pag.
- Ngo, Van Chan, Mario Dehesa-Azuara, Matt Fredrikson and Jan Hoffmann. “Verifying and Synthesizing Constant-Resource Implementations with Types.” 2017 IEEE Symposium on Security and Privacy (SP) (2017): 710-728.
- Nguyen, Hiep H.. “MeshCloak: A Map-Based Approach for Personalized Location Privacy.” ArXivabs/1709.03642 (2017): n. pag.
- Nguyen, Luong Ha and James A. Goulet. “Analytically Tractable Hidden-States Inference in Bayesian Neural Networks.” ArXiv abs/2107.03759 (2022): n. pag.
- Ni, Xingyang, Heikki Huttunen and Esa Rahtu. “On the Importance of Encrypting Deep Features.” 2021 IEEE/CVF International Conference on Computer Vision Workshops (ICCVW) (2021): 4125-4132.
- Nisslmueller, Utz, Klaus-Tycho Foerster, Stefan Schmid and Christian Decker. “Toward Active and Passive Confidentiality Attacks On Cryptocurrency Off-Chain Networks.” ArXiv abs/2003.00003 (2020): n. pag.

- Nock, Richard, Giorgio Patrini, Finnian Lattimore and Tibério S. Caetano. “The Crossover Process: Learnability and Data Protection from Inference Attacks.” arXiv: Learning (2016): n. pag.
- Noever, David and Samantha E. Miller Noever. “Knife and Threat Detectors.” ArXivabs/2004.03366 (2020): n. pag.
- Nooraiepour, Alireza, Kenza Hamidouche, Waheed Uz Zaman Bajwa and Narayan B. Mandayam. “How Secure are Multicarrier Communication Systems Against Signal Exploitation Attacks?” MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM) (2018): 201-206.
- Nwadike, Munachiso, Takumi Miyawaki, Esha Sarkar, Michail Maniatakos and Farah E. Shamout. “Explainability Matters: Backdoor Attacks on Medical Imaging.” ArXiv abs/2101.00008 (2021): n. pag.
- O.Gituliar. “Higher-order corrections to the splitting functions from differential equations in QCD.” (2016).
- Odetola, Tolulope A. and Syed Rafay Hasan. “SoWaF: Shuffling of Weights and Feature Maps: A Novel Hardware Intrinsic Attack (HIA) on Convolutional Neural Network (CNN).” 2021 IEEE International Symposium on Circuits and Systems (ISCAS) (2021): 1-5.
- Olatunji, Iyiola E., Thorben Funke and Megha Khosla. “Releasing Graph Neural Networks with Differential Privacy Guarantees.” ArXiv abs/2109.08907 (2021): n. pag.
- Olatunji, Iyiola E., Wolfgang Nejdl and Megha Khosla. “Membership Inference Attack on Graph Neural Networks.” 2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA) (2021): 11-20.
- Oprisanu, Bristena, Christophe Dessimoz and Emiliano De Cristofaro. “How Much Does GenoGuard Really "Guard"?: An Empirical Analysis of Long-Term Security for Genomic Data.” Proceedings of the 18th ACM Workshop on Privacy in the Electronic Society (2019): n. pag.
- Oprisanu, Bristena, Georgi Ganev and Emiliano De Cristofaro. “On Utility and Privacy in Synthetic Genomic Data.” Proceedings 2022 Network and Distributed System Security Symposium (2022): n. pag.
- Osorio-Roig, Daile, Christian Rathgeb, Pawel Drozdowski, Philipp Terhorst, Vitomir Štruc and Cristoph Busch. “An Attack on Facial Soft-Biometric Privacy Enhancement.” IEEE Transactions on Biometrics, Behavior, and Identity Science 4 (2022): 263-275.
- Ossia, Seyed Ali, Borzoo Rassouli, Hamed Haddadi, Hamid R. Rabiee and Deniz Gündüz. “Privacy Against Brute-Force Inference Attacks.” 2019 IEEE International Symposium on Information Theory (ISIT) (2019): 637-641.
- Ottavi, Gianmarco, Angelo Garofalo, Giuseppe Tagliavini, Francesco Conti, Luca Benini and Davide Rossi. “A Mixed-Precision RISC-V Processor for Extreme-Edge DNN Inference.” 2020 IEEE Computer Society Annual Symposium on VLSI (ISVLSI) (2020): 512-517.
- Oya, Simon, Carmela Troncoso and Fernando Pérez-González. “Understanding the effects of real-world behavior in statistical disclosure attacks.” 2014 IEEE International Workshop on Information Forensics and Security (WIFS) (2014): 72-77.
- Paccagnella, Riccardo, Licheng Luo and Christopher W. Fletcher. “Lord of the Ring(s): Side Channel Attacks on the CPU On-Chip Ring Interconnect Are Practical.” USENIX Security Symposium (2021).

- Palia, Abhinav and Rajat Tandon. “Optimizing noise level for perturbing geo-location data.” ArXivabs/1705.02108 (2018): n. pag.
- Pan, Jonathan. “IoT Network Behavioral Fingerprint Inference with Limited Network Trace for Cyber Investigation: A Meta Learning Approach.” ArXiv abs/2001.04705 (2020): n. pag.
- Pan, Xinlei, Weiyao Wang, Xiaoshuai Zhang, Bo Li, Jinfeng Yi and Dawn Xiaodong Song. “How You Act Tells a Lot: Privacy-Leakage Attack on Deep Reinforcement Learning.” ArXiv abs/1904.11082 (2019): n. pag.
- Pan, Yanjun, Alon Efrat, Ming Li, Boyang Wang, Hanyu Quan, Joseph S. B. Mitchell, Jie Gao and Esther M. Arkin. “Data inference from encrypted databases: a multi-dimensional order-preserving matching approach.” Proceedings of the Twenty-First International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing(2020): n. pag.
- Pan, Yanjun, Ziqi Xu, Ming Li and Loukas Lazos. “Man-in-the-Middle Attack Resistant Secret Key Generation via Channel Randomization.” Proceedings of the Twenty-second International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing (2021): n. pag.
- Pang, Qi, Yuanyuan Yuan and Shuai Wang. “Dominating Vertical Collaborative Learning Systems.” (2022).
- Pang, Ren, Xinyang Zhang, Shouling Ji, Xiapu Luo and Ting Wang. “AdvMind: Inferring Adversary Intent of Black-Box Attacks.” Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining (2020): n. pag.
- Pang, Tianyu, Kun Xu and Jun Zhu. “Mixup Inference: Better Exploiting Mixup to Defend Adversarial Attacks.” ArXiv abs/1909.11515 (2020): n. pag.
- Panousis, Konstantinos P., Sotirios P. Chatzis and Sergios Theodoridis. “Stochastic Local Winner-Takes-All Networks Enable Profound Adversarial Robustness.” ArXiv abs/2112.02671 (2021): n. pag.
- Panousis, Konstantinos P., Sotirios P. Chatzis, Antonios Alexos and Sergios Theodoridis. “Local Competition and Stochasticity for Adversarial Robustness in Deep Learning.” AISTATS (2021).
- Panwar, Nisha, Shantanu Sharma, Guoxi Wang, Sharad Mehrotra and Nalini Venkatasubramanian. “Verifiable Round-Robin Scheme for Smart Homes.” Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy (2019): n. pag.
- Papadogeorgou, Georgia, Kosuke Imai, Jason Lyall and Fan Li. “Causal Inference with Spatio-temporal Data: Estimating the Effects of Airstrikes on Insurgent Violence in Iraq.” arXiv: Methodology (2020): n. pag.
- Papernot, Nicolas, Patrick Mcdaniel, Arunesh Sinha and Michael P. Wellman. “Towards the Science of Security and Privacy in Machine Learning.” ArXiv abs/1611.03814 (2016): n. pag.
- Parekh, Swapnil, Yaman Kumar Singla, Somesh Singh, Changyou Chen, Balaji Krishnamurthy and Rajiv Ratn Shah. “MINIMAL: Mining Models for Data Free Universal Adversarial Triggers.” ArXivabs/2109.12406 (2021): n. pag.
- Parisot, Mathias P. M., Balázs Pejó and Dayana Spagnuelo. “Property Inference Attacks on Convolutional Neural Networks: Influence and Implications of Target Model’s Complexity.” SECRYPT (2021).

- Park, Yeachan and Myung-joo Kang. “Membership Inference Attacks Against Object Detection Models.” ArXiv abs/2001.04011 (2020): n. pag.
- Pashamokhtari, Arman, Gustavo E. A. P. A. Batista and Hassan Habibi Gharakheili. “AdIoTack: Quantifying and Refining Resilience of Decision Tree Ensemble Inference Models against Adversarial Volumetric Attacks on IoT Networks.” ArXiv abs/2203.09792 (2022): n. pag.
- Pasquini, Dario, Danilo Francati and Giuseppe Ateniese. “Eluding Secure Aggregation in Federated Learning via Model Inconsistency.” ArXiv abs/2111.07380 (2021): n. pag.
- Pasquini, Dario, Giuseppe Ateniese and Massimo Bernaschi. “Unleashing the Tiger: Inference Attacks on Split Learning.” Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (2021): n. pag.
- Pasquini, Dario, Marco Mingione and Massimo Bernaschi. “Adversarial Out-domain Examples for Generative Models.” 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (2019): 272-280.
- Patel, Lekha, Lyndsay Shand, James Derek Tucker and Gabriel Huerta. “Spatio-temporal extreme event modeling of terror insurgencies.” (2021).
- Paul, William, Yinzhi Cao, Miaomiao Zhang and Philippe Burlina. “Defending Medical Image Diagnostics against Privacy Attacks using Generative Methods.” ArXiv abs/2103.03078 (2021): n. pag.
- Pauling, Cato, Michael Gimson, Muhammed Qaid, Ahmad Kida and Basel Halak. “A Tutorial on Adversarial Learning Attacks and Countermeasures.” ArXiv abs/2202.10377 (2022): n. pag.
- Pedersen, Joseph, Rafael Munoz-G’omez, Jiangnan Huang, Haozhe Sun, Wei-Wei Tu and Isabelle Guyon. “LTU Attacker for Membership Inference.” ArXiv abs/2202.02278 (2022): n. pag.
- Pei, Sen, Jiaxi Sun, Xiaopeng Zhang and Gaofeng Meng. “Gradient Concealment: Free Lunch for Defending Adversarial Attacks.” ArXiv abs/2205.10617 (2022): n. pag.
- Pejic, Ignjat, Rui Wang and Kaitai Liang. “Effect of Homomorphic Encryption on the Performance of Training Federated Learning Generative Adversarial Networks.” ArXiv abs/2207.00263 (2022): n. pag.
- Pejó, Balázs, Mina Remeli, Adam Arany, Mathieu Galtier and Gergely Ács. “Collaborative Drug Discovery: Inference-level Data Protection Perspective.” ArXiv abs/2205.06506 (2022): n. pag.
- Pereteanu, George-Liviu, Amir Alansary and Jonathan Passerat-Palmbach. “Split HE: Fast Secure Inference Combining Split Learning and Homomorphic Encryption.” ArXiv abs/2202.13351 (2022): n. pag.
- Pérez, Jorge Luis Rivero and Bernardete Ribeiro. “Attribute Learning for Network Intrusion Detection.” INNS Conference on Big Data (2016).
- Pérez, Jorge Luis Rivero, Bernardete Ribeiro, Ningshan Chen and Fatima Silva Leite. “A Grassmannian Approach to Zero-Shot Learning for Network Intrusion Detection.” ICONIP (2017).
- Peri, Neehar, Neal Gupta, W. Ronny Huang, Liam Fowl, Chen Zhu, Soheil Feizi, Tom Goldstein and John P. Dickerson. “Deep k-NN Defense Against Clean-Label Data Poisoning Attacks.” ECCV Workshops (2020).
- Pewny, Jannik, Philipp Koppe, Lucas Davi and Thorsten Holz. “Breaking and Fixing Destructive Code Read Defenses.” Proceedings of the 33rd Annual Computer Security Applications Conference (2017): n. pag.

- Pham, Ngoc Duy, Alsharif Abuadbba, Yansong Gao, Tran Dang Khoa Phan and Naveen K. Chilamkurti. “Binarizing Split Learning for Data Privacy Enhancement and Computation Reduction.” ArXiv abs/2206.04864 (2022): n. pag.
- Pichler, Georg, Marco Romanelli, Leonardo Rey Vega and Pablo Piantanida. “Perfectly Accurate Membership Inference by a Dishonest Central Server in Federated Learning.” ArXivabs/2203.16463 (2022): n. pag.
- Pinot, Rafael, Laurent Meunier, Alexandre Araujo, Hisashi Kashima, Florian Yger, Cédric Gouy-Pailler and Jamal Atif. “Theoretical evidence for adversarial robustness through randomization.” NeurIPS (2019).
- Polad, Hadar, Rami Puzis and Bracha Shapira. “Attack Graph Obfuscation.” CSCML (2017).
- Pomponi, Jary, Simone Scardapane and Aurelio Uncini. “Bayesian Neural Networks With Maximum Mean Discrepancy Regularization.” Neurocomputing 453 (2021): 428-437.
- Ponader, Jonathan, Sandip Kundu and Yan Solihin. “MILR: Mathematically Induced Layer Recovery for Plaintext Space Error Correction of CNNs.” 2021 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) (2021): 75-87.
- Poursaeed, Omid, Isay Katsman, Bicheng Gao and Serge J. Belongie. “Generative Adversarial Perturbations.” 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition (2018): 4422-4431.
- Powell, Brian A. “Securing LSB embedding against structural steganalysis.” ArXiv abs/2003.03658 (2021): n. pag.
- Prakash, Kritika, Fiza Husain, Praveen Paruchuri and Sujit Gujar. “How Private Is Your RL Policy? An Inverse RL Based Analysis Framework.” ArXiv abs/2112.05495 (2022): n. pag.
- Prematilake, Malin, Younghyun Kim, Vijay Raghunathan, Anand Raghunathan and Niraj Kumar Jha. “HW/SW Framework for Improving the Safety of Implantable and Wearable Medical Devices.” ArXiv abs/2103.01781 (2021): n. pag.
- Pricop, Emil and Sanda Florentina Mihalache. “Fuzzy approach on modelling cyber attacks patterns on data transfer in industrial control systems.” 2015 7th International Conference on Electronics, Computers and Artificial Intelligence (ECAI) (2015): SSS-23-SSS-28.
- Pyrgelis, Apostolos, Carmela Troncoso and Emiliano De Cristofaro. “Knock Knock, Who’s There? Membership Inference on Aggregate Location Data.” ArXiv abs/1708.06145 (2018): n. pag.
- Pyrgelis, Apostolos, Carmela Troncoso and Emiliano De Cristofaro. “Measuring Membership Privacy on Aggregate Location Time-Series.” Proceedings of the ACM on Measurement and Analysis of Computing Systems 4 (2020): 1 - 28.
- Pyrgelis, Apostolos, Carmela Troncoso and Emiliano De Cristofaro. “What Does The Crowd Say About You? Evaluating Aggregation-based Location Privacy.” Proceedings on Privacy Enhancing Technologies 2017 (2017): 156 - 176.
- Qi, Fanchao, Mukai Li, Yangyi Chen, Zhengyan Zhang, Zhiyuan Liu, Yasheng Wang and Maosong Sun. “Hidden Killer: Invisible Textual Backdoor Attacks with Syntactic Trigger.” ArXivabs/2105.12400 (2021): n. pag.
- Qin, Minghai and Dejan Vucinic. “Noisy Computations during Inference: Harmful or Helpful?” ArXivabs/1811.10649 (2018): n. pag.

- Qin, Ruoxi, Linyuan Wang, Xing-yuan Chen, Xuehui Du and Bin Yan. “Dynamic Defense Approach for Adversarial Robustness in Deep Neural Networks via Stochastic Ensemble Smoothed Model.” ArXiv abs/2105.02803 (2021): n. pag.
- Qin, Yujia, Fanchao Qi, Sicong Ouyang, Zhiyuan Liu, Cheng Yang, Yasheng Wang, Qun Liu and Maosong Sun. “Improving Sequence Modeling Ability of Recurrent Neural Networks via Sememes.” IEEE/ACM Transactions on Audio, Speech, and Language Processing 28 (2020): 2364-2373.
- Qiu, Han, Yi Zeng, Tianwei Zhang, Yong Jiang and Meikang Qiu. “FenceBox: A Platform for Defeating Adversarial Examples with Data Augmentation Techniques.” ArXiv abs/2012.01701 (2020): n. pag.
- Quick, Harrison. “Improving the Utility of Poisson-Distributed, Differentially Private Synthetic Data via Prior Predictive Truncation with an Application to CDC WONDER.” (2021).
- Rahimian, Shadi, Tribhuvanesh Orekondy and Mario Fritz. “Sampling Attacks: Amplification of Membership Inference Attacks by Repeated Queries.” ArXiv abs/2009.00395 (2020): n. pag.
- Rahman, Mohammad Saidur, Mohsen Imani, Nate Mathews and Matthew K. Wright. “Mockingbird: Defending Against Deep-Learning-Based Website Fingerprinting Attacks With Adversarial Traces.” IEEE Transactions on Information Forensics and Security 16 (2021): 1594-1609.
- Rahman, Tahleen A., Mario Fritz, Michael Backes and Yang Zhang. “Everything About You: A Multimodal Approach towards Friendship Inference in Online Social Networks.” ArXivabs/2003.00996 (2020): n. pag.
- Rajagopal, A. and V. Nirmala. “Strategies to architect AI Safety: Defense to guard AI from Adversaries.” ArXiv abs/1906.03466 (2019): n. pag.
- Rakin, Adnan Siraj, Li Yang, Jingtao Li, Fan Yao, Chaitali Chakrabarti, Yu Cao, Jae-sun Seo and Deliang Fan. “RA-BNN: Constructing Robust & Accurate Binary Neural Network to Simultaneously Defend Adversarial Bit-Flip Attack and Improve Accuracy.” ArXiv abs/2103.13813 (2021): n. pag.
- Rakin, Adnan Siraj, Zhezhi He and Deliang Fan. “TBT: Targeted Neural Network Attack With Bit Trojan.” 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2020): 13195-13204.
- Rakin, Adnan Siraj, Zhezhi He, Boqing Gong and Deliang Fan. “Blind Pre-Processing: A Robust Defense Method Against Adversarial Examples.” ArXiv abs/1802.01549 (2018): n. pag.
- Ramanan, Paritosh, Dan Li and Nagi Z. Gebraeel. “Blockchain-Based Decentralized Replay Attack Detection for Large-Scale Power Systems.” IEEE Transactions on Systems, Man, and Cybernetics(2020): n. pag.
- Ramírez, Miguel A., Song-Kyoo Kim, Hussam Al Hamadi, Ernesto Damiani, Young-Ji Byon, Tae-Yeon Kim, Chung-Suk Cho and Chan Yeob Yeun. “Poisoning Attacks and Defenses on Artificial Intelligence: A Survey.” ArXiv abs/2202.10276 (2022): n. pag.
- Rao, Raghunandan M., Sean Ha, Vuk Marojevic and Jeffrey H. Reed. “LTE PHY layer vulnerability analysis and testing using open-source SDR tools.” MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM) (2017): 744-749.
- Rapp, Max, Axel Adrian and Michael Kohlhase. “Context Graphs for Legal Reasoning and Argumentation.” ArXiv abs/2007.00732 (2020): n. pag.

- Rassouli, Borzoo and Deniz Gündüz. “Optimal Utility-Privacy Trade-off with Total Variation Distance as a Privacy Measure.” 2018 IEEE Information Theory Workshop (ITW) (2018): 1-5.
- Ravi, Nikhil and Anna Scaglione. “Detection and Isolation of Adversaries in Decentralized Optimization for Non-Strongly Convex Objectives.” ArXiv abs/1910.13020 (2019): n. pag.
- Real, Maria Méndez and Rubén Salvador. “Physical Side-Channel Attacks on Embedded Neural Networks: A Survey.” ArXiv abs/2110.11290 (2021): n. pag.
- Recabarren, Ruben and Bogdan Carbunar. “Hardening Stratum, the Bitcoin Pool Mining Protocol.” Proceedings on Privacy Enhancing Technologies 2017 (2017): 57 - 74.
- Reddy, Saichethan Miriyala and Saisree Miriyala. “Security and Privacy Preserving Deep Learning.” ArXiv abs/2006.12698 (2020): n. pag.
- Restuccia, Francesco and Tommaso Melodia. “PolymoRF: polymorphic wireless receivers through physical-layer deep learning.” Proceedings of the Twenty-First International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing (2020): n. pag.
- Rezaei, Aria, Jie Gao and Anand D. Sarwate. “Influencers and the Giant Component: the Fundamental Hardness in Privacy Protection for Socially Contagious Attributes.” SDM (2021).
- Rezaei, Shahbaz and Xin Liu. “An Efficient Subpopulation-based Membership Inference Attack.” ArXiv abs/2203.02080 (2022): n. pag.
- Rezaei, Shahbaz and Xin Liu. “On the Difficulty of Membership Inference Attacks.” 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2021): 7888-7896.
- Rezaei, Shahbaz, Zubair Shafiq and Xin Liu. “Accuracy-Privacy Trade-off in Deep Ensemble: A Membership Inference Perspective.” (2021).
- Rocca, Gusseppe Bravo, Peini Liu, Jordi Guitart, Ajay Dholakia, David Ellison, Jeffrey Falkanger and Miroslav Hodak. “Scanflow: A multi-graph framework for Machine Learning workflow management, supervision, and debugging.” Expert Syst. Appl. 202 (2022): 117232.
- Rodríguez, Sandra Servia, Liang Wang, Jianxin R. Zhao, Richard Mortier and Hamed Haddadi. “Privacy-Preserving Personal Model Training.” 2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI) (2018): 153-164.
- Rohrer, Elias and Florian Tschorsch. “Counting Down Thunder: Timing Attacks on Privacy in Payment Channel Networks.” Proceedings of the 2nd ACM Conference on Advances in Financial Technologies (2020): n. pag.
- Roy, Deboleena, Indrani Chakraborty, Timur Ibrayev and Kaushik Roy. “On the Intrinsic Robustness of NVM Crossbars Against Adversarial Attacks.” 2021 58th ACM/IEEE Design Automation Conference (DAC) (2021): 565-570.
- Rudnik, Charlotte, Thibault Ehrhart, Olivier Ferret, Denis Teyssou, Raphael Troncy and Xavier Tannier. “Searching News Articles Using an Event Knowledge Graph Leveraged by Wikidata.” Companion Proceedings of The 2019 World Wide Web Conference (2019): n. pag.
- Ryu, Jihyeon, Yifeng Zheng, Yansong Gao, Sharif Abuadbba, Junyaup Kim, Dongho Won, Surya Nepal, Hyoungshick Kim and Cong Wang. “Can Differential Privacy

Practically Protect Collaborative Deep Learning Inference for the Internet of Things?" ArXiv abs/2104.03813 (2021): n. pag.
- Ryu, Minseok and Kibaek Kim. "Differentially Private Federated Learning via Inexact ADMM with Multiple Local Updates." ArXiv abs/2202.09409 (2022): n. pag.
- Ryu, Minseok and Kibaek Kim. "Differentially Private Federated Learning via Inexact ADMM." ArXivabs/2106.06127 (2021): n. pag.
- Sablayrolles, Alexandre, Matthijs Douze, Cordelia Schmid, Yann Ollivier and Hervé Jégou. "White-box vs Black-box: Bayes Optimal Strategies for Membership Inference." ICML (2019).
- Sabra, Mohd, Anindya Maiti and Murtuza Jadliwala. "Zoom on the Keystrokes: Exploiting Video Calls for Keystroke Inference Attacks." ArXiv abs/2010.12078 (2021): n. pag.
- Saeidian, Sara, Giulia Cervia, Tobias J. Oechtering and Mikael Skoglund. "Quantifying Membership Privacy via Information Leakage." IEEE Transactions on Information Forensics and Security 16 (2021): 3096-3108.
- Sagduyu, Yalin Evren, Yi Shi and Tugba Erpek. "IoT Network Security from the Perspective of Adversarial Deep Learning." 2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON) (2019): 1-9.
- Sah, Ramesh Kumar and Hassan Ghasemzadeh. "Adversarial Transferability in Wearable Sensor Systems." ArXiv abs/2003.07982 (2020): n. pag.
- Saha, Aniruddha, Akshayvarun Subramanya, Koninika Patil and Hamed Pirsiavash. "Role of Spatial Context in Adversarial Robustness for Object Detection." 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW) (2020): 3403-3412.
- Sahu, Abhijeet, Zeyu Mao, Patrick Wlazlo, Hao Huang, Katherine R. Davis, Ana Elisa P. Goulart and S. Zonouz. "Multi-Source Multi-Domain Data Fusion for Cyberattack Detection in Power Systems." IEEE Access 9 (2021): 119118-119138.
- Saileshwar, Gururaj and Moinuddin K. Qureshi. "Lookout for Zombies: Mitigating Flush+Reload Attack on Shared Caches by Monitoring Invalidated Lines." ArXiv abs/1906.02362 (2019): n. pag.
- Saki, Abdullah Ash and Swaroop Ghosh. "Qubit Sensing: A New Attack Model for Multi-programming Quantum Computing." (2021).
- Salamatian, Loqman, Frédérick Douzet, Kevin Limonier and Kave Salamatian. "The geopolitics behind the routes data travels: a case study of Iran." J. Cybersecur. 7 (2021): n. pag.
- Salem, A., Apratim Bhattacharyya, Michael Backes, Mario Fritz and Yang Zhang. "Updates-Leak: Data Set Inference and Reconstruction Attacks in Online Learning." ArXiv abs/1904.01067 (2020): n. pag.
- Salem, A., Yang Zhang, Mathias Humbert, Mario Fritz and Michael Backes. "ML-Leaks: Model and Data Independent Membership Inference Attacks and Defenses on Machine Learning Models." ArXiv abs/1806.01246 (2019): n. pag.
- Salem, A., Yannick Sautter, Michael Backes, Mathias Humbert and Yang Zhang. "BAAAN: Backdoor Attacks Against Autoencoder and GAN-Based Machine Learning Models." ArXivabs/2010.03007 (2020): n. pag.
- Salimitari, Mehrdad, Shameek Bhattacharjee, Mainak Chatterjee and Yaser P. Fallah. "A Prospect Theoretic Approach for Trust Management in IoT Networks Under Manipulation Attacks." ACM Transactions on Sensor Networks (TOSN) 16 (2020): 1 - 26.

- Samangouei, Pouya, Maya Kabkab and Rama Chellappa. “Defense-GAN: Protecting Classifiers Against Adversarial Attacks Using Generative Models.” ArXiv abs/1805.06605 (2018): n. pag.
- Samavatian, Mohammad Hossein, Saikat Majumdar, Kristin Barber and Radu Teodorescu. “HASI: Hardware-Accelerated Stochastic Inference, A Defense Against Adversarial Machine Learning Attacks.” ArXiv abs/2106.05825 (2021): n. pag.
- Sammani, Fawaz, Tanmoy Mukherjee and Nikos Deligiannis. “NLX-GPT: A Model for Natural Language Explanations in Vision and Vision-Language Tasks.” ArXiv abs/2203.05081 (2022): n. pag.
- Sánchez-Matilla, Ricardo, Chau Yi Li, Ali Shahin Shamsabadi, Riccardo Mazzon and Andrea Cavallaro. “Exploiting Vulnerabilities of Deep Neural Networks for Privacy Protection.” IEEE Transactions on Multimedia 22 (2020): 1862-1873.
- Sang, Jitao, Xian Zhao, Jiaming Zhang and Zhiyu Lin. “Benign Adversarial Attack: Tricking Models for Goodness.” (2021).
- Sarhan, Mohanad, Siamak Layeghy, Marcus R. Gallagher and Marius Portmann. “From Zero-Shot Machine Learning to Zero-Day Attack Detection.” ArXiv abs/2109.14868 (2022): n. pag.
- Sarwar, Omair, Bernhard Rinner and Andrea Cavallaro. “Concealing the identity of faces in oblique images with adaptive hopping Gaussian mixtures.” ArXiv abs/1810.12435 (2018): n. pag.
- Schaeffer, Rylan, Gabrielle K. Liu, Yilun Du, Scott W. Linderman and Ila R. Fiete. “Streaming Inference for Infinite Non-Stationary Clustering.” ArXiv abs/2205.01212 (2022): n. pag.
- Scharwachter, Erik and Emmanuel Muller. “Does terrorism trigger online hate speech? On the association of events and time series.” The Annals of Applied Statistics (2020): n. pag.
- Schink, Marc and Johannes Obermaier. “Taking a Look into Execute-Only Memory.” ArXivabs/1909.05771 (2019): n. pag.
- Schulman, John and Dandelion Mané. “DEFENSIVE QUANTIZATION: WHEN EFFICIENCY MEETS ROBUSTNESS.” (2018).
- Schwarz, Michael, Moritz Lipp, Daniel Gruss, Samuel Weiser, Clémentine Maurice, Raphael Spreitzer and Stefan Mangard. “KeyDrown: Eliminating Keystroke Timing Side-Channel Attacks.” ArXiv abs/1706.06381 (2017): n. pag.
- Schwarzschild, Avi, Micah Goldblum, Arjun Gupta, John P. Dickerson and Tom Goldstein. “Just How Toxic is Data Poisoning? A Unified Benchmark for Backdoor and Data Poisoning Attacks.” ICML (2021).
- Segura, Gustavo A. Nunez, Sotiris Skaperas, Arsenia Chorti, Lefteris Mamatas and Cíntia B. Margi. “Denial of Service Attacks Detection in Software-Defined Wireless Sensor Networks.” 2020 IEEE International Conference on Communications Workshops (ICC Workshops) (2020): 1-7.
- Sena, Luiz, Xidan Song, Erickson H. da S. Alves, Iury V. Bessa, Edoardo Manino and Lucas C. Cordeiro. “Verifying Quantized Neural Networks using SMT-Based Model Checking.” ArXivabs/2106.05997 (2021): n. pag.
- Seng, Jonas, M. Zecevic, Devendra Singh Dhami and Kristian Kersting. “Tearing Apart NOTEARS: Controlling the Graph Prediction via Variance Manipulation.” ArXiv abs/2206.07195 (2022): n. pag.
- Sengupta, Abhrajit, Mohammed Thari Nabeel, Johann Knechtel and Ozgur Sinanoglu. “A New Paradigm in Split Manufacturing: Lock the FEOL, Unlock at the BEOL.” 2019

Design, Automation & Test in Europe Conference & Exhibition (DATE) (2019): 414-419.
- Seyedi, Salman, Li Xiong, Shamim Nemati and Gari D. Clifford. “An Analysis Of Protected Health Information Leakage In Deep-Learning Based De-Identification Algorithms.” ArXivabs/2101.12099 (2021): n. pag.
- Seyedi, Salman, Zifan Jiang, Allan Levey and Gari D. Clifford. “Privacy-Preserving Eye-tracking Using Deep Learning.” ArXiv abs/2106.09621 (2021): n. pag.
- Shafqat, Narmeen, Daniel J. Dubois, David R. Choffnes, Aaron Schulman, Dinesh Bharadia and Aanjhan Ranganathan. “ZLeaks: Passive Inference Attacks on Zigbee based Smart Homes.” ArXivabs/2107.10830 (2022): n. pag.
- Shafran, Avital, Shmuel Peleg and Yedid Hoshen. “Membership Inference Attacks are Easier on Difficult Problems.” 2021 IEEE/CVF International Conference on Computer Vision (ICCV) (2021): 14800-14809.
- Shaham, Sina, Ming Ding, Bo Liu, Zihuai Lin and Jun Yu Li. “Privacy Preservation in Location-Based Services: A Novel Metric and Attack Model.” IEEE Transactions on Mobile Computing 20 (2021): 3006-3019.
- Shan, Shawn, Arjun Nitin Bhagoji, Haitao Zheng and Ben Y. Zhao. “A Real-time Defense against Website Fingerprinting Attacks.” ArXiv abs/2102.04291 (2021): n. pag.
- Shan, Shawn, Wen-Luan Ding, Emily Wenger, Haitao Zheng and Ben Y. Zhao. “Post-breach Recovery: Protection against White-box Adversarial Examples for Leaked DNN Models.” ArXivabs/2205.10686 (2022): n. pag.
- Shao, Rui, Pramuditha Perera, Pong Chi Yuen and Vishal M. Patel. “Federated Face Presentation Attack Detection.” arXiv: Computer Vision and Pattern Recognition (2020): n. pag.
- Sharma, Piyush Kumar, Devashish Gosain and Claudia Díaz. “On the Anonymity of Peer-To-Peer Network Anonymity Schemes Used by Cryptocurrencies.” ArXiv abs/2201.11860 (2022): n. pag.
- Shateri, Mohammadhadi, Francisco Messina, Pablo Piantanida and Fabrice Labeau. “Deep Directed Information-Based Learning for Privacy-Preserving Smart Meter Data Release.” 2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm) (2019): 1-7.
- Shateri, Mohammadhadi, Francisco Messina, Pablo Piantanida and Fabrice Labeau. “Learning Sparse Privacy-Preserving Representations for Smart Meters Data.” 2021 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm) (2021): 333-338.
- Shateri, Mohammadhadi, Francisco Messina, Pablo Piantanida and Fabrice Labeau. “On the Impact of Side Information on Smart Meter Privacy-Preserving Methods.” 2020 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm) (2020): 1-6.
- Shateri, Mohammadhadi, Francisco Messina, Pablo Piantanida and Fabrice Labeau. “Privacy-Cost Management in Smart Meters Using Deep Reinforcement Learning.” 2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe) (2020): 929-933.
- Shateri, Mohammadhadi, Francisco Messina, Pablo Piantanida and Fabrice Labeau. “Real-Time Privacy-Preserving Data Release for Smart Meters.” IEEE Transactions on Smart Grid 11 (2020): 5174-5183.

- Sheikholeslami, Fatemeh, Swayambhoo Jain and Georgios B. Giannakis. “Minimum Uncertainty Based Detection of Adversaries in Deep Neural Networks.” 2020 Information Theory and Applications Workshop (ITA) (2020): 1-16.
- Shejwalkar, Virat and Amir Houmansadr. “Membership Privacy for Machine Learning Models Through Knowledge Transfer.” AAAI (2021).
- Shen, Juncheng, Juzheng Liu, Yiran Chen and Hai Helen Li. “Towards Efficient and Secure Delivery of Data for Training and Inference with Privacy-Preserving.” arXiv: Learning (2018): n. pag.
- Shi, Yi and Yalin Evren Sagduyu. “Membership Inference Attack and Defense for Wireless Signal Classifiers with Deep Learning.” ArXiv abs/2107.12173 (2022): n. pag.
- Shi, Yi, Kemal Davaslioglu and Yalin Evren Sagduyu. “Over-the-air membership inference attacks as privacy threats for deep learning-based wireless signal classifiers.” Proceedings of the 2nd ACM Workshop on Wireless Security and Machine Learning (2020): n. pag.
- Shi, Yi, Tugba Erpek, Yalin Evren Sagduyu and Jason H. Li. “Spectrum Data Poisoning with Adversarial Deep Learning.” MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM) (2018): 407-412.
- Shi, Yi, Yalin Evren Sagduyu, Kemal Davaslioglu and Jason H. Li. “Active Deep Learning Attacks under Strict Rate Limitations for Online API Calls.” 2018 IEEE International Symposium on Technologies for Homeland Security (HST) (2018): 1-6.
- Shi, Yi, Yalin Evren Sagduyu, Kemal Davaslioglu and Jason H. Li. “Generative Adversarial Networks for Black-Box API Attacks with Limited Training Data.” 2018 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT) (2018): 453-458.
- Shokri, R., Marco Stronati, Congzheng Song and Vitaly Shmatikov. “Membership Inference Attacks Against Machine Learning Models.” 2017 IEEE Symposium on Security and Privacy (SP) (2017): 3-18.
- Shokri, R., Martin Strobel and Yair Zick. “On the Privacy Risks of Model Explanations.” Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society (2021): n. pag.
- Shou, Chaofan, Ismet Burak Kadron, Qi Su and Tevfik Bultan. “CorbFuzz: Checking Browser Security Policies with Fuzzing.” 2021 36th IEEE/ACM International Conference on Automated Software Engineering (ASE) (2021): 215-226.
- Shumailov, Ilia, Laurent Simon, Jeff Yan and Ross Anderson. “Hearing your touch: A new acoustic side channel on smartphones.” ArXiv abs/1903.11137 (2019): n. pag.
- Shumailov, Ilia, Yiren Zhao, Daniel Bates, Nicolas Papernot, Robert D. Mullins and Ross Anderson. “Sponge Examples: Energy-Latency Attacks on Neural Networks.” 2021 IEEE European Symposium on Security and Privacy (EuroS&P) (2021): 212-231.
- Sieck, Florian, Sebastian Berndt, Jan Wichelmann and Thomas Eisenbarth. “Util::Lookup: Exploiting Key Decoding in Cryptographic Libraries.” Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (2021): n. pag.
- Sihag, Saurabh and Ali Tajer. “Secure Estimation Under Causative Attacks.” IEEE Transactions on Information Theory 66 (2020): 5145-5166.
- Simas, Tiago, Rion Brattig Correia and Luis Mateus Rocha. “The distance backbone of complex networks.” ArXiv abs/2103.04668 (2021): n. pag.

- Simmons, Anj and Rajesh Vasa. “Signal Knowledge Graph.” ArXiv abs/2206.12111 (2022): n. pag.
- Sirone, Deepak and Pramod Subramanyan. “Functional Analysis Attacks on Logic Locking.” 2019 Design, Automation & Test in Europe Conference & Exhibition (DATE) (2019): 936-939.
- Sivamani, Kirthi Shankar, Rajeev Sahay and Aly El Gamal. “Non-Intrusive Detection of Adversarial Deep Learning Attacks via Observer Networks.” IEEE Letters of the Computer Society 3 (2020): 25-28.
- Sivanathan, Arunan. “IoT Behavioral Monitoring via Network Traffic Analysis.” ArXivabs/2001.10632 (2020): n. pag.
- Song, Congzheng and Ananth Raghunathan. “Information Leakage in Embedding Models.” Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security(2020): n. pag.
- Song, Congzheng and R. Shokri. “Robust Membership Encoding: Inference Attacks and Copyright Protection for Deep Learning.” arXiv: Learning (2019): n. pag.
- Song, Liwei and Prateek Mittal. “Systematic Evaluation of Privacy Risks of Machine Learning Models.” USENIX Security Symposium (2021).
- Song, Liwei, R. Shokri and Prateek Mittal. “Privacy Risks of Securing Machine Learning Models against Adversarial Examples.” Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (2019): n. pag.
- Song, Qun, Zhenyu Yan and Rui Tan. “Moving Target Defense for Deep Visual Sensing against Adversarial Examples.” ACM Trans. Sens. Networks 18 (2022): 5:1-5:32.
- Song, Qun, Zhenyu Yan, Wenjie Luo and Rui Tan. “Sardino: Ultra-Fast Dynamic Ensemble for Secure Visual Sensing at Mobile Edge.” ArXiv abs/2204.08189 (2022): n. pag.
- Sontakke, Sumedh Anand, Buvaneswari Ramanan, Laurent Itti and Thomas Woo. “Model2Detector: Widening the Information Bottleneck for Out-of-Distribution Detection using a Handful of Gradient Steps.” ArXiv abs/2202.11226 (2022): n. pag.
- Souri, Hossein, Micah Goldblum, Liam Fowl, Ramalingam Chellappa and Tom Goldstein. “Sleeper Agent: Scalable Hidden Trigger Backdoors for Neural Networks Trained from Scratch.” ArXivabs/2106.08970 (2021): n. pag.
- Spaans, Jeroen Paul. “Intrinsic Argument Strength in Structured Argumentation: a Principled Approach.” CLAR (2021).
- Srivastava, Brij Mohan Lal, Nathalie Vauquier, Md. Sahidullah, Aurélien Bellet, Marc Tommasi and Emmanuel Vincent. “Evaluating Voice Conversion-Based Privacy Protection against Informed Attackers.” ICASSP 2020 - 2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (2020): 2802-2806.
- Staat, Paul, S R Mulzer, Stefan Roth, Veelasha Moonsamy, Aydin Sezgin and Christof Paar. “IRShield: A Countermeasure Against Adversarial Physical-Layer Wireless Sensing.” ArXivabs/2112.01967 (2021): n. pag.
- Stadler, Theresa, Bristena Oprisanu and Carmela Troncoso. “Synthetic Data -- Anonymisation Groundhog Day.” (2020).
- Stock, Joshua, Jens Wettlaufer, Daniel Demmler and Hannes Federrath. “Property Unlearning: A Defense Strategy Against Property Inference Attacks.” ArXiv abs/2205.08821 (2022): n. pag.

- Stock, Pierre, Igor Shilov, Ilya Mironov and Alexandre Sablayrolles. “Defending against Reconstruction Attacks with Rényi Differential Privacy.” ArXiv abs/2202.07623 (2022): n. pag.
- Stoidis, Dimitrios and Andrea Cavallaro. “Generating gender-ambiguous voices for privacy-preserving speech recognition.” ArXiv abs/2207.01052 (2022): n. pag.
- Stoidis, Dimitrios and Andrea Cavallaro. “Protecting gender and identity with disentangled speech representations.” Interspeech (2021).
- Stripelis, Dimitris, Hamza Saleem, Tanmay Ghai, Nikhil J. Dhinagar, Umang Gupta, Chrysovalantis Anastasiou, Greg Ver Steeg, Srivatsan Ravi, Muhammad Naveed, Paul M. Thompson and J. Ambite. “Secure neuroimaging analysis using federated learning with homomorphic encryption.” Symposium on Medical Information Processing and Analysis (2021).
- Struppek, Lukas, Dominik Hintersdorf, Daniel Neider and Kristian Kersting. “Learning to Break Deep Perceptual Hashing: The Use Case NeuralHash.” 2022 ACM Conference on Fairness, Accountability, and Transparency (2022): n. pag.
- Subedar, Mahesh, Nilesh A. Ahuja, Ranganath Krishnan, Ibrahima J. Ndiour and Omesh Tickoo. “Deep Probabilistic Models to Detect Data Poisoning Attacks.” ArXiv abs/1912.01206 (2019): n. pag.
- Sudhodanan, Avinash, Soheil Khodayari and Juan Caballero. “Cross-Origin State Inference (COSI) Attacks: Leaking Web Site States through XS-Leaks.” ArXiv abs/1908.02204 (2020): n. pag.
- Sun, Chuangchuang, Dong-Ki Kim and Jonathan P. How. “ROMAX: Certifiably Robust Deep Multiagent Reinforcement Learning via Convex Relaxation.” ArXiv abs/2109.06795 (2021): n. pag.
- Sun, Jiankai, Xin Yang, Yuanshun Yao and Chong Wang. “Label Leakage and Protection from Forward Embedding in Vertical Federated Learning.” ArXiv abs/2203.01451 (2022): n. pag.
- Sun, Jingwei, Ang Li, Binghui Wang, Huanrui Yang, Hai Li and Yiran Chen. “Soteria: Provable Defense against Privacy Leakage in Federated Learning from Representation Perspective.” 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2021): 9307-9315.
- Sun, Lichao and L. Lyu. “Federated Model Distillation with Noise-Free Differential Privacy.” IJCAI(2021).
- Sun, Qi-Chao, Ya-li Mao, Yang-Fan Jiang, Qi Zhao, Sijing Chen, Wei Zhang, Weijun Zhang, Xiao Jiang, Teng-Yun Chen, Lixing You, Li Li, Yidong Huang, Xianfeng Chen, Zhen Wang, Xiongfeng Ma, Qiang Zhang and Jian-Wei Pan. “Entanglement swapping with independent sources over an optical-fiber network.” Physical Review A 95 (2017): 032306.
- Sun, Rihui, Pefei Qiu, Yongqiang Lyu, Donsheng Wang, Jiang Dong and Gang Qu. “Lightning: Striking the Secure Isolation on GPU Clouds with Transient Hardware Faults.” ArXivabs/2112.03662 (2021): n. pag.
- Sun, Shuai and Yilin Mo. “Security Protection in Cooperative Control of Multi-agent Systems.” 2021 40th Chinese Control Conference (CCC) (2021): 4696-4701.
- Sun, Zhen, R. Schuster and Vitaly Shmatikov. “De-Anonymizing Text by Fingerprinting Language Generation.” ArXiv abs/2006.09615 (2020): n. pag.
- Sun, Zhichuang, Ruimin Sun and Long Lu. “Mind Your Weight(s): A Large-scale Study on Insufficient Machine Learning Model Protection in Mobile Apps.” ArXiv abs/2002.07687 (2021): n. pag.

- Sung, Keen, Brian Neil Levine and Mariya Zhivkova Zheleva. “ZipPhone: Protecting user location privacy from cellular service providers.” ArXiv abs/2002.04731 (2020): n. pag.
- Suri, Anshuman and David Evans. “Formalizing and Estimating Distribution Inference Risks.” ArXivabs/2109.06024 (2021): n. pag.
- Suri, Anshuman and David Evans. “Formalizing Distribution Inference Risks.” ArXivabs/2106.03699 (2021): n. pag.
- Suri, Anshuman, Pallika H. Kanani, Virendra J. Marathe and Daniel W. Peterson. “Subject Membership Inference Attacks in Federated Learning.” ArXiv abs/2206.03317 (2022): n. pag.
- Szyller, Sebastian, Vasisht Duddu, Tommi Grondahl and N. Asokan. “Good Artists Copy, Great Artists Steal: Model Extraction Attacks Against Image Translation Generative Adversarial Networks.” ArXiv abs/2104.12623 (2021): n. pag.
- Tahmasebian, Farnaz, Jian Lou and Li Xiong. “RobustFed: A Truth Inference Approach for Robust Federated Learning.” ArXiv abs/2107.08402 (2021): n. pag.
- Takko, Tuomas, Kunal Bhattacharya, Martti Lehto, Pertti Jalasvirta, Aapo Cederberg and Kimmo K. Kaski. “Knowledge mining of unstructured information: application to cyber-domain.” ArXivabs/2109.03848 (2021): n. pag.
- Tan, Jasper, Blake Mason, Hamid Javadi and Richard Baraniuk. “Parameters or Privacy: A Provable Tradeoff Between Overparameterization and Membership Inference.” ArXivabs/2202.01243 (2022): n. pag.
- Tan, Jasper, Daniel LeJeune, Blake Mason, Hamid Javadi and Richard Baraniuk. “Benign Overparameterization in Membership Inference with Early Stopping.” ArXiv abs/2205.14055 (2022): n. pag.
- Tan, Juntao, Lan Zhang, Yang Liu, Anran Li and Yeshu Wu. “Residue-based Label Protection Mechanisms in Vertical Logistic Regression.” ArXiv abs/2205.04166 (2022): n. pag.
- Tang, Xinyu, Saeed Mahloujifar, Liwei Song, Virat Shejwalkar, Milad Nasr, Amir Houmansadr and Prateek Mittal. “Mitigating Membership Inference Attacks by Self-Distillation Through a Novel Ensemble Architecture.” ArXiv abs/2110.08324 (2021): n. pag.
- Tao, Guanhong, Shiqing Ma, Yingqi Liu and X. Zhang. “Attacks Meet Interpretability: Attribute-steered Detection of Adversarial Samples.” ArXiv abs/1810.11580 (2018): n. pag.
- Tao, Liangde, Lin Chen, Lei Xu and W. Shi. “Local Differential Privacy Meets Computational Social Choice - Resilience under Voter Deletion.” ArXiv abs/2205.00771 (2022): n. pag.
- Tao, Shuchang, Qi Cao, Huawei Shen, Junjie Huang, Yunfan Wu and Xueqi Cheng. “Single Node Injection Attack against Graph Neural Networks.” Proceedings of the 30th ACM International Conference on Information & Knowledge Management (2021): n. pag.
- Teerapittayanon, Surat and H. T. Kung. “DaiMoN: A Decentralized Artificial Intelligence Model Network.” 2019 IEEE International Conference on Blockchain (Blockchain) (2019): 132-139.
- Thiruloga, Sooryaa Vignesh, Vipin Kumar Kukkala and Sudeep Pasricha. “TENET: Temporal CNN with Attention for Anomaly Detection in Automotive Cyber-Physical Systems.” 2022 27th Asia and South Pacific Design Automation Conference (ASP-DAC) (2022): 326-331.

- Thorne, James and Andreas Vlachos. “Adversarial attacks against Fact Extraction and VERification.” ArXiv abs/1903.05543 (2019): n. pag.
- Thudi, Anvith, Ilia Shumailov, Franziska Boenisch and Nicolas Papernot. “Bounding Membership Inference.” ArXiv abs/2202.12232 (2022): n. pag.
- Tian, Guiyu, Wenhao Jiang, Wei Liu and Yadong Mu. “Poisoning MorphNet for Clean-Label Backdoor Attack to Point Clouds.” ArXiv abs/2105.04839 (2021): n. pag.
- Tian, Qi, Kun Kuang, Ke Jiang, Fei Wu and Yisen Wang. “Analysis and Applications of Class-wise Robustness in Adversarial Training.” Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery & Data Mining (2021): n. pag.
- Tian, Yongqiang, Shiqing Ma, Ming Wen, Yepang Liu, S. C. Cheung and X. Zhang. “Testing Deep Learning Models for Image Analysis Using Object-Relevant Metamorphic Relations.” ArXivabs/1909.03824 (2019): n. pag.
- Toffalini, Flavio, Mathias Payer, Jianying Zhou and Lorenzo Cavallaro. “Designing a Provenance Analysis for SGX Enclaves.” ArXiv abs/2206.07418 (2022): n. pag.
- Tol, M. Caner, Saad Islam, Berk Sunar and Ziming Zhang. “Toward Realistic Backdoor Injection Attacks on DNNs using Rowhammer.” (2021).
- Tomashenko, Natalia A., Salima Mdhaffar, Marc Tommasi, Y. Estève and Jean-François Bonastre. “Privacy attacks for automatic speech recognition acoustic models in a federated learning framework.” ICASSP (2022).
- Tonni, Shakila Mahjabin, Farhad Farokhi, Dinusha Vatsalan and Dali Kaafar. “Data and Model Dependencies of Membership Inference Attack.” ArXiv abs/2002.06856 (2020): n. pag.
- Tople, Shruti, Amit Sharma and Aditya V. Nori. “Alleviating Privacy Attacks via Causal Learning.” ArXiv abs/1909.12732 (2020): n. pag.
- Tramèr, Florian, R. Shokri, Ayrton San Joaquin, Hoang M. Le, Matthew Jagielski, Sanghyun Hong and Nicholas Carlini. “Truth Serum: Poisoning Machine Learning Models to Reveal Their Secrets.” ArXiv abs/2204.00032 (2022): n. pag.
- Trimananda, Rahmadi, Janus Varmarken, Athina Markopoulou and Brian Demsky. “PingPong: Packet-Level Signatures for Smart Home Device Events.” ArXiv abs/1907.11797 (2019): n. pag.
- Troupe, James E. and Jacob M. Farinholt. “Quantum Cryptography with Weak Measurements.” arXiv: Quantum Physics (2017): n. pag.
- Truex, Stacey, Ling Liu, Mehmet Emre Gursoy, Lei Yu and Wenqi Wei. “Towards Demystifying Membership Inference Attacks.” ArXiv abs/1807.09173 (2018): n. pag.
- Truex, Stacey, Ling Liu, Mehmet Emre Gursoy, Wenqi Wei and Lei Yu. “Effects of Differential Privacy and Data Skewness on Membership Inference Vulnerability.” 2019 First IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)(2019): 82-91.
- Truex, Stacey, Nathalie Baracaldo, Ali Anwar, Thomas Steinke, Heiko Ludwig and Rui Zhang. “A Hybrid Approach to Privacy-Preserving Federated Learning.” Proceedings of the 12th ACM Workshop on Artificial Intelligence and Security (2019): n. pag.
- Tsai, Chi-Yo, Gaurav Kumar Agarwal, Christina Fragouli and Suhas N. Diggavi. “A distortion based approach for protecting inferences.” 2017 IEEE International Symposium on Information Theory (ISIT) (2017): 1913-1917.
- Tseng, Wei-Cheng, Wei-Tsung Kao and Hung-yi Lee. “Membership Inference Attacks Against Self-supervised Speech Models.” ArXiv abs/2111.05113 (2021): n. pag.
- Turner, Alexander, Dimitris Tsipras and Aleksander Madry. “Label-Consistent Backdoor Attacks.” ArXiv abs/1912.02771 (2019): n. pag.

- Uchendu, Adaku, Daniel Campoy, Christopher Menart and Alexandra Hildenbrandt. “Robustness of Bayesian Neural Networks to White-Box Adversarial Attacks.” 2021 IEEE Fourth International Conference on Artificial Intelligence and Knowledge Engineering (AIKE) (2021): 72-80.
- Uppal, Utkarsh and Bharat Giddwani. “Normalized Label Distribution: Towards Learning Calibrated, Adaptable and Efficient Activation Maps.” ArXiv abs/2012.06876 (2020): n. pag.
- Usman, Muhammad, Divya Gopinath, Youcheng Sun, Yannic Noller and Corina S. Pasareanu. “NNrepair: Constraint-based Repair of Neural Network Classifiers.” CAV (2021).
- Usynin, Dmitrii, Helena Klause, Daniel Rueckert and Georgios Kaissis. “Can collaborative learning be private, robust and scalable?” ArXiv abs/2205.02652 (2022): n. pag.
- Vadera, Meet P., Satya Narayan Shukla, Borhan Jalaeian and Benjamin M Marlin. “Assessing the Adversarial Robustness of Monte Carlo and Distillation Methods for Deep Bayesian Neural Network Classification.” ArXiv abs/2002.02842 (2020): n. pag.
- Veale, Michael, Reuben Binns and Lilian Edwards. “Algorithms that remember: model inversion attacks and data protection law.” Philosophical transactions. Series A, Mathematical, physical, and engineering sciences 376 (2018): n. pag.
- Venkatesaramani, Rajagopal, Zhiyu Wan, Bradley A. Malin and Yevgeniy Vorobeychik. “Defending Against Membership Inference Attacks on Beacon Services.” ArXiv abs/2112.13301 (2021): n. pag.
- Vepakomma, Praneeth, Abhishek Singh, Otkrist Gupta and Ramesh Raskar. “NoPeek: Information leakage reduction to share activations in distributed deep learning.” 2020 International Conference on Data Mining Workshops (ICDMW) (2020): 933-942.
- Villarreal-Vasquez, Miguel and Bharat K. Bhargava. “ConFoc: Content-Focus Protection Against Trojan Attacks on Neural Networks.” ArXiv abs/2007.00711 (2020): n. pag.
- Wallace, Eric, Mitchell Stern and Dawn Xiaodong Song. “Imitation Attacks and Defenses for Black-box Machine Translation Systems.” EMNLP (2020).
- Wan, Junpeng, Yanxiang Bi, Zhe Zhou and Zhou Li. “Volcano: Stateless Cache Side-channel Attack by Exploiting Mesh Interconnect.” ArXiv abs/2103.04533 (2021): n. pag.
- Wang, Binghui and Neil Zhenqiang Gong. “Attacking Graph-based Classification via Manipulating the Graph Structure.” Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (2019): n. pag.
- Wang, Binghui, Jinyuan Jia and Neil Zhenqiang Gong. “Graph-based Security and Privacy Analytics via Collective Classification with Joint Weight Learning and Propagation.” ArXivabs/1812.01661 (2019): n. pag.
- Wang, Boxin, Shuohang Wang, Yu Cheng, Zhe Gan, R. Jia, Bo Li and Jingjing Liu. “InfoBERT: Improving Robustness of Language Models from An Information Theoretic Perspective.” ArXivabs/2010.02329 (2021): n. pag.
- Wang, Chenggang, Sean Kennedy, Haipeng Li, King Hudson, Gowtham Atluri, Xuetao Wei, Wenhai Sun and Boyang Wang. “Fingerprinting encrypted voice traffic on smart speakers with deep learning.” Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks (2020): n. pag.

- Wang, Han. “Leaked-Web: Accurate and Efficient Machine Learning-Based Website Fingerprinting Attack through Hardware Performance Counters.” ArXiv abs/2110.01202 (2021): n. pag.
- Wang, Hang, Zhen Xiang, David J. Miller and George Kesidis. “Universal Post-Training Backdoor Detection.” ArXiv abs/2205.06900 (2022): n. pag.
- Wang, Hanrui, Xingbo Dong, Zhe Jin, A.B.J. Teoh and M. Tistarelli. “Interpretable security analysis of cancellable biometrics using constrained-optimized similarity-based attack.” 2021 IEEE Winter Conference on Applications of Computer Vision Workshops (WACVW) (2021): 70-77.
- Wang, Jiali and Martin Neil. “A Bayesian-network-based cybersecurity adversarial risk analysis framework with numerical examples.” ArXiv abs/2106.00471 (2021): n. pag.
- Wang, Jingjing, Jingyi Zhang, Ying Bian, Youyi Cai, Chunmao Wang and Shiliang Pu. “Self-Domain Adaptation for Face Anti-Spoofing.” ArXiv abs/2102.12129 (2021): n. pag.
- Wang, Jinwen, Yueqiang Cheng, Qi Li and Yong Jiang. “Interface-Based Side Channel Attack Against Intel SGX.” ArXiv abs/1811.05378 (2018): n. pag.
- Wang, Lixu, Shichao Xu, Xiao Wang and Qi Zhu. “Eavesdrop the Composition Proportion of Training Labels in Federated Learning.” ArXiv abs/1910.06044 (2019): n. pag.
- Wang, Lun, Qi Pang, Shuai Wang and Dawn Xiaodong Song. “Towards Bidirectional Protection in Federated Learning.” (2020).
- Wang, Qian and Daniel Kurz. “Reconstructing Training Data from Diverse ML Models by Ensemble Inversion.” 2022 IEEE/CVF Winter Conference on Applications of Computer Vision (WACV) (2022): 3870-3878.
- Wang, Qifan, Shujie Cui, Lei Zhou, Ocean Wu, Yong Zhu and Giovanni Russello. “EnclaveTree: Privacy-preserving Data Stream Training and Inference Using TEE.” Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security (2022): n. pag.
- Wang, Shusen. “Matrix Sketching for Secure Collaborative Machine Learning.” ICML (2021).
- Wang, Tianhao, Yuheng Zhang and R. Jia. “Improving Robustness to Model Inversion Attacks via Mutual Information Regularization.” AAAI (2021).
- Wang, Tong, Yuan Yao, Feng Xu, Shengwei An, Hanghang Tong and Ting Wang. “Backdoor Attack through Frequency Domain.” ArXiv abs/2111.10991 (2021): n. pag.
- Wang, Yijue, Chenghong Wang, Zigeng Wang, Shangli Zhou, Hang Liu, Jinbo Bi, Caiwen Ding and Sanguthevar Rajasekaran. “Against Membership Inference Attack: Pruning is All You Need.” IJCAI(2021).
- Wang, Yu and Lichao Sun. “Membership Inference Attacks on Knowledge Graphs.” ArXivabs/2104.08273 (2021): n. pag.
- Wang, Yu, Jiebo Luo, Richard G. Niemi, Y. Li and Tianran Hu. “Catching Fire via "Likes": Inferring Topic Preferences of Trump Followers on Twitter.” ArXiv abs/1603.03099 (2016): n. pag.
- Wang, Zhuo, Zezheng Wang, Zitong Yu, Weihong Deng, Jiahong Li, Size Li and Zhong Wang. “Domain Generalization via Shuffled Style Assembly for Face Anti-Spoofing.” ArXivabs/2203.05340 (2022): n. pag.
- Wang, Zihan, Na Huang, Fei Sun, Pengjie Ren, Zhumin Chen, Hengliang Luo, M. de Rijke and Zhaochun Ren. “Debiasing Learning for Membership Inference Attacks Against Recommender Systems.” ArXiv abs/2206.12401 (2022): n. pag.

- Watson, Lauren, Chuan Guo, Graham Cormode and Alexandre Sablayrolles. “On the Importance of Difficulty Calibration in Membership Inference Attacks.” ArXiv abs/2111.08440 (2021): n. pag.
- Weiss, Jonah O’Brien, Tiago A. O. Alves and Sandip Kundu. “Hardening DNNs against Transfer Attacks during Network Compression using Greedy Adversarial Pruning.” ArXiv abs/2206.07406 (2022): n. pag.
- Weng, Haiqin, Juntao Zhang, Feng Xue, Tao Wei, Shouling Ji and Zhiyuan Zong. “Privacy Leakage of Real-World Vertical Federated Learning.” ArXiv abs/2011.09290 (2020): n. pag.
- Weng, Jiasi, Jian Weng, Hongwei Huang, Chengjun Cai and Cong Wang. “FedServing: A Federated Prediction Serving Framework Based on Incentive Mechanism.” IEEE INFOCOM 2021 - IEEE Conference on Computer Communications (2021): 1-10.
- Whitaker, Gavin A., Ricardo Silva and Daniel L. Edwards. “Modeling goal chances in soccer: a Bayesian inference approach.” arXiv: Applications (2018): n. pag.
- Whitehill, Jacob. “Climbing the Kaggle Leaderboard by Exploiting the Log-Loss Oracle.” ArXivabs/1707.01825 (2018): n. pag.
- Won, Yoo-Seung, Soham Chatterjee, Dirmanto Jap, Arindam Basu and Shivam Bhasin. “DeepFreeze: Cold Boot Attacks and High Fidelity Model Recovery on Commercial EdgeML Device.” 2021 IEEE/ACM International Conference On Computer Aided Design (ICCAD) (2021): 1-9.
- Wood, Michael. “How sure are we? Two approaches to statistical inference.” arXiv: Other Statistics (2018): n. pag.
- Woods, Walt. “RL-GRIT: Reinforcement Learning for Grammar Inference.” 2021 IEEE Security and Privacy Workshops (SPW) (2021): 171-183.
- Woszczyk, Dominika, Alvin Lee and Soteris Demetriou. “Open, Sesame!: Introducing Access Control to Voice Services.” Proceedings of the 1st Workshop on Security and Privacy for Mobile AI(2021): n. pag.
- Wu, Bang, Shuo Wang, Xingliang Yuan, Cong Wang, Carsten Rudolph and Xiangwen Yang. “Defeating Misclassification Attacks Against Transfer Learning.” IEEE Transactions on Dependable and Secure Computing (2022): n. pag.
- Wu, Bang, Xiangwen Yang, Shirui Pan and Xingliang Yuan. “Adapting Membership Inference Attacks to GNN for Graph Classification: Approaches and Implications.” 2021 IEEE International Conference on Data Mining (ICDM) (2021): 1421-1426.
- Wu, Chuhan, Fangzhao Wu, Tao Qi, Yongfeng Huang and Xing Xie. “FedAttack: Effective and Covert Poisoning Attack on Federated Recommendation via Hard Sampling.” ArXivabs/2202.04975 (2022): n. pag.
- Wu, Fan, Yunhui Long, Ce Zhang and Bo Li. “LinkTeller: Recovering Private Edges from Graph Neural Networks via Influence Analysis.” ArXiv abs/2108.06504 (2021): n. pag.
- Wu, Hao, Yuhang Gong, Xiaopeng Ke, Hanzhong Liang, Minghao Li, Fengyuan Xu, Yunxin Liu and Sheng Zhong. “Automation Slicing and Testing for in-App Deep Learning Models.” ArXivabs/2205.07228 (2022): n. pag.
- Wu, Jing, Mingyi Zhou, Shuaicheng Liu, Yipeng Liu and Ce Zhu. “Decision-based Universal Adversarial Attack.” ArXiv abs/2009.07024 (2020): n. pag.
- Wu, Kunhong, Yucheng Shi, Yahong Han, Yunfeng Shao, Bingshuai Li and Qi Tian. “Domain Adaptation without Model Transferring.” (2021).

- Wu, Maoqiang, Xinyue Zhang, Jiahao Ding, Hien Van Nguyen, Rong Yu, Miao Pan and Stephen T. C. Wong. “Evaluation of Inference Attack Models for Deep Learning on Medical Data.” ArXivabs/2011.00177 (2020): n. pag.
- Wu, Ruihan, Jinfu Zhou, Kilian Q. Weinberger and Chuan Guo. “Does Label Differential Privacy Prevent Label Inference Attacks?” ArXiv abs/2202.12968 (2022): n. pag.
- Wu, Young, Jermey McMahan, Xiaojin Zhu and Qiaomin Xie. “Reward Poisoning Attacks on Offline Multi-Agent Reinforcement Learning.” ArXiv abs/2206.01888 (2022): n. pag.
- Wunderlich, Dominik, Daniel Bernau, Francesco Aldà, Javier Parra-Arnau and Thorsten Strufe. “On the privacy-utility trade-off in differentially private hierarchical text classification.” ArXivabs/2103.02895 (2021): n. pag.
- Xiang, Liyao, Hao Zhang, Haotian Ma, Yifan Zhang, Jie Ren and Quanshi Zhang. “Interpretable Complex-Valued Neural Networks for Privacy Protection.” arXiv: Learning (2020): n. pag.
- Xiang, Zhen, David J. Miller and George Kesidis. “Detection of Backdoors in Trained Classifiers Without Access to the Training Set.” IEEE Transactions on Neural Networks and Learning Systems33 (2022): 1177-1191.
- Xiang, Zhen, David J. Miller and George Kesidis. “Revealing Perceptible Backdoors, without the Training Set, via the Maximum Achievable Misclassification Fraction Statistic.” ArXivabs/1911.07970 (2019): n. pag.
- Xiang, Zhen, David J. Miller, Siheng Chen, Xi Li and George Kesidis. “Detecting Backdoor Attacks Against Point Cloud Classifiers.” ICASSP (2022).
- Xiao, Yuan, Mengyuan Li, Sanchuan Chen and Yinqian Zhang. “STACCO: Differentially Analyzing Side-Channel Traces for Detecting SSL/TLS Vulnerabilities in Secure Enclaves.” Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (2017): n. pag.
- Xie, Cihang, Jianyu Wang, Zhishuai Zhang, Zhou Ren and Alan Loddon Yuille. “Mitigating adversarial effects through randomization.” ArXiv abs/1711.01991 (2018): n. pag.
- Xie, Yuan-ai, Jiawen Kang, Dusit Tao Niyato, Nguyen Thi Thanh Van, Nguyen Cong Luong, Zhixin Liu and Han Yu. “Securing Federated Learning: A Covert Communication-based Approach.” ArXivabs/2110.02221 (2021): n. pag.
- Xiong, Sijie, Anand D. Sarwate and Narayan B. Mandayam. “Network Traffic Shaping for Enhancing Privacy in IoT Systems.” IEEE/ACM Transactions on Networking 30 (2022): 1162-1177.
- Xu, Haifeng, Shaddin Dughmi, Milind Tambe and Venil Loyd Noronha. “Mitigating the Curse of Correlation in Security Games by Entropy Maximization.” AAMAS (2018).
- Xu, Henry, An Ju and David A. Wagner. “Model-Agnostic Defense for Lane Detection against Adversarial Attack.” ArXiv abs/2103.00663 (2021): n. pag.
- Xu, Jie, Lingjie Duan and Rui Zhang. “Surveillance and Intervention of Infrastructure-Free Mobile Communications: A New Wireless Security Paradigm.” IEEE Wireless Communications 24 (2017): 152-159.
- Xu, Jie, Wei Zhang and Fei Wang. “A(DP)2SGD: Asynchronous Decentralized Parallel Stochastic Gradient Descent with Differential Privacy.” IEEE transactions on pattern analysis and machine intelligence PP (2021): n. pag.

- Xu, Mengting, T. Zhang, Zhongnian Li, Mingxia Liu and Daoqiang Zhang. “Towards Evaluating the Robustness of Deep Diagnostic Models by Adversarial Attack.” Medical image analysis 69 (2021): 101977 .
- Xu, Mengting, Tao Zhang and Daoqiang Zhang. “MedRDF: A Robust and Retrain-Less Diagnostic Framework for Medical Pretrained Models Against Adversarial Attack.” IEEE transactions on medical imaging PP (2022): n. pag.
- Xu, Nuo, Binghui Wang, Ran Ran, Wujie Wen and Parv Venkitasubramaniam. “NeuGuard: Lightweight Neuron-Guided Defense against Membership Inference Attacks.” ArXivabs/2206.05565 (2022): n. pag.
- Xu, Runhua, Nathalie Baracaldo and James Joshi. “Privacy-Preserving Machine Learning: Methods, Challenges and Directions.” ArXiv abs/2108.04417 (2021): n. pag.
- Xu, Runhua, Nathalie Baracaldo, Yi Zhou, Ali Anwar, Swanand Kadhe and Heiko Ludwig. “DeTrust-FL: Privacy-Preserving Federated Learning in Decentralized Trust Setting.” ArXiv abs/2207.07779 (2022): n. pag.
- Xu, Xiaogang, Hengshuang Zhao and Jiaya Jia. “Dynamic Divide-and-Conquer Adversarial Training for Robust Semantic Segmentation.” 2021 IEEE/CVF International Conference on Computer Vision (ICCV) (2021): 7466-7475.
- Xu, Zirui, Fuxun Yu and Xiang Chen. “LanCe: A Comprehensive and Lightweight CNN Defense Methodology against Physical Adversarial Attacks on Embedded Multimedia Applications.” 2020 25th Asia and South Pacific Design Automation Conference (ASP-DAC) (2020): 470-475.
- Xue, Mingfu, Chengxiang Yuan, Can He, Zhiyu Wu, Yushu Zhang, Zhe Liu and Weiqiang Liu. “Use the Spear as a Shield: A Novel Adversarial Example based Privacy-Preserving Technique against Membership Inference Attacks.” ArXiv abs/2011.13696 (2022): n. pag.
- Xue, Mingfu, Yinghao Wu, Zhiyu Wu, Jian Wang, Yushu Zhang and Weiqiang Liu. “Detecting Backdoor in Deep Neural Networks via Intentional Adversarial Perturbations.” ArXivabs/2105.14259 (2021): n. pag.
- Yan, Haonan, Xiaoguang Li, Hui Li, Jiamin Li, Wenhai Sun and Fenghua Li. “Monitoring-based Differential Privacy Mechanism Against Query-Flooding Parameter Duplication Attack.” ArXivabs/2011.00418 (2020): n. pag.
- Yan, Mengjia, Christopher W. Fletcher and Josep Torrellas. “Cache Telepathy: Leveraging Shared Resource Attacks to Learn DNN Architectures.” ArXiv abs/1808.04761 (2020): n. pag.
- Yan, Zhiwen and Teck Khim Ng. “Adaptive Modeling Against Adversarial Attacks.” ArXivabs/2112.12431 (2021): n. pag.
- Yang, Chao-Han Huck, I-Te Danny Hung, Yi-Chieh Liu and Pin-Yu Chen. “Treatment Learning Transformer for Noisy Image Classification.” ArXiv abs/2203.15529 (2022): n. pag.
- Yang, Fangfang and Shaolei Ren. “Adversarial Attacks on Brain-Inspired Hyperdimensional Computing-Based Classifiers.” ArXiv abs/2006.05594 (2020): n. pag.
- Yang, Ruikang, Jianfeng Ma, Yinbin Miao and Xindi Ma. “Privacy-preserving Generative Framework Against Membership Inference Attacks.” ArXiv abs/2202.05469 (2022): n. pag.
- Yang, Xue, Yan Feng, Weijun Fang, Jun Shao, Xiaohu Tang, Shutao Xia and Rongxing Lu. “An Accuracy-Lossless Perturbation Method for Defending Privacy Attacks in Federated Learning.” Proceedings of the ACM Web Conference 2022 (2022): n. pag.

- Yang, Yijun, Ruiyuan Gao, Yu Li, Qiuxia Lai and Qiang Xu. “MixDefense: A Defense-in-Depth Framework for Adversarial Example Detection Based on Statistical and Semantic Analysis.” ArXivabs/2104.10076 (2021): n. pag.
- Yang, Yijun, Ruiyuan Gao, Yu Li, Qiuxia Lai and Qiang Xu. “What You See is Not What the Network Infers: Detecting Adversarial Examples Based on Semantic Contradiction.” ArXiv abs/2201.09650 (2022): n. pag.
- Yang, Yunhao, Parham Gohari and Ufuk Topcu. “Additive Logistic Mechanism for Privacy-Preserving Self-Supervised Learning.” ArXiv abs/2205.12430 (2022): n. pag.
- Yang, Yunhao, Parham Gohari and Ufuk Topcu. “On the Privacy Risks of Deploying Recurrent Neural Networks in Machine Learning Models.” (2021).
- Yang, Zhixiong, Arpita Gang and Waheed Uz Zaman Bajwa. “Adversary-Resilient Distributed and Decentralized Statistical Inference and Machine Learning: An Overview of Recent Advances Under the Byzantine Threat Model.” IEEE Signal Processing Magazine 37 (2020): 146-159.
- Yang, Ziqi, Bin Shao, Bohan Xuan, Ee-Chien Chang and Fan Zhang. “Defending Model Inversion and Membership Inference Attacks via Prediction Purification.” ArXiv abs/2005.03915 (2020): n. pag.
- Yao, Fan, Adnan Siraj Rakin and Deliang Fan. “DeepHammer: Depleting the Intelligence of Deep Neural Networks through Targeted Chain of Bit Flips.” ArXiv abs/2003.13746 (2020): n. pag.
- Yao, Feng, Suleiman Y. Yerima, Boojoong Kang and Sakir Sezer. “Continuous implicit authentication for mobile devices based on adaptive neuro-fuzzy inference system.” 2017 International Conference on Cyber Security And Protection Of Digital Services (Cyber Security)(2017): 1-7.
- Yao, Qingsong, Zecheng He and S. Kevin Zhou. “Medical Aegis: Robust adversarial protectors for medical images.” ArXiv abs/2111.10969 (2021): n. pag.
- Yao, Yuan, Haoxiang Zhong, Zhengyan Zhang, Xu Han, Xiaozhi Wang, Kai Zhang, Chaojun Xiao, Guoyang Zeng, Zhiyuan Liu and Maosong Sun. “Adversarial Language Games for Advanced Natural Language Intelligence.” AAAI (2021).
- Yarkony, Julian and Kamalika Chaudhuri. “Convex Optimization For Non-Convex Problems via Column Generation.” ArXiv abs/1602.04409 (2016): n. pag.
- Ye, Dayong, Sheng Shen, Tianqing Zhu, B. Liu and Wanlei Zhou. “One Parameter Defense—Defending Against Data Inference Attacks via Differential Privacy.” IEEE Transactions on Information Forensics and Security 17 (2022): 1466-1480.
- Ye, Dayong, Tianqing Zhu, Sheng Shen and Wanlei Zhou. “A Differentially Private Game Theoretic Approach for Deceiving Cyber Adversaries.” IEEE Transactions on Information Forensics and Security 16 (2021): 569-584.
- Ye, Jiayuan, Aadyaa Maddi, Sasi Kumar Murakonda and R. Shokri. “Enhanced Membership Inference Attacks against Machine Learning Models.” ArXiv abs/2111.09679 (2021): n. pag.
- Yeom, Samuel, Irene Giacomelli, Matt Fredrikson and Somesh Jha. “Privacy Risk in Machine Learning: Analyzing the Connection to Overfitting.” 2018 IEEE 31st Computer Security Foundations Symposium (CSF) (2018): 268-282.
- Yilmaz, Emre, Tianxi Ji, Erman Ayday and Pan Li. “Genomic Data Sharing under Dependent Local Differential Privacy.” Proceedings of the Twelfth ACM Conference on Data and Application Security and Privacy (2022): n. pag.
- Yin, Zeyuan, Ye Yuan, Panfeng Guo and Pan Zhou. “Backdoor Attacks on Federated Learning with Lottery Ticket Hypothesis.” ArXiv abs/2109.10512 (2021): n. pag.

- Yong, Sze Zheng, Minghui Zhu and Emilio Frazzoli. “Switching and Data Injection Attacks on Stochastic Cyber-Physical Systems.” ACM Transactions on Cyber-Physical Systems 2 (2018): 1 - 2.
- Yoon, Man-Ki, Jung-Eun Kim, Richard M. Bradford and Zhong Shao. “TaskShuffler++: Real-Time Schedule Randomization for Reducing Worst-Case Vulnerability to Timing Inference Attacks.” ArXiv abs/1911.07726 (2019): n. pag.
- Yu, Da, Gautam Kamath, Janardhan Kulkarni, Tie-Yan Liu, Jian Yin and Huishuai Zhang. “Per-Instance Privacy Accounting for Differentially Private Stochastic Gradient Descent.” ArXivabs/2206.02617 (2022): n. pag.
- Yu, Da, Huishuai Zhang, Wei Chen, Jian Yin and Tie-Yan Liu. “How Does Data Augmentation Affect Privacy in Machine Learning?” AAAI (2021).
- Yu, Ruotong, Francesca Del Nin, Yuchen Zhang, Shan Huang, Pallavi Kaliyar, Sarah Zakto, Mauro Conti, Georgios Portokalidis and Jun Xu. “Building Embedded Systems Like It’s 1996.” ArXivabs/2203.06834 (2022): n. pag.
- Yu, S., Yulei Niu, Shuohang Wang, Jing Jiang and Qianru Sun. “Counterfactual Variable Control for Robust and Interpretable Question Answering.” ArXiv abs/2010.05581 (2020): n. pag.
- Yu, Xiaotian, Hanling Yi, Yi Yu, Ling Xing, Shiliang Zhang and Xiaoyu Wang. “Enhancing Social Relation Inference with Concise Interaction Graph and Discriminative Scene Representation.” ArXiv abs/2107.14425 (2021): n. pag.
- Yuan, Fengkai, Kai Wang, Rui Hou, Xiaoxin Li, Peinan Li, Lutan Zhao, Jiameng Ying, Amro Awad and Dan Meng. “PiPoMonitor: Mitigating Cross-core Cache Attacks Using the Auto-Cuckoo Filter.” 2021 Design, Automation & Test in Europe Conference & Exhibition (DATE) (2021): 1697-1702.
- Yuan, Xiaoyong and Lan Zhang. “Membership Inference Attacks and Defenses in Neural Network Pruning.” ArXiv abs/2202.03335 (2022): n. pag.
- Yue, K., Richeng Jin, Chau-Wai Wong and Huaiyu Dai. “Federated Learning via Plurality Vote.” ArXivabs/2110.02998 (2021): n. pag.
- Yue, Xiang, Minxin Du, Tianhao Wang, Yaliang Li, Huan Sun and Sherman S. M. Chow. “Differential Privacy for Text Analytics via Natural Text Sanitization.” FINDINGS (2021).
- Zanella-B’eguelin, Santiago, Lukas Wutschitz, Shruti Tople, A. Salem, Victor Ruhle, Andrew J. Paverd, Mohammad Naseri and Boris Kopf. “Bayesian Estimation of Differential Privacy.” ArXivabs/2206.05199 (2022): n. pag.
- Zang, Yuan, Bairu Hou, Fanchao Qi, Zhiyuan Liu, Xiaojun Meng and Maosong Sun. “Learning to Attack: Towards Textual Adversarial Attacking in Real-world Situations.” ArXiv abs/2009.09192 (2020): n. pag.
- Zarandy, Almos, Ilia Shumailov and Ross Anderson. “Hey Alexa what did I just type? Decoding smartphone sounds with a voice assistant.” ArXiv abs/2012.00687 (2020): n. pag.
- Zari, Oualid, Chuan Xu and Giovanni Neglia. “Efficient passive membership inference attack in federated learning.” ArXiv abs/2111.00430 (2021): n. pag.
- Zeng, Yi, Han Qiu, Shangwei Guo, Tianwei Zhang, Meikang Qiu and Bhavani M. Thuraisingham. “DeepSweep: An Evaluation Framework for Mitigating DNN Backdoor Attacks using Data Augmentation.” Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security (2021): n. pag.

- Zeng, Yi, Minzhou Pan, Hoang A. Just, L. Lyu, Meikang Qiu and R. Jia. “Narcissus: A Practical Clean-Label Backdoor Attack with Limited Information.” ArXiv abs/2204.05255 (2022): n. pag.
- Zhan, Pengwei, Liming Wang and Yi Tang. “Website Fingerprinting on Early QUIC Traffic.” ArXivabs/2101.11871 (2021): n. pag.
- Zhang, Bo, Ruotong Yu, Haipei Sun, Yanying Li, Jun Xu and Wendy Hui Wang. “Privacy for All: Demystify Vulnerability Disparity of Differential Privacy against Membership Inference Attack.” ArXiv abs/2001.08855 (2020): n. pag.
- Zhang, Haimin and Min Xu. “Improving Transformation-based Defenses against Adversarial Examples with First-order Perturbations.” (2021).
- Zhang, Honglei, Fangyuan Luo, Jun Wu, Xiangnan He and Yidong Li. “LightFR: Lightweight Federated Recommendation with Privacy-preserving Matrix Factorization.” ArXiv abs/2206.11743 (2022): n. pag.
- Zhang, Jie, Dongdong Chen, Jing Liao, Weiming Zhang, Gang Hua and Nenghai Yu. “Passport-aware Normalization for Deep Model Protection.” ArXiv abs/2010.15824 (2020): n. pag.
- Zhang, Jinxue. “Private Social Network Data Sharing.” (2017).
- Zhang, Kai, Yu Wang, Hongyi Wang, Lifu Huang, Carl Yang and Lichao Sun. “Efficient Federated Learning on Knowledge Graphs via Privacy-preserving Relation Embedding Aggregation.” ArXivabs/2203.09553 (2022): n. pag.
- Zhang, Kaixiang, Kaian Chen, Zhaojian Li, Jun Chen and Yang Zheng. “Privacy-Preserving Data-Enabled Predictive Leading Cruise Control in Mixed Traffic.” ArXiv abs/2205.10916 (2022): n. pag.
- Zhang, Kaixiang, Zhaojian Li, Yongqiang Wang and Nan Li. “Privacy-Preserved Nonlinear Cloud-based Model Predictive Control via Affine Masking.” ArXiv abs/2112.10625 (2021): n. pag.
- Zhang, Lu, Luis Vega and Michael Bedford Taylor. “Power Side Channels in Security ICs: Hardware Countermeasures.” ArXiv abs/1605.00681 (2016): n. pag.
- Zhang, Minxing, Zhaochun Ren, Zihan Wang, Pengjie Ren, Zhumin Chen, Pengfei Hu and Yang Zhang. “Membership Inference Attacks Against Recommender Systems.” Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (2021): n. pag.
- Zhang, Shijie and Hongzhi Yin. “Comprehensive Privacy Analysis on Federated Recommender System against Attribute Inference Attacks.” ArXiv abs/2205.11857 (2022): n. pag.
- Zhang, Shijie, Hongzhi Yin, Tong Chen, Zi-Liang Huang, Li-zhen Cui and Xiangliang Zhang. “Graph Embedding for Recommendation against Attribute Inference Attacks.” Proceedings of the Web Conference 2021 (2021): n. pag.
- Zhang, Shuang, Liyao Xiang, Congcong Li, Yixuan Wang, Quanshi Zhang, Wei Wang and Bo-chen Li. “Learning to Prevent Leakage: Privacy-Preserving Inference in the Mobile Cloud.” (2019).
- Zhang, Shuang, Liyao Xiang, Xi Yu, Pengzhi Chu, Yingqi Chen, Chen Cen and Li Juan Wang. “Privacy-Preserving Federated Learning on Partitioned Attributes.” ArXiv abs/2104.14383 (2021): n. pag.
- Zhang, T. and Quanyan Zhu. “Differentially Private Collaborative Intrusion Detection Systems For VANETs.” ArXiv abs/2005.00703 (2020): n. pag.
- Zhang, Wanrong, Shruti Tople and Olga Ohrimenko. “Leakage of Dataset Properties in Multi-Party Machine Learning.” USENIX Security Symposium (2021).

- Zhang, Xiaoyu, Chao Chen, Yi Xie, Xiaofeng Chen, Jun Zhang and Yang Xiang. “Privacy Inference Attacks and Defenses in Cloud-based Deep Neural Network: A Survey.” ArXiv abs/2105.06300 (2021): n. pag.
- Zhang, Y., Ya Xiao, Md Mahir Asef Kabir, Danfeng Daphne Yao and Na Meng. “Example-Based Vulnerability Detection and Repair in Java Code.” 2022 IEEE/ACM 30th International Conference on Program Comprehension (ICPC) (2022): 190-201.
- Zhang, You, Ge Zhu and Zhiyao Duan. “A Probabilistic Fusion Framework for Spoofing Aware Speaker Verification.” The Speaker and Language Recognition Workshop (Odyssey 2022) (2022): n. pag.
- Zhang, Yu, Tao Gu and Xi Zhang. “MDLdroid: a ChainSGD-reduce Approach to Mobile Deep Learning for Personal Mobile Sensing.” 2020 19th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN) (2020): 73-84.
- Zhang, Yuheng, R. Jia, Hengzhi Pei, Wenxiao Wang, Bo Li and Dawn Xiaodong Song. “The Secret Revealer: Generative Model-Inversion Attacks Against Deep Neural Networks.” 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2020): 250-258.
- Zhang, Zaixi, Qi Liu, Zhenya Huang, Hao Wang, Chengqiang Lu, Chuanren Liu and Enhong Chen. “GraphMI: Extracting Private Graph Data from Graph Neural Networks.” IJCAI (2021).
- Zhang, Zhaoxi, Leo Yu Zhang, Xufei Zheng, Bilal Hussain Abbasi and Shengshan Hu. “Evaluating Membership Inference Through Adversarial Robustness.” ArXiv abs/2205.06986 (2022): n. pag.
- Zhang, Zhikun, Min Chen, Michael Backes, Yun Shen and Yang Zhang. “Inference Attacks Against Graph Neural Networks.” ArXiv abs/2110.02631 (2021): n. pag.
- Zhang, Zhi-Li, Jiahao Qi, Yueqiang Cheng, Shijie Jiang, Yiyang Lin, Yansong Gao, Surya Nepal and Yuexian Zou. “A Retrospective and Futurespective of Rowhammer Attacks and Defenses on DRAM.” ArXiv abs/2201.02986 (2022): n. pag.
- Zhang, Zhiwen, Hongjun Wang, Jiyuan Chen, Zipei Fan, Xuan Song and Ryosuke Shibasaki. “GOF-TTE: Generative Online Federated Learning Framework for Travel Time Estimation.” ArXivabs/2207.00838 (2022): n. pag.
- Zhao, Benjamin Zi Hao, Aviral Agrawal, Catisha Coburn, Hassan Jameel Asghar, Raghav Bhaskar, Mohamed Ali Kâafar, Darren Webb and Peter Dickinson. “On the (In)Feasibility of Attribute Inference Attacks on Machine Learning Models.” 2021 IEEE European Symposium on Security and Privacy (EuroS&P) (2021): 232-251.
- Zhao, Benjamin Zi Hao, Hassan Jameel Asghar, Raghav Bhaskar and Mohamed Ali Kâafar. “On Inferring Training Data Attributes in Machine Learning Models.” ArXiv abs/1908.10558 (2019): n. pag.
- Zhao, Benjamin Zi Hao, Mohamed Ali Kâafar and Nicolas Kourtellis. “Not one but many Tradeoffs: Privacy Vs. Utility in Differentially Private Machine Learning.” Proceedings of the 2020 ACM SIGSAC Conference on Cloud Computing Security Workshop (2020): n. pag.
- Zhao, Jiaojiao, Li Liu, Cees G. M. Snoek, J. Han and Ling Shao. “Pixel-level Semantics Guided Image Colorization.” BMVC (2018).
- Zhao, Kangfei, Yu Rong, Jeffrey Xu Yu, Junzhou Huang and Hao Zhang. “Graph Ordering: Towards the Optimal by Learning.” WISE (2021).

- Zhao, Zhiqun, Hengyou Wang, Hao Sun and Zhihai He. “Structure-Preserving Progressive Low-rank Image Completion for Defending Adversarial Attacks.” ArXiv abs/2103.02781 (2021): n. pag.
- Zheng, Tianyue, Zhe Chen, Chao Cai, Jun Luo and Xu Zhang. “V2iFi: in-Vehicle Vital Sign Monitoring via Compact RF Sensing.” Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. 4 (2020): 70:1-70:27.
- Zhou, Chunyi, Yansong Gao, Anmin Fu, Kai Chen, Zhiyang Dai, Zhi Zhang, Minhui Xue and Yuqing Zhang. “PPA: Preference Profiling Attack Against Federated Learning.” ArXiv abs/2202.04856 (2022): n. pag.
- Zhou, Dawei, Nannan Wang, Bo Han and Tongliang Liu. “Modeling Adversarial Noise for Adversarial Training.” ICML (2022).
- Zhou, Junhao, Yufei Chen, Chao Shen and Yang Zhang. “Property Inference Attacks Against GANs.” ArXiv abs/2111.07608 (2022): n. pag.
- Zhou, Lifeng, Vasileios Tzoumas, George J. Pappas and Pratap Tokekar. “Distributed Attack-Robust Submodular Maximization for Multi-Robot Planning.” 2020 IEEE International Conference on Robotics and Automation (ICRA) (2020): 2479-2485.
- Zhou, Man, Qian Wang, Jingxiao Yang, Qi Li, Feng Xiao, Zhibo Wang and Xiaofeng Chen. “PatternListener: Cracking Android Pattern Lock Using Acoustic Signals.” Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (2018): n. pag.
- Zhou, Man, Qian Wang, Qi Li, Peipei Jiang, Jingxiao Yang, Chao Shen, Cong Wang and Shouhong Ding. “Securing Face Liveness Detection Using Unforgeable Lip Motion Patterns.” ArXivabs/2106.08013 (2021): n. pag.
- Zhou, Mo and Vishal M. Patel. “On Trace of PGD-Like Adversarial Attacks.” ArXiv abs/2205.09586 (2022): n. pag.
- Zhou, Pei, Rahul Khanna, Bill Yuchen Lin, Daniel Ho, Jay Pujara and Xiang Ren. “RICA: Evaluating Robust Inference Capabilities Based on Commonsense Axioms.” EMNLP (2021).
- Zhou, Qi, Haipeng Chen, Yitao Zheng and Zhen Wang. “EvaLDA: Efficient Evasion Attacks Towards Latent Dirichlet Allocation.” AAAI (2021).
- Zhou, Wei, Yan Jia, Yao Yao, Lipeng Zhu, Le Guan, Yuhang Mao, Peng Liu and Yuqing Zhang. “Discovering and Understanding the Security Hazards in the Interactions between IoT Devices, Mobile Apps, and Clouds on Smart Home Platforms.” USENIX Security Symposium (2019).
- Zhu, R., Tao Shu and Huirong Fu. “Statistical Inference Attack Against PHY-layer Key Extraction and Countermeasures.” Wirel. Networks 27 (2021): 4853-4873.
- Zhu, Youxiang, Bang Tran, Xiaohui Liang, John A. Batsis and Robert M. Roth. “Towards Interpretability of Speech Pause in Dementia Detection using Adversarial Learning.” ICASSP(2022).
- Zhu, Yuankun, Yueqiang Cheng, Husheng Zhou and Yantao Lu. “Hermes Attack: Steal DNN Models with Lossless Inference Accuracy.” USENIX Security Symposium (2021).
- Zhuang, Jun and Mohammad al Hasan. “Deperturbation of Online Social Networks via Bayesian Label Transition.” (2020).
- Ziller, Alexander, Jonathan Passerat-Palmbach, Theo Ryffel, Dmitrii Usynin, Andrew Trask, Ionesio Junior, Jason V. Mancuso, Marcus R. Makowski, Daniel Rueckert, Rickmer F Braren and G. Kaissis. “Privacy-preserving medical image analysis.” ArXiv abs/2012.06354 (2020): n. pag.

- Zizzo, Giulio, Ambrish Rawat, Mathieu Sinn and Beat Buesser. “FAT: Federated Adversarial Training.” ArXiv abs/2012.01791 (2020): n. pag.
- Zou, Yang, Zhikun Zhang, Michael Backes and Yang Zhang. “Privacy Analysis of Deep Learning in the Wild: Membership Inference Attacks against Transfer Learning.” ArXiv abs/2009.04872 (2020): n. pag.
- Zuo, Pengfei, Yu Hua, Ling Liang, Xinfeng Xie, Xing Hu and Yuan Xie. “SEALing Neural Network Models in Secure Deep Learning Accelerators.” ArXiv abs/2008.03752 (2020): n. pag.

Chapter 6. *Conclusion*

This research investigated the foundations on which the whole European system is built, namely the GDPR and the FFDR, which introduced the main semantic difference between personal data and non-personal data. Specifically focusing on *further processing* in Big Data analysis systems in IoE environments, its aim was to question the semantic nature of data in the further uses of data and the consequent protection recognised for data subjects' rights. The investigation was carried out referring to two points of view that are considered to challenge the process of conciliate law with reality: the risk of deanonymisation/re-identification (allowing the turning of non-personal data - processed personal data - into personal data) and the right to erasure (*right to be forgotten*).

Scientific literature shows that the technological development of deanonymisation/re-identification techniques is growing remarkably, especially in some geographical areas which tend to invest more in such research.

Therefore, despite the fact that the GDPR is considered to be a gold standard in protecting data subjects, technological development certainly impacts on data subjects' rights, especially on the right to erasure *ex* art. 17 of the GDPR (*right to be forgotten*).

The two different perspectives, objective and subjective, investigated in the thesis confirm the above-mentioned impact. The objective one, questioning the extent of the protection granted by the two main data processing models recalled by the GDPR, namely, anonymisation and pseudonymisation, led to framing the limits of these models. Therefore, it demonstrates that anonymisation may represent a sufficient data protection model only in a few cases, but not necessarily for Big Data. Here, the diversity of the data consistently challenges the model and contextual evaluations are needed, in addition to a Data Protection Impact Assessment (DPIA), aimed at better empowering data processors and data controllers in the processing of anonymised data.

Contrarily, pseudonymisation seems to satisfy the need to grant better data protection, ensuring a better level of data anonymity compared to anonymisation. Such an approach seems to be validated and endorsed in the evolution of the legislation, namely the DGA. In line with this point, the subjective perspective confirmed the potential of granting better protection by relying on the proliferation of stakeholders' roles and responsibilities, also with the introduction of new neutral intermediaries.

However, considering the fact that the DGA pins specific roles and duties on these new public entity figures, this type of approach is limited to generating a data ecosystem solely dependent on the public sector orientations, thus it may represent a challenge for democracy. This situation may be exacerbated by the lack of specification concerning general interest in the

DGA and public interest in the GDPR, eventually leading to the concentration of data in the public sector challenging privacy and data protection of citizens. In this scenario, the right to erasure may evolve to a dead letter.

Moreover, the implementation of the DGA expected in the following months and implemented by Member States may generate the data subjection of some Member States in favour of others, in pooling data into the Data Spaces, thus justified by general interest and/or public interest.

In line with these considerations, it is considered that more work is required to control this possible drift. On one hand, improving the empirical research approach aimed at framing the new trends in the creation and evolution of data ecosystems. On the other hand, incentivising the establishment of legal entities aiming to represent data subject rights solely and uniquely, conjugate legal and technological knowledge in line with the technological development.

References

1. Nezami, Z., Zamanifar, K.: Internet of Things/Internet of Everything: Structure and Ingredients. IEEE Potentials. 38, 12–17 (2019). https://doi.org/10.1109/MPOT.2018.2855439.
2. Security, Privacy and Trust in the IoT Environment. Security, Privacy and Trust in the IoT Environment. (2019). https://doi.org/10.1007/978-3-030-18075-1.
3. Sollins, K.R.: IoT big data security and privacy versus innovation. IEEE Internet Things J. 6, 1628–1635 (2019). https://doi.org/10.1109/JIOT.2019.2898113.
4. Marjani, M., Nasaruddin, F., Gani, A., Karim, A., Hashem, I.A.T., Siddiqa, A., Yaqoob, I.: Big IoT Data Analytics: Architecture, Opportunities, and Open Research Challenges. IEEE Access. 5, 5247–5261 (2017). https://doi.org/10.1109/ACCESS.2017.2689040.
5. Raj, A., Prakash, S.: Internet of Everything: A survey based on Architecture, Issues and Challenges. 2018 5th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering, UPCON 2018. (2018). https://doi.org/10.1109/UPCON.2018.8596923.
6. Purtova, N.: From knowing by name to targeting: the meaning of identification under the GDPR. International Data Privacy Law. 12, 163–183 (2022). https://doi.org/10.1093/IDPL/IPAC013.
7. Finck, M., Pallas, F.: They Who Must Not Be Identified - Distinguishing Personal from Non-Personal Data Under the GDPR. International Data Privacy Law. (2020). https://doi.org/10.2139/SSRN.3462948.
8. Sweeney, L.: Simple demographics often identify people uniquely. Carnegie Mellon University, Data Privacy Working Paper 3. Pittsburgh 2000. (2000).
9. Sweeney Latanya: Dr. Latanya Sweeney's Home Page, http://latanyasweeney.org/, last accessed 2022/03/19.
10. Sweeney, L.: Confidentiality, Disclosure, and Data Access: Theory and Practical Applications for Statistical Agencies. In: Confidentiality, Disclosure, and Data Access: Theory and Practical Applications for Statistical Agencies (2001).

11. Sweeney, L.: Computational disclosure control: A Primer on Data Privacy Protection, (2001).

12. Liang, G., Weller, S.R., Luo, F., Zhao, J., Dong, Z.Y.: Distributed Blockchain-Based Data Protection Framework for Modern Power Systems Against Cyber Attacks. IEEE Trans Smart Grid. 10, 3162–3173 (2019). https://doi.org/10.1109/TSG.2018.2819663.

13. Yang, Q., Liu, Y., Cheng, Y., Kang, Y., Chen, T., Yu, H.: Federated Learning. Synthesis Lectures on Artificial Intelligence and Machine Learning. 13, 1–207 (2020). https://doi.org/10.2200/S00960ED2V01Y201910AIM043.

14. Bogetoft, P., Christensen, D.L., Damgård, I., Geisler, M., Jakobsen, T., Krøigaard, M., Nielsen, J.D., Nielsen, J.B., Nielsen, K., Pagter, J., Schwartzbach, M., Toft, T.: Secure multiparty computation goes live. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). pp. 325–343 (2009). https://doi.org/10.1007/978-3-642-03549-4_20.

15. Ohm, P.: Broken promises of privacy: Responding to the surprising failure of anonymization. UCLA Law Review. 57, (2010).

16. Cavoukian, A., Emam, K. el: Dispelling the Myths Surrounding Anonymization Remains a Strong Tool for Protecting Privacy. Information and Privacy Commissioner, Ontario, Canada. (2011).

17. Elliot, M., O'Hara, K., Raab, C., O'Keefe, C.M., Mackey, E., Dibben, C., Gowans, H., Purdam, K., McCullagh, K.: Functional anonymisation: Personal data and the data environment. Computer Law and Security Review. 34, 204–221 (2018). https://doi.org/10.1016/j.clsr.2018.02.001.

18. Narayanan, A., Huey, J., Felten, E.W.: A Precautionary Approach to Big Data Privacy. 357–385 (2016). https://doi.org/10.1007/978-94-017-7376-8_13.

19. Narayanan, A., Paskov, H., Gong, N.Z., Bethencourt, J., Stefanov, E., Shin, E.C.R., Song, D.: On the feasibility of internet-scale author identification. In: Proceedings - IEEE Symposium on Security and Privacy (2012). https://doi.org/10.1109/SP.2012.46.

20. Mosley, Mark, Michael H. Brackett, S.: DAMA guide to the data management body of knowledge." (2010). (2010).

21. Abraham, R., Schneider, J., vom Brocke, J.: Data governance: A conceptual framework, structured review, and research agenda. Int J Inf Manage. 49, 424–438 (2019). https://doi.org/10.1016/J.IJINFOMGT.2019.07.008.

22. Zygmuntowski, J.J., Zoboli, L., Nemitz, P.F.: Embedding european values in data governance: A case for public data commons. Internet Policy Review. 10, (2021). https://doi.org/10.14763/2021.3.1572.

23. Purtova, N.: The law of everything. Broad concept of personal data and future of EU data protection law. Law Innov Technol. (2018). https://doi.org/10.1080/17579961.2018.1452176.

24. Marchant, G., Tournas, L., Gutierrez, C.I.: Governing Emerging Technologies Through Soft Law: Lessons For Artificial Intelligence. Jurimetrics. 61, (2020).

25. Palmirani, M., Martoni, M.: Big data, data governance, and new vulnerabilities [Big data, governance dei dati e nuove vulnerabilità]. Not Polit. (2019).

26. Micheli, M.: Emerging models of data governance and the politics of data. (2020).

27. Micheli, M., Ponti, M., Craglia, M., Berti Suman, A.: Emerging models of data governance in the age of datafication, (2020). https://doi.org/10.1177/2053951720948087.

28. Mariniello, M.: A timid start for European Union data governance., https://go.gale.com/ps/i.do?p=AONE&sw=w&issn=&v=2.1&it=r&id=GALE%7CA643536962&sid=googleScholar&linkaccess=fulltext%0Ahttps://go.gale.com/ps/i.do?p=AONE&sw=w&issn=&v=2.1&it=r&id=GALE%7CA643536962&sid=googleScholar&linkaccess=abs, (2020).

29. Zygmuntowski, J.J., Zoboli, L., Nemitz, P.F.: Embedding european values in data governance: A case for public data commons. Internet Policy Review. 10, (2021). https://doi.org/10.14763/2021.3.1572.

30. Epstein L., Martin A. D.: An Introduction to Empirical Legal Research. Oxford University Press, London, United Kingdom (2014).

31. Narayanan, A., Shmatikov, V.: Robust de-anonymization of large sparse datasets. In: Proceedings - IEEE Symposium on Security and Privacy (2008). https://doi.org/10.1109/SP.2008.33.

32. de Montjoye, Y.A., Hidalgo, C.A., Verleysen, M., Blondel, V.D.: Unique in the Crowd: The privacy bounds of human mobility. Sci Rep. 3, (2013). https://doi.org/10.1038/srep01376.

33. Su, J., Shukla, A., Goel, S., Narayanan, A.: De-anonymizing web browsing data with social networks. In: 26th International World Wide Web Conference, WWW 2017 (2017). https://doi.org/10.1145/3038912.3052714.

34. Rocher, L., Hendrickx, J.M., de Montjoye, Y.A.: Estimating the success of re-identifications in incomplete datasets using generative models. Nat Commun. 10, (2019). https://doi.org/10.1038/s41467-019-10933-3.

35. Basalla, G.: The Evolution of Technology - George Basalla - Google Libri. Cambridge University Press (1988).

36. Hariri, R.H., Fredericks, E.M., Bowers, K.M.: Uncertainty in big data analytics: survey, opportunities, and challenges. https://doi.org/10.1186/s40537-019-0206-3.

37. Rouvroy, A.: Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence. Stud Ethics Law Technol. 2, no, 1–51 (2008).

38. Floridi, L.: The Fourth Revolution: How the Infosphere is Reshaping Human Reality. Oxford University Press (2014).

39. Iafrate, F.: A Journey from Big Data to Smart Data. Advances in Intelligent Systems and Computing. 261, 25–33 (2014). https://doi.org/10.1007/978-3-319-04313-5_3.

40. Lenk, A., Bonorden, L., Hellmanns, A., Roedder, N., Jaehnichen, S.: Towards a taxonomy of standards in smart data. Proceedings - 2015 IEEE International Conference on Big Data, IEEE Big Data 2015. 1749–1754 (2015). https://doi.org/10.1109/BIGDATA.2015.7363946.

41. A European strategy for data - Communication from teh Commission to the Parliament, the Council, the Council Committee and teh Committee of the Regions, (2021).

42. Mayer-Schönberger, Viktor., Cukier, Kenneth.: Big data a revolution that will transform how we live, work, and think. Houghton Mifflin Harcourt (2013).

43. Mejias, U.A., Couldry, N.: Datafication. Internet Policy Review. 8, (2019). https://doi.org/10.14763/2019.4.1428.

44. Westin, A.F.: Privacy And Freedom. Wash Lee Law Rev. 25, 3–4.

45. Miller, A.R. (Arthur R.: The assault on privacy : computers, data banks, and dossiers. New American Library (1972).

46. Burnham, D.: The Rise of the Computer State: The Chilling Account of The Computer's Threat to Society. Vintage Books (1984).

47. M.Regan, P.: Legislating Privacy:Technology,Social Values,and Public Policy. The University of North Carolina (1995).

48. Porter, T.M.: Trust in numbers : the pursuit of objectivity in science and public life. 310.

49. Nissenbaum, H.: Privacy in context : technology, policy, and the integrity of social life. Stanford Law Books (2010).

50. Tzanou, M.: Data Protection as a Fundamental Right Next to Privacy? 'Reconstructing' a Not so New Right by Maria Tzanou :: SSRN. International Data Privacy Law. 3, 88–99 (2013).

51. Mantelero, A.: The EU proposal for a general data protection regulation and the roots of the "right to be forgotten" (Computer Law and Security (2013) 29 (229-235)). Computer Law and Security Review. 29, 637 (2013). https://doi.org/10.1016/j.clsr.2013.06.002.

52. Bunn, A.: The curious case of the right to be forgotten. Computer Law & Security Review. 31, 336–350 (2015). https://doi.org/10.1016/J.CLSR.2015.03.006.

53. Lee, J.: What the Right to be Forgotten Means to Companies: Threat or Opportunity? Procedia Comput Sci. 91, 542–546 (2016). https://doi.org/10.1016/J.PROCS.2016.07.138.

54. Villaronga, E.F., Kieseberg, P., Li, T.: Humans forget, machines remember: Artificial intelligence and the Right to Be Forgotten. Computer Law & Security Review. 34, 304–313 (2018). https://doi.org/10.1016/J.CLSR.2017.08.007.

55. Politou, E., Michota, A., Alepis, E., Pocs, M., Patsakis, C.: Backups and the right to be forgotten in the GDPR: An uneasy relationship. Computer Law & Security Review. 34, 1247–1257 (2018). https://doi.org/10.1016/J.CLSR.2018.08.006.

56. Bansal, G., Nah, F.F.H.: Internet Privacy Concerns Revisited: Oversight from Surveillance and Right To Be Forgotten as New Dimensions. Information & Management. 59, 103618 (2022). https://doi.org/10.1016/J.IM.2022.103618.

57. Mayer-Schönberger, V.: Delete : The Virtue of Forgetting in the Digital Age. Princeton University Press (2011). https://doi.org/10.1080/10286632.2010.493215.

58. Gonzalez Fuster, G.: The Emergence of Personal Data Protection as a Fundamental Right of the EU - Gloria González Fuster - Google Libri. Springer (2014).

59. Mangini, V., Tal, I., Moldovan, A.-N.: An Empirical Study on the Impact of GDPR and Right to be Forgotten - Organisations and Users Perspective. Proceedings of the 15th International Conference on Availability, Reliability and Security. (2020). https://doi.org/10.1145/3407023.

60. Politou, E., Alepis, E., Virvou, M., Patsakis, C.: The "Right to Be Forgotten" in the GDPR: Implementation Challenges and Potential Solutions. In: Learning and Analytics in Intelligent Systems. pp. 41–68. Springer (2022). https://doi.org/10.1007/978-3-030-85443-0_4/COVER.

61. Tsai, C.W., Lai, C.F., Chao, H.C., Vasilakos, A. v.: Big data analytics: a survey. J Big Data. 2, 1–32 (2015). https://doi.org/10.1186/S40537-015-0030-3/TABLES/3.

62. Fisher, D., DeLine, R., Czerwinski, M., Drucker, S.: Interactions with big data analytics. Interactions. 19, 50–59 (2012). https://doi.org/10.1145/2168931.2168943.

63. Gellert, R., Gutwirth, S.: The legal construction of privacy and data protection. Computer Law & Security Review. 29, 522–530 (2013). https://doi.org/10.1016/J.CLSR.2013.07.005.

64. Tzanou, M.: Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right. International Data Privacy Law. 3, 88–99 (2013). https://doi.org/10.1093/IDPL/IPT004.

65. Gutwirth, S., de Hert, P.: Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power. Direito Público. 18, (2022). https://doi.org/10.11117/RDP.V18I100.6200.

66. Fuster, G.G., Gellert, R.: The fundamental right of data protection in the European Union: in search of an uncharted right. International Review of Law, Computers & Technology. 26, 73–82 (2012). https://doi.org/10.1080/13600869.2012.646798.

67. Rodotà, S.: Data Protection as a Fundamental Right. In: Gutwirth, S., Poullet, Y., de Hert, P., de Terwangne, C., and Nouwt, S. (eds) (eds.) Reinventing Data Protection? pp. 77–82. Springer, Dordrecht (2009). https://doi.org/10.1007/978-1-4020-9498-9_3.

68. Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J.-H., Metayer, D. le, Tirtea, R., Schiffner, S.: Privacy and Data Protection by Design - from policy to engineering. (2015). https://doi.org/10.2824/38623.

69. Zarsky, T.Z.: Incompatible: The GDPR in the Age of Big Data. Seton Hall Law Rev. 47, (2016).

70. Zarsky, T.Z.: Incompatible: The GDPR in the Age of Big Data. Seton Hall Law Rev. 47, (2016).

71. Lane, J.I.: Privacy, big data, and the public good : frameworks for engagement. (214)AD.

72. Nouwens, M., Liccardi, I., Veale, M., Karger, D., Kagal, L.: Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence. In: Conference on Human Factors in Computing Systems - Proceedings. Association for Computing Machinery (2020). https://doi.org/10.1145/3313831.3376321.

73. Politou, E., Alepis, E., Patsakis, C.: Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. J Cybersecur. 4, (2018). https://doi.org/10.1093/CYBSEC/TYY001.

74. Custers, B., Uršič, H.: Big data and data reuse: A taxonomy of data reuse for balancing big data benefits and personal data protection. International Data Privacy Law. 6, 4–15 (2016). https://doi.org/10.1093/IDPL/IPV028.

75. Ducato, R.: Data protection, scientific research, and the role of information. Computer Law & Security Review. 37, 105412 (2020). https://doi.org/10.1016/J.CLSR.2020.105412.

76. Peloquin, D., DiMaio, M., Bierer, B., Barnes, M.: Disruptive and avoidable: GDPR challenges to secondary research uses of data. European Journal of Human Genetics 2020 28:6. 28, 697–705 (2020). https://doi.org/10.1038/s41431-020-0596-x.

77. Biega, A.J., Finck, M.: Reviving Purpose Limitation and Data Minimisation in Data-Driven Systems. Technology and Regulation. (2021). https://doi.org/10.26116/techreg.2021.004.

78. OECD: Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies. OECD (2019). https://doi.org/10.1787/276AACA8-EN.

79. Meszaros, J., Ho, C. hsing: AI research and data protection: Can the same rules apply for commercial and academic research under the GDPR? Computer Law & Security Review. 41, 105532 (2021). https://doi.org/10.1016/J.CLSR.2021.105532.

80. Quinn, P.: Research under the GDPR – a level playing field for public and private sector research? Life Sci Soc Policy. 17, 1–33 (2021). https://doi.org/10.1186/S40504-021-00111-Z/METRICS.

81. Meszaros, J., Ho, C. hsing: AI research and data protection: Can the same rules apply for commercial and academic research under the GDPR? Computer Law & Security Review. 41, 105532 (2021). https://doi.org/10.1016/J.CLSR.2021.105532.

82. United Nations Statistical Commission and Economic Commission for Europe Conference of European Statisticians: Statistical Standards and Studies n. 53 Terminology on Statistical Metadata . , Geneva (2000).

83. Organisation for Economic Co-operation and Development, Organisation de Coopération et de Développement Economiques: OECD Glossary of Statistical Terms , https://stats.oecd.org/glossary/glossary.pdf, (2004).

84. Gray, J., Chaudhuri, S., Bosworth, A., Layman, A., Reichart, D., Venkatrao, M., Pellow, F., Pirahesh, H.: Data Cube: A Relational Aggregation Operator Generalizing Group-By, Cross-Tab, and Sub-Totals. Data Min Knowl Discov. 1, 29–53 (1997).

85. Fasolo, E., Rossi, M., Widmer, J., Zorzi, M.: In-network aggregation techniques for wireless sensor networks: A survey. IEEE Wirel Commun. 14, 70–87 (2007). https://doi.org/10.1109/MWC.2007.358967.

86. Iftikhar, N.: Integration, aggregation and exchange of farming device data: A high level perspective. Applications of Digital Information and Web Technologies, 2009. ICADIWT `09. Second International Conference on the. 2009, 14–19 (2009).

87. Cai, S., Gallina, B., Nyström, D., Seceleanu, C.: Data aggregation processes: a survey, a taxonomy, and design guidelines. Computing. 101, 1397–1429 (2019). https://doi.org/10.1007/S00607-018-0679-5/FIGURES/11.

88. Stalla-Bourdillon, S.: Aggregation, Synthesisation and Anonymisation - A Call For A Risk-Based Assessment of anonymisation Approaches. In: Hallinan, D., Leenes, R., and de Hert, P. (eds.) Data Protection and Privacy: Data Protection and Artificial Intelligence, CPDP 2021. Hart Publishing (2021). https://doi.org/10.5040/9781509941780.

89. Rubinstein, I.S., Good, N.: The trouble with Article 25 (and how to fix it): the future of data protection by design and default. International Data Privacy Law. 10, 37–56 (2020). https://doi.org/10.1093/IDPL/IPZ019.

90. Berman, J.J.: Identification, Deidentification, and Reidentification. In: Principles and Practice of Big Data. pp. 53–84. Academic Press (2018). https://doi.org/10.1016/B978-0-12-815609-4.00003-0.

91. Rubinstein, I.S., Hartzog, W.: Anonymization and risk. Washington Law Review. 91, (2016).

92. M. Schwartz, P., J. Solove, D.: The PII problem: privacy and a new concept of personal identifible information. New York University Law Review. (2011).

93. Narayanan, A., Shmatikov, V.: Myths and fallacies of "Personally Identifiable Information." Commun ACM. 53, 24–26 (2010). https://doi.org/10.1145/1743546.1743558.

94. Leenes, R.: Do you know me? – Deconstructing identifiability. University of Ottawa Law & Technology Journal. 4, (2008).

95. Galič, M., Gellert, R.: Data protection law beyond identifiability? Atmospheric profiles, nudging and the Stratumseind Living Lab. Computer Law and Security Review. 40, 105486 (2021). https://doi.org/10.1016/j.clsr.2020.105486.

96. Pfitzmann, A., Hansen, M.: A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management. (2010).

97. Galič, M., Gellert, R.: Data protection law beyond identifiability? Atmospheric profiles, nudging and the Stratumseind Living Lab. Computer Law and Security Review. 40, 105486 (2021). https://doi.org/10.1016/j.clsr.2020.105486.

98. Murthy, S., Abu Bakar, A., Abdul Rahim, F., Ramli, R.: A Comparative Study of Data Anonymization Techniques. In: 2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS). pp. 306–309. Institute of Electrical and Electronics Engineers Inc. (2019). https://doi.org/10.1109/BIGDATASECURITY-HPSC-IDS.2019.00063.

99. European Commission: Commission Staff Working Document Report on the stakeholder consultation and engagement activities Accompanying the document COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMM. (2022).

100. Narayanan, A., Shmatikov, V.: Myths and fallacies of personally identifiable information, (2010). https://doi.org/10.1145/1743546.1743558.

101. Pfitzmann, A., Hansen, M.: A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management. Technical University Dresden. (2010). https://doi.org/10.1.1.154.635.

102. Wing, J.M.: The Data Life Cycle. Harv Data Sci Rev. (2019). https://doi.org/10.1162/99608f92.e26845b4.

103. Abuosba, K.: Formalizing big data processing lifecycles: Acquisition, serialization, aggregation, analysis, mining, knowledge representation, and information dissemination. In: 2015 International Conference and Workshop on Computing and Communication, IEMCON 2015 (2015). https://doi.org/10.1109/IEMCON.2015.7344533.

104. Hu, R., Stalla-Bourdillon, S., Yang, M., Schiavo, V., Sassone, V.: Bridging Policy, Regulation and Practice? A techno-legal Analysis of Three Types of Data in the GDPR Runshan Hu, Sophie Stalla-Bourdillon, Mu Yang, Valeria Schiavo and Vladimiro Sassone. Data Protection and Privacy: The Age of Intelligent Machines. (2017).

105. Leenes Ronald, van Brakel Rosamunde, Gutwirth Serge, de Hert Paul: Data protection and privacy: The age of intelligent machines — Tilburg University Research Portal. Hart Publishing Ltd., Oxford (2017).

106. Finck, M., Pallas, F.: They who must not be identified—distinguishing personal from non-personal data under the GDPR. International Data Privacy Law. 10, (2020). https://doi.org/10.1093/idpl/ipz026.

107. Baloup, J., Bayamlıoğlu, E., Benmayor, A., Ducuing, C., Dutkiewicz, L., Lalova, T., Miadzvetskaya, Y., Peeters, B.: White Paper on the Data Governance Act. SSRN Electronic Journal. (2021). https://doi.org/10.2139/ssrn.3872703.

108. European Commission: Communication from the Commission to the European Parliament and the Council: Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union COM(2019) 250 final. 21 (2019).

109. Graef, I., Gellert, R., Husovec, M.: Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data is Counterproductive to Data Innovation. SSRN Electronic Journal. (2018). https://doi.org/10.2139/ssrn.3256189.

110. Stalla-Bourdillon, S., Knight, A.: Anonymous data v. personal data—a false debate: an EU perspective on anonymization, pseudonymization and personal data. Wisconsin International Law Journal. 34, (2017).

111. European Commission: Commission Staff Working Document - Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on a framework for the free-flow of non-personal data in the European Union COM(2017)304 final .

112. Rosenbaum, S.: Data governance and stewardship: Designing data stewardship entities and advancing data access. Health Serv Res. 45, 1442–1455 (2010). https://doi.org/10.1111/j.1475-6773.2010.01140.x.

113. ENISA, European Union Agency for Cybersecurity: Recommendations on shaping technology according to GDPR provisions - An overview on data pseudonymisation — ENISA. (2019).

114. Article 29 Working Party: Opinion 05/2014 on Anonymisation Techniques. Working Party Opinions. (2014).

115. ARTICLE 29 DATA PROTECTION WORKING PARTY Opinion 03/2013 on purpose limitation. (2013).

116. Zhu, L.: Privacy in Context: Technology, Policy, and the Integrity of Social Life. Journal of Information Privacy and Security. 7, (2011). https://doi.org/10.1080/15536548.2011.10855919.

117. O'hara, K.: Transparent Government, Not Transparent Citizens: A Report on Privacy and Transparency for the Cabinet Office.

118. Doyle, P.: Confidentiality, disclosure, and data access: Theory and practical applications for statistical agencies. Elsevier, Amsterdam (2001).

119. Yakowitz Bambauer, J.: Tragedy of the Data Commons. Harv J Law Technol. 25, (2011). https://doi.org/10.2139/SSRN.1789749.

120. Stevens, L.: The Proposed Data Protection Regulation and Its Potential Impact on Social Sciences Research in the UK. European Data Protection Law Review. (2017). https://doi.org/10.21552/edpl/2015/2/4.

121. Mourby, M., Mackey, E., Elliot, M., Gowans, H., Wallace, S.E., Bell, J., Smith, H., Aidinlis, S., Kaye, J.: Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK. Computer Law and Security Review. 34, (2018). https://doi.org/10.1016/j.clsr.2018.01.002.

122. Dwork, C.: The promise of differential privacy: A tutorial on algorithmic techniques. Proceedings - Annual IEEE Symposium on Foundations of Computer Science, FOCS. 1–2 (2011). https://doi.org/10.1109/FOCS.2011.88.

123. Dinur, I., Nissim, K.: Revealing Information while Preserving Privacy. In: Proceedings of the ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems (2003). https://doi.org/10.1145/773153.773173.

124. Domingo-Ferrer, J., Sánchez, D., Blanco-Justicia, A., Blanco, A.: The Limits of Differential Privacy (and its Misuse in Data Release and Machine Learning). Commun ACM. 64, 33–35 (2020). https://doi.org/10.48550/arxiv.2011.02352.

125. Samarati, P., Sweeney, L.: Protecting Privacy when Disclosing Information: k-Anonymity and Its Enforcement through Generalization and Suppression.

126. LeFevre, K., DeWitt, D.J., Ramakrishnan, R.: Incognito: efficient full-domain K-anonymity. In: SIGMOD Conference 2005. pp. 49–60 (2005). https://doi.org/10.1145/1066157.1066164.

127. Xu, J., Wang, W., Pei, J., Wang, X., Shi, B., Fu, A.W.C.: Utility-based anonymization using local recoding. Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. 2006, 785–790 (2006). https://doi.org/10.1145/1150402.1150504.

128. Machanavajjhala, A., Kifer, D., Gehrke, J., Venkitasubramaniam, M.: L-diversity. ACM Transactions on Knowledge Discovery from Data (TKDD). 1, (2007). https://doi.org/10.1145/1217299.1217302.

129. Ninghui, L., Tiancheng, L., Venkatasubramanian, S.: t-Closeness: Privacy beyond k-anonymity and ℓ-diversity. Proc Int Conf Data Eng. 106–115 (2007). https://doi.org/10.1109/ICDE.2007.367856.

130. Soria-Comas, J., Domingo-Ferrer, J.: Mitigating the Curse of Dimensionality in Data Anonymization.

131. Elliot, M., Mackey, E., O'Hara, K., Tudor, C.: The Anonymisation Decision-Making Framework. (2016). https://doi.org/10.1017/CBO9781107415324.004.

132. Elliot, M., Domingo-Ferrer, J.: The future of statistical disclosure control. A contributing article to the National Statistician's Quality Review into Privacy and Data Confidentiality Methods. , London (2018). https://doi.org/10.48550/arxiv.1812.09204.

133. Matthews, G.J., Harel, O.: Data confidentiality: A review of methods for statistical disclosure limitation and methods for assessing privacy. Statistic Surveys. 5, 1–29 (2011). https://doi.org/10.1214/11-SS074.

134. Sweeney, L.: Computational Disclosure Control: A Primer on Data Privacy Protection, (2001).

135. Rubinstein, I.S., Hartzog, W.: Anonymization and Risk. Washington Law Review. 91, 6–7.

136. Perera, C., Ranjan, R., Wang, L., Khan, S.U., Zomaya, A.Y.: Big data privacy in the internet of things era. IT Prof. 17, 32–39 (2015). https://doi.org/10.1109/MITP.2015.34.

137. Abraham, R., Schneider, J., vom Brocke, J.: Data governance: A conceptual framework, structured review, and research agenda. Int J Inf Manage. 49, 424–438 (2019). https://doi.org/10.1016/j.ijinfomgt.2019.07.008.

138. Raphaël Gellert, B., Graef, I.: TILEC Discussion Paper The European Commission's proposed Data Governance Act: some initial reflections on the increasingly complex EU regulatory puzzle of stimulating data sharing The European Commission's proposed Data Governance Act: some initial refle. (2021).

139. Leistner, M., Abraham, R., Schneider, J., vom Brocke, J., Micheli, M., Ponti, M., Craglia, M., Berti Suman, A., Mayer-Schönberger, V., Borgogno, O., Colangelo, G., Peukert, C., Bechtold, S., Batikas, M., Kretschmer, T., Shabani, M., Zygmuntowski, J.J., Zoboli, L., Nemitz, P.F., Jason, R., Cybersecurity, J.D., Report, P., May, N.Y., Kerber, W.: Regulatory Spillovers and Data Governance: Evidence from the GDPR. Int J Inf Manage. 35, 1–3 (2021). https://doi.org/10.1287/mksc.2021.1339.

140. Mayer-Schönberger, V.: Beyond privacy, beyond rights-toward a "systems" theory of information governance. Calif Law Rev. 98, 1853–1885 (2010).

141. Baloup, J., Bayamlıoğlu, E., Benmayor, A., Ducuing, C., Dutkiewicz, L., Lalova, T., Miadzvetskaya, Y., Peeters, B.: CiTiP Working Paper Series White Paper on the Data Governance Act White Paper on the Data Governance Act. (2021).

142. Leistner, M.: The Commission's vision for Europe's Digital Future: Proposals for the Data Governance Act, the Digital Markets Act and the Digital Services Act-A critical primer.

143. EDPB, EDPS: Statement 05/2021 on the Data Governance Act in light of the legislative developments. (2021).

144. EDPB, EDPS: Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act). (2021).

145. Graef, I., Gellert, R., Husovec, M.: Towards a holistic regulatory approach for the European data economy: Why the illusive notion of non-personal data is counterproductive to data innovation. Eur Law Rev. 44, 605–621 (2019). https://doi.org/10.2/JQUERY.MIN.JS.

146. Wendehorst, C.: Elephants in the Room and Paper Tigers: How to Reconcile Data Protection and the Data Economy. In: Trading Data in the Digital Economy: Legal Concepts and Tools. pp. 327–356. Nomos Verlagsgesellschaft mbH & Co. KG (2017). https://doi.org/10.5771/9783845288185-327.

147. Eltinge, J.L.: Disclosure Protection in the Context of Statistical Agency Operations: Data Quality and Related Constraints. Harv Data Sci Rev. (2022). https://doi.org/10.1162/99608F92.1CFAD278.

148. Bogetoft, P., Christensen, D.L., Damgård, I., Geisler, M., Jakobsen, T., Krøigaard, M., Nielsen, J.D., Nielsen, J.B., Nielsen, K., Pagter, J., Schwartzbach, M., Toft, T.: Secure multiparty computation goes live. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 5628 LNCS, 325–343 (2009). https://doi.org/10.1007/978-3-642-03549-4_20.

149. Bestavros, A., Lapets, A., Varia, M.: User-centric distributed solutions for privacy-preserving analytics. Commun ACM. 60, 37–39 (2017). https://doi.org/10.1145/3029603.

150. Agahari, W., Ofe, H., de Reuver, M.: It is not (only) about privacy: How multi-party computation redefines control, trust, and risk in data sharing. Electronic Markets. 1–26 (2022). https://doi.org/10.1007/S12525-022-00572-W/TABLES/2.

151. Ricciato F., Bujnowska A.: Privacy and data confidentiality for Official Statistics: new challenges and new tools. , Luxembourg (2021).

152. Zygmuntowski, J.J., Zoboli, L., Nemitz, P.F.: Embedding european values in data governance: A case for public data commons. Internet Policy Review. 10, (2021). https://doi.org/10.14763/2021.3.1572.

153. Shabani, M.: The Data Governance Act and the EU's move towards facilitating data sharing. Mol Syst Biol. 17, 1–3 (2021). https://doi.org/10.15252/msb.202110229.

154. Zygmuntowski, J.J., Zoboli, L., Nemitz, P.F.: Embedding european values in data governance: A case for public data commons. Internet Policy Review. 10, (2021). https://doi.org/10.14763/2021.3.1572.

155. Hafen, E.: Personal Data Cooperatives – A New Data Governance Framework for Data Donations and Precision Health. Philosophical Studies Series. 137, 141–149 (2019). https://doi.org/10.1007/978-3-030-04363-6_9.

156. O'Donell, G.A.: Delegative Democracy. Journal of Democracy. 5, 55–69 (1994).

157. Prainsack, B., Forgó, N.: Why paying individual people for their health data is a bad idea. Nature Medicine 2022 28:10. 28, 1989–1991 (2022). https://doi.org/10.1038/S41591-022-01955-4.

158. Slokenberga, S., Tzortzatou, O., Reichel, J.: Setting the Foundations: Individual Rights, Public Interest, Scientifc Research and Biobanking. In: GDPR and Biobanking: Individual Rights, Public Interest and Research Regulation across Europe. pp. 11–30. Springer International Publishing (2021).

159. Kotschy, W.: The proposal for a new General Data Protection Regulation-problems solved? International Data Privacy Law. 4, 274–281 (2014).

160. Samonte, M.: Google v. CNIL: The Territorial Scope of the Right to Be Forgotten Under EU Law. European Papers - A Journal on Law and Integration. 2019 4, 839–851 (2020). https://doi.org/10.15166/2499-8249/332.

Other relevant sources

Binjubeir M., Ahmed A.A., Ismail M.A.B., Sadiq A.S., Khurram Khan M., Comprehensive survey on big data privacy protection, IEEE Access, vol. 8, pp. 20067–20079, (2020).

Cai, S., Gallina, B., Nyström, D., Seceleanu, C., Data aggregation processes: a survey, a taxonomy, and design guidelines, in Computing (2019) 101:1397–1429.

Custer B., Ursic H., Big Data and Data Reuse: a Taxonomy of data reuse for balancing big data benefits and personal data protection, in International Data Privacy Law, 1-12, (2016).

De Filippi P., The Interplay between Decentralization and Privacy: The Case of Blockchain Technologies (September 14, 2016). Journal of Peer Production, Issue n.7: Alternative Internets, Available at SSRN: https://ssrn.com/abstract=2852689.

Domingo-Ferrer J., The limits of differential privacy (and its misuse in data release and machine learning), in Communications of the ACM 64(7): 33-35, (2021).

Domingo-Ferrer J., Personal Big Data, GDPR and Anonymization, in 13th International Conference, FQAS 2019, Amantea, Italy, July 2–5, 2019, Proceedings. 7-10, (2019).

Domingo-Ferrer J., Justicia A.B., Towards Machine Learning-Assisted Output Checking for Statistical Disclosure Control, in Towards Machine Learning-Assisted Output Checking for Statistical Disclosure Control. In: Torra V., Narukawa Y. (eds) Modeling Decisions for Artificial Intelligence. MDAI 2021. Lecture Notes in Computer Science, vol 12898. Springer (2021).

Domingo-Ferrer, J., Sánchez, D., Rufian-Torrell, G., Anonymization of nominal data based on semantic marginality. Information Sciences, 242, 35–48 (2013).

Elliot, M. J., Domingo Ferrer, J., The future of statistical disclosure control. Paper published as part of The National Statistician's Quality Review. London, December (2018).

Elliot, M., O'Hara, K., Raab, C., O'Keefe, C. M., Mackey, E., Dibben, C., Gowans, H., Purdam, K., & McCullagh, K., Functional anonymisation: Personal data and the data environment. Computer Law and Security Review, 34(2), 204-221, (2018).

Fasolo, E., Rossi, M., Widmer, J., Zorzi, M., In-network aggregation techniques for wireless sensor networks: a survey. IEEE Wirel Commun 14(2):70–87, (2007).

Fink M., Biega A., Reviving Purpose Limitation and Data Minimisation in Personalisation,

Profiling and Decision-Making Systems, Max Planck Institute for Innovation & Competition Research Paper No. 21-04, (2021).
Forgó, N., Hänold S., Schütze, B., The Principle of Purpose Limitation and Big Data, Perspectives in Law, Business, and Innovation, in: Marcelo Corrales & Mark Fenwick & Nikolaus Forgó (ed.), New Technology, Big Data and the Law, pages 17-42, (2017).
Garfinkel, S., Abowd, J.M., Martindale, C., Understanding Database Reconstruction Attacks on Public Data, in Communications of the ACM, Volume 62, Issue 3March 2019, pp 46–53 (2019).
Gray, J., Chaudhuri, S., Bosworth, A., Layman, A., Reichart, D., Venkatrao, M., Pellow, F., Pirahesh, H., Data cube: a relational aggregation operator generalizing group-by, cross-tab, and sub-totals. Data Mining Knowledge Discovery, 1(1):29–53, (1997).
Iftikhar, N., Integration, aggregation and exchange of farming device data: a high level perspective. In: Proceedings of the 2nd international conference on the applications of digital information and web technologies, pp 14–19, (2009).
Majeed A., Lee S., Anonymization Techniques for Privacy Preserving Data Publishing: A Comprehensive Survey, in IEEE Access, vol. 9, pp. 8512-8545, (2021).
Mantelero A., Esposito M.S., An evidence-based methodology for human rights impact assessment (HRIA) in the development of AI data-intensive systems, in The computer law and security report, 2021-07, Vol.41, p.105561, (2021).
Mehrabi, N., Morstatter, F., Saxena, N., Lerman, K., Galstyan, A., A Survey on Bias and Fairness in Machine Learning, in ArXiv (2019).
Meszaros J., and Chih-hsing, H., AI research and data protection: Can the same rules apply for commercial and academic research under the GDPR? In Computer Law & Security Review 41, 105532, (2021).
Nanni, M., Domingo-Ferrer, J., et al., Give more data, awareness and control to individual citizens, and they will help COVID-19 containment, in ArXiv (2020).
Quinn P., Research under the GDPR – a level playing field for public and private sector research? In Life Sciences, Society and Policy, 17(1), 4, (2021).
Rubinstein I.S., Good N., The trouble with Article 25 (and how to fix it): the future of data protection by design and default, in International Data Privacy Law, Volume 10, Issue 1, February 2020, Pages 37–56, (2020).
Schiffner S. et al., Towards a Roadmap for Privacy Technologies and the General Data Protection Regulation: A Transatlantic Initiative. In: Medina M., Mitrakas A., Rannenberg K., Schweighofer E., Tsouroulas N. (eds) Privacy Technologies and Policy. APF 2018. Lecture Notes in Computer Science, vol 11079. Springer, (2018).
Shah S.M., Khan R.A., Secondary Use of Electronic Health Record: Opportunities and Challenges, in IEEE Access (2020).
Sharma A., Singh G., Rehman S., A review of big data challenges and preserving privacy in big data, in Advances in Data and Information Sciences. Singapore: Springer, pp. 57–65, (2020).
Singh, R., Haasler, I., Zhang, Q., Karlsson, J., Chen, Y., Inference with Aggregate Data: An Optimal Transport Approach, in ArXiv (2020).
Skovgaard Lea L., Wadmann S., Hoeyer K., A review of attitudes towards the reuse of health data among people in the European Union: The primacy of purpose and the common good, in Health Policy, 123 (2019), 564-571.
Stalla-Bourdillon S., Rossi A., Aggregation, Synthesisation and Anonymisation - A Call For A Risk-Based Assessment of Anonymisation Approaches, in Data Protection and Privacy: Data Protection and Artificial Intelligence, CPDP Vol. 13, Hart Publishing

(2021).
Stalla-Bourdillon, S., A Maturity Spectrum for Data Institutions, in IEEE Security & Privacy, Volum 19, Issue 5, (2021).
Talat R., Obaidat M.S., Muzammal M., Sodhro A.H., Luo Z., Pirbhulal S., A decentralised approach to privacy preserving trajectory mining, in Future Gener. Comput. Syst., vol. 102, pp. 382–392, (2020).
Wang H., Wang X.A., Xiao S., Liu J., Decentralized data outsourcing auditing protocol based on blockchain, in J. Ambient Intell. Humanized Comput., pp. 1–12, (2020).