Alma Mater Studiorum – Università di Bologna
In collaborazione con LAST-JD consortium:
Università degli studi di Torino
Universitat Autonoma de Barcelona
Mykolas Romeris University
Tilburg University
e in cotutela con
Luxembourg University

DOTTORATO DI RICERCA IN

Erasmus Mundus Joint International Doctoral Degree in Law, Science and Technology

Ciclo 29 – A.Y. 2013/2014

Settore Concorsuale di afferenza: 12H3

Settore Scientifico disciplinare: IUS20

SLA Violation Detection Model and SLA Assured Service Brokering (SLaB) in Multi-Cloud Architecture

Presentata da: Shyam Sharan WAGLE

Coordinatore

Prof. Monica Palmirani

Relatore

Prof. Pascal Bouvry

Co- Relatore

Prof. Monica Palmirani

Esame finale anno 2017

Alma Mater Studiorum – Università di Bologna
in partnership with LAST-JD Consoritum
Università degli studi di Torino
Universitat Autonoma de Barcelona
Mykolas Romeris University
Tilburg University
and in cotutorship with the
University of Luxembourg

PhD Programme in

Erasmus Mundus Joint International Doctoral Degree in Law, Science and Technology
Cycle 29 – a.y. 2013/14

Settore Concorsuale di afferenza: 12H3

Settore Scientifico disciplinare: IUS20

SLA Violation Detection Model and SLA Assured Service Brokering (SLaB) in Multi-Cloud Architecture

Submitted by: Shyam Sharan WAGLE

The PhD Programme Coordinator
Prof. Monica Palmirani

Supervisor (s)

Prof. Pascal Bouvry
Prof. Monica Palmirani

Year 2017

UNIVERSITÉ DU LUXEMBOURG

PhD-FSTC-2017-01
The Faculty of Sciences, Technology and Communication

University of Bologna
Law School

DISSERTATION

Defence held on 31/01/2017 in Bologna
to obtain the degree of

DOCTEUR DE L'UNIVERSITÉ DU LUXEMBOURG EN INFORMATIQUE

AND

DOTTORE DI RICERCA in Law, Science and Technology

by

SHYAM SHARAN WAGLE
Born on 23rd September, 1982 in Syangja (Nepal)

SLA VIOLATION DETECTION MODEL AND SLA ASSURED SERVICE BROKERING (SLaB) IN MULTI-CLOUD ARCHITECTURE

Dissertation defence committee

Dr Pascal Bouvry, dissertation supervisor
Professor, Université du Luxembourg

Dr Monica Palmirani
Professor, Università degli Studi di Bologna

Dr El-Ghazali Talbi, Chairman
Professor, Professor at Polytech'Lille

Dr Jean-Marc Pierson
Professor, University Paul Sabatier

Dr Ivona Brandic, Vice Chairman
Professor, Vienna University of Technology

Alma Mater Studiorum Universita di Bologna

in partnership with LAST-JD Consoritum

Universit delgi studi di Turin

Universitat Autonoma de Barcelona

Mykolas Romeris University

Tilburg University

and in cotutorship with the

University of Luxembourg

PhD Programme in

Erasmus Mundus Joint International Doctoral Degree in Law, Science and Technology

Cycle 29 a.y. 2013/14

Settore Concorsuale di afferenza: 12H3

Settore Scientifico disciplinare: IUS20

SLA Violation Detection Model and SLA Assured Service Brokering (SLaB) in Multi-Cloud Architecture

Submitted By: **Shyam S. Wagle**

The PhD Programme Coordinator
Prof. Monica Palmirani

Supervisors:
Prof. Pascal Bouvry
Prof Monica Palmirani

January 2017

b

Acknowledgement

There are a number of people without whom this thesis work might not have been completed/written and to whom I would like to give my sincere thanks. First, I would like to express my deepest gratitude to my PhD supervisor Prof. Pascal Bouvry, Univerisity of Luxembourg who gave me the opportunity to pursue my PhD and for his constructive guidance/direction throughout this work, which showed me how research can be performed. I am very thankful to Prof. Raymond Bisdorff, University of Luxembourg for accepting me to work in his research team. He has provided me with constructive feedback during the research period and given me the support needed to pursue this work in performance evaluation. I am particularly grateful to Dr. Mateusz Guzek for his patience and continuous support towards my research work which helped to improve the quality of scientific research in this thesis.

I would like to thank Erasmus Mundus Law, Science and Technology PhD (LAST-JD) program for allowing me to pursue this research. I am specially thankful to Prof. Monica Palmirani, Director of LAST-JD program and Prof. Guido Boella, Vice-Director of LAST-JD program for their guidance and continuous support in every steps during my research period. I would like to thank Prof. Antoni Roig, IDT at Autonoma University of Autonoma Barcelona for his support during my stay in University of Autonoma Barcelona. I am also very thankful to IShOP (POLLUX/13/IS/6466384) project and Green@Cloud(INTER/ CNRS/11/03) project funded by National Research Fund (FNR), Luxemboug for financially supporting (partially) to perform this research.

Furthermore, I would like to thank the faculties and staff of University of Bologna and University of Turin, Italy, University of Autonoma Barcelona (UAB) Spain and University of Luxembourg, Luxembourg. I would like to express my deepest gratitude to Prof. Leon Ven Der Torre, Univerisity of Luxembourg for his unconditional support during my stay in Univerisity of Luxembourg.

I am deeply grateful to my family for supporting me during this long journey. My daughter was born in the middle of my PhD research. As she grew up, this thesis completed also. This thesis is dedicated to my lovely daughter. Last and most importantly, I would like to thank my beloved wife. I would not have been able to go through this without her support.

Shyam S. Wagle

September 2016, Luxembourg

Abstract

Cloud brokering facilitates Cloud Service Users (CSUs) to find cloud services according to their requirements. In the current practice, CSUs or Cloud Service Brokers (CSBs) select cloud services according to *Service Level Agreement* (SLA) committed by Cloud Service Providers (CSPs) in their website. In our observation, it is found that most of the CSPs do not fulfill the service commitment mentioned in the SLA agreement. Verified cloud service performances against their SLA commitment of CSPs provide an additional trust on CSBs to recommend services to the CSUs. In this thesis work, we propose a SLA assured service-brokering framework, which considers both committed and delivered SLA by CSPs in cloud service recommendation to the users.

For the evaluation of the performance of CSPs, two evaluation techniques: Heat Map and Intuinistic Fuzzy Logic (IFL) are proposed, which include both directly measurable and non-measurable parameters in the performance evaluation CSPs. These two techniques are implemented using real data measured from CSPs. Both performance evaluation techniques rank/-sort CSPs according to their service performances. The result shows that Heat Map technique is more transparent and consistent in CSP performance evaluation than IFL technique. As cloud computing is location independent technology, CSPs should respect the current regulatory framework in delivering services to the users. In this work, regulatory compliance status of the

CSPs is also analyzed and visualized in performance heat map table to provide legal status of CSPs. Moreover, missing points in their terms of service and SLA document are analyzed and recommended to add in the contract document. In the revised European data protection regulation (GPDR), data protection impact assessment (DPIA) is going to be mandatory for all organizations/tools. The decision recommendation tool developed using above mentioned evaluation techniques may cause potential harm to individuals in assessing data from multiple CSPs. So, DPIA is carried out to assess the potential harm/risks to individuals due to decision recommendation tool and necessary precaution to be taken in decision recommendation tool to minimize possible data privacy risks.

To help CSUs in easy decision making to select cloud services from multi-cloud environment, service pattern analysis techniques and prediction of future performance behavior of CSPs are also proposed in the thesis work. Prediction patterns and error measurement shows that automatic prediction methods can be implemented for short time period as well as longer time period.

Contents

List of Figures **xi**

List of Tables **xiv**

I Introduction **1**

1 Introduction **3**

1.1 Problem Statement 5

1.2 Research Questions 9

1.3 Scientific Contributions 11

1.4 List of Publications 14

1.5 Thesis Structure 16

2 Background **19**

2.1 Cloud Computing 19

2.1.1 Cloud IT Infrastructure Forecast 23

2.2 The NIST Cloud Reference Architecture 24

2.3 Multi-Cloud Computing 25

2.3.1 Use of Multi-Clouds 27

2.4 Cloud Computing Contracts 28

2.5 Service Level Agreement(SLA) 29

2.5.1 Cloud SLA Metrics . . . 30
2.5.1.1 Performance Service Level . . . 31
2.5.1.2 Security Service Level . . . 31
2.5.1.3 Data Management Service Level . . . 32
2.5.1.4 Personal Data Protection Service Level . . . 32
2.5.2 Detail Analysis of Performance Service Level . . . 33
2.5.3 SLA Standards . . . 35
2.5.3.1 SLA Standardization Initiatives . . . 36
2.6 Cloud Service Brokering . . . 37
2.7 Multi-Criteria Decision-Making(Multicriteria Decision Making (MCDM)) 39
2.8 Prediction Methods . . . 41
2.8.1 Exponential Smoothing . . . 42
2.8.2 Autoregressive Integrated Moving Average (ARIMA) . . . 42
2.9 Summary . . . 42

II Related Works 45

3 Related Works 47
3.1 SLA Monitoring/Measurement, Service Verification . . . 47
3.1.1 SLA Standarization . . . 48
3.1.2 SLA Monitoring/Measurement and Verification . . . 49
3.2 Service Evaluation and Service recommendation of cloud providers . . . 52
3.2.1 Cloud Service Provider Ranking . . . 52
3.2.2 Cloud Service Performance Analysis . . . 52
3.2.3 Multi-Cloud Architecture . . . 54
3.3 Performance Pattern Analysis and Performance Prediction . . . 57
3.4 Summary . . . 60

III Regulatory Issues in Cloud Computing **61**

4 Legal Issues and Service Commitments in Cloud Computing **63**

4.1 Cloud Contract and SLA . . . 63

4.2 Regulatory Issues from cloud computing contractual point of view . . . 66

4.2.1 Data Privacy . . . 66

4.2.2 Trans-boarder Data Flow . . . 67

4.2.3 Processor and Sub-processor Agreement . . . 68

4.2.4 Governing Laws and Jurisdiction . . . 69

4.2.5 Data Subject Rights . . . 69

4.3 Important Issues to be considered in Cloud Computing Contracts . . . 69

4.3.1 Liabilities . . . 69

4.3.2 Provider Lock-In and Exit . . . 70

4.3.3 Terms and Conditions . . . 70

4.3.4 Service Level Agreement(SLA) . . . 70

4.3.5 Changing Service Features . . . 71

4.3.6 Intellectual Property Rights (IPR) . . . 71

4.4 Summary . . . 71

IV Design Implementation and Evaluation **73**

5 Design and Implementation **75**

5.1 Overall Implementation Framework . . . 75

5.2 Cloud Performance Monitoring Framework . . . 80

5.2.1 SLA Commitment Verification . . . 80

5.3 Service Performance Ranking and Evaluation . . . 81

5.3.1 Experiment Setup for Service recommendation and CSP Ranking 82

5.4 General Overview of Cloud User's Request and Relations with Stakeholders 83

5.4.1 Cloud Users 83
5.4.2 Cloud Broker 83
5.5 Summary 85

6 Cloud Service Provider Ranking/Sorting Algorithm 87
6.1 Intuinistic Fuzzy Logic (IFL) Concept 87
6.1.1 Algorithm 88
6.1.2 Cloud Service Ranking Algorithm 89
6.1.2.1 Interpretation of Auditors' Measurement in IFS 91
6.1.2.2 Ranking/Sorting 92
6.2 Performance Heat Map Table 93
6.2.1 CSP Selection aiding Approach 93
6.2.1.1 Sorting marginal performances into quantile classes . . 94
6.2.1.2 *q-tiles* Sorting on a Single Criteria 94
6.2.1.3 Multi-Criteria Extension 95
6.2.1.4 Interpretation of Auditors' Measurement in Heat Map . 95
6.3 Summary 96

7 Evaluation 97
7.1 Experiment Setup for Service recommendation and CSP Ranking 97
7.1.1 Performance Evaluation by IFL Technique 100
7.1.2 Performance Evaluation by Heat Map Technique 100
7.1.3 Multi-Criteria Ranking of the CSPs 108
7.2 Service Verification 109
7.3 Comparisons of Two Techniques 111
7.3.1 Result Analysis 114
7.4 Experiment Setup for Pattern Analysis of CSPs 116
7.5 Prediction Methods and Prediction Accuracy 118

7.5.1 Exponential Smoothing 118
7.5.2 Autoregressive integrated moving average(ARIMA) 119
7.5.3 Prediction Accuracy 119
7.5.3.1 Scale-dependent measures 119
7.5.3.2 Measures based on percentage errors 120
7.5.3.3 Scaled errors 120
7.5.3.4 Information Criteria(IC) 121
7.6 Performance Measurement 122
7.6.1 Performance Pattern Analysis 144
7.7 Service Performance Prediction 144
7.8 Errors Measurement and Prediction Accuracy 155
7.8.1 Matching predicted performances with actual measurement . . . 155
7.8.2 Conclusions 156
7.9 Summary 157

V Regulatory Compliance Analysis of Cloud Providers 159

8 Cloud Service Providers' Regulatory Compliance Analysis 161
8.1 Analysis of Term of Services and SLA committed by Cloud Service Providers 161
8.1.1 Terms of service and SLA provided by International Cloud Providers 162
8.2 Legal and/or Major Missing Points in the Current Cloud Contracts Offered by Cloud Providers 168
8.2.1 Pictorial Analysis of Cloud Provider's Contracts in HeatMap Table 170
8.2.2 Concluding Remarks 172
8.3 Data Protection Impact Assessment (DPIA) 173
8.3.1 Privacy Risk Indicators 174

8.3.2 Major Risks and Precautions to be Performed 174
8.4 Summary 176

VI Concluding Remarks 181

9 Conclusion and Future Works 183
9.1 Summary 183
9.2 Experimental Constraints 187
9.3 Research Challenges and Future Works 188

A Published Works 191

B Scripts for Performance Evaluator Using Heat Map 193
B.1 Performance Evaluator implementation 193

List of Figures

1.1 Structure of Thesis and Scientific Contributions 16

2.1 Cloud Computing delivery and deployment(right) models 21
2.2 Worldwide Cloud Computing IT Infrastructure Market Forecast by Deployment Type 2014-2019 [80] 23
2.3 NIST Cloud Reference Architecture 26
2.4 Multi-Cloud/Inter-Cloud Architecture 26
2.5 Resasons of Use of Multi-Cloud 28
2.6 SLA Metrics in Cloud Computing 31
2.7 Cloud Service Brokering 38
2.8 MCDM process 40

5.1 SLA based brokering and Service Verification Framework 76
5.2 Extracting the status from CSP's premises 81
5.3 CSP Performance Measurement Model 82
5.4 Service Request from different Cloud Users 84
5.5 Cloud Broker Relation with Cloud Users and Cloud Service Providers . 84
5.6 Cloud Service Auditor/Verifier 85

7.1 CSP Performance Measurement Model 99
7.2 Heat map table by Auditor 1 104

7.3 Heat map table by Auditor 2 110
7.4 Heat map table by All Auditors 110
7.5 Monthly Service Performance/Deviation Pattern of Amazon-S3 Cloud . 123
7.6 Monthly Service Performance/Deviation Pattern of GMO Cloud 124
7.7 Monthly Service Performance/Deviation Pattern of City Cloud 125
7.8 Monthly Service Performance/Deviation Pattern of Digital Cloud 126
7.9 Monthly Service Performance/Deviation Pattern of Elastic Host Cloud . 127
7.10 Monthly Service Performance/Deviation Pattern of Microsoftazure . . . 128
7.11 Monthly Service Performance/Deviation Pattern of Google 129
7.12 Monthly Service Performance/Deviation Pattern of Cloudsigma 130
7.13 Monthly Service Performance/Deviation Pattern of Gogrid 131
7.14 Monthly Service Performance/Deviation Pattern of Rackspace 132
7.15 Monthly Service Performance/Deviation Pattern of Centurylink 134
7.16 Monthly Service Performance/Deviation Pattern of Upcloud 135
7.17 Monthly Service Performance/Deviation Pattern of Softlayer 136
7.18 Monthly Service Performance/Deviation Pattern of IBM 137
7.19 Monthly Service Performance/Deviation Pattern of HP 138
7.20 Monthly Service Performance/Deviation Pattern of Exoscale 139
7.21 Monthly Service Performance/Deviation Pattern of Cloudcentral 140
7.22 Monthly Service Performance/Deviation Pattern of Aruba 141
7.23 Monthly Service Performance/Deviation Pattern of Baremetal 142
7.24 Monthly Service Performance/Deviation Pattern of VaultNetwork 143
7.25 Monthly Service Performance Pattern of Digital Cloud 145
7.26 Monthly Service Performance Pattern of Exoscale Cloud 146
7.27 Service Performance Prediction of Digital Cloud using ETS 148
7.28 Service Performance Prediction of Digital Cloud using ARIMA 149
7.29 Service Performance Prediction of Exoscale Cloud using ARIMA 150

7.30 Service Performance Prediction of Exoscale Cloud using ETS 152
7.31 Errors comparisions in ARIMA and ETS prediction method of ME, MAE, RMSE, MPE, ACF1and MASE 153
7.32 Errors comparisions in in ARIMA and ETS prediction method of MAPE, AIC, BIC, AICc 154

List of Tables

2.1 Top 10 reasons for using multiple cloud 27

2.2 Funtional Parameter Mapping to SLA Parameter 33

6.1 Linguistic terms for the Importance of a Criteria and Performance Rating 92

6.2 Ordinal Level and Interpretation of auditor measurement in Ordinal Value 96

7.1 Criteria and Subcriteria for evaluating cloud services 98

7.2 Internet connection between Local Test Environment and Cloud Providers 98

7.3 Service Measurement by $CloudAuditor_1$ 101

7.4 Service Measurement by $CloudAuditor_2$ 102

7.5 The ratings of importance weight of each criteria by decision makers . . 103

7.6 Performance Matrix 103

7.7 Decision Matrix $Z(CSP_i)$ 104

7.8 Scoring Value for CSP based on SLA Paramters $S_{W(C_j)}$ 104

7.9 Service Measurement by $CloudAuditor_2$ 105

7.10 Service Mapping to ordinal value measurement by $CloudAuditor_1$ . . . 106

7.11 Service Mapping to ordinal value measurement by $CloudAuditor_2$ . . . 107

7.12 Performance Evaluation by $CloudAuditor_1$ 112

7.13 Performance Evaluation by $CloudAuditor_2$ 112

7.14 Performance Evaluation by $User_1$ 113

7.15 Performance Evaluation by $User_2$ 113
7.16 Performance Evaluation by all Auditors 113
7.17 Performance Evaluation of All Auditors and Users 114
7.18 Notation for Monthly Performance Measurement from CSPs' Premises . 122
7.19 Errors Measurement in Performance Prediction of Digital Cloud 151
7.20 Errors Measurement in Performance Prediction of Exoscale Cloud . . . 151

8.1 Criteria and sub-criteria for evaluating cloud services 163
8.2 SLA offered by International Cloud Providers 177
8.3 Pictorial View of Cloud Contracts offered by International Cloud Service Providers 178
8.4 Answers of DPIA Screening Questions 178
8.5 Answers of DPIA Questions 179

Part I

Introduction

Chapter 1

Introduction

In the recent years, Cloud Computing (CC) is introduced as a novel computing paradigm that offers computing facilities as a service [111], [38]. A specific feature of cloud computing, in comparison with other computing paradigm such as grid computing [58], is that it allows the provision of on-demand, scalable storage resources and customized computing environments, using a pay-as-you-go pricing model. Increasing number of Cloud User/Customers (CUs) of Cloud Service Provider (CSP) makes more complex to handle all the services for the cloud service providers. However, outsourcing of duties and infrastructure to external parties minimizes the extra burden of the cloud providers in some extent. Cloud users requirements are different according to their nature of business but it is very difficult to get services exactly according to their requirement from single cloud service provider [136]. Generally, cloud service providers are focused on specific cloud services such as IaaS, PaaS and SaaS. So, it is not possible to fulfill all the expectations of each customer of different categories. User prefers some features of one cloud service provider and some features of another cloud service provider.

In this context, it is necessary to develop a framework, which considers the cloud users' requirements, the cloud service provider's commitments and verification of these commitments by an independent 3rd party mediator. All this in order to recommend services to the cloud users. At the same time, it is also important to assess the regulatory compliance of the provided services according to the current regulatory framework [55], [67].

Several organizations and bodies ([61], [95]) designed a cloud brokering architecture in order to deal with the interactions between users and providers in a inter-cloud environment [26]. It mediates multiple cloud providers by integrating, aggregating and customizing their services. Inter-cloud computing architecture allows users to easily transfer the cloud users application workloads via clouds irrespective of cloud service provider platform. Cloud service broker identifies the suitable cloud service provider by satisfying the cloud user's service needs. Architecture for cloud service broker is proposed to operate in inter-cloud environment. Cloud service brokers are also defined as trusted advisors who make possible business deal [133].

In this thesis, we investigate service performance and regulatory compliance status of the cloud providers. In particular, firstly, we measure the service performance of the cloud provider to check the SLA compliance against the SLA commitment in their website to the users. To evaluate the service performance status, we propose two algorithms and compare each other in terms of their feasibility in cloud brokering architecture. Secondly, we analyze the regulatory compliance status of cloud providers according to the terms and conditions mentioned in a cloud contract document. We also implement proposed most efficient algorithm, Heat Map Technique, for evaluating the service performance of cloud provider to evaluate the regulatory compliance status of the cloud provider. To shortly introduce the work carried out in this thesis, in Section 1.1, we present the problem statement, detailing the motivation for this work. In Section 1.2, we present the research questions that will be addressed in this thesis. Major scientific contributions of the thesis are summarized in Section 1.3. Finally, in Section 1.5, we present the organization of the remainder of the thesis.

1.1 Problem Statement

Cloud computing has recently emerged as a promising technology for IT industry. Due to the fast emerging cloud computing market over the last several years, the number of cloud providers has significantly increased. Requirements of the CUs are different according to the nature of business and usage. SLA agreement and terms of service in cloud computing help CUs to easily enter into cloud environment. At the same time CUs face many problems because of unclear terms and conditions or unbalanced terms and conditions, which are sometimes in the favor of cloud providers. Cloud contract may not follow the existing regulations and contract law [47]; in other words, it is not mandatory to fully adopt contract law in cloud computing contract [46]. Most of the big international cloud service providers offer terms of service including Service Level Agreement (SLA) in their website. In practice, there are two contracting models in cloud computing: 1) Online agreement; 2) Standard, negotiated and signature based agreement [35]. *Online-based agreement* is the most commonly followed model by cloud providers, where cloud users do not have any bargaining power to negotiate the standard agreement offered by cloud providers. The *standard, negotiated, signature based agreement*, which generally occurs when larger companies want to move their critical data or applications to the cloud (for instance, to the public cloud). In such agreement, cloud users are free to push their terms and conditions as well as requirements according to them in the contract document.

With the increasing number of CSPs, selecting an appropriate CSP according to their requirements is a complex and tedious job for the cloud users [138]. In the current practice, SLA and terms and conditions committed by CSPs are considered to select an appropriate CSP. In reality, it is seen that all the cloud provider may not fully comply the service performance commitments mentioned in their contract document [136]. If a cloud provider does not meet the committed service offer, cloud users are eligible to receive a Service Credit [134]. The service credit is a credit calculated as a percentage of the total charges paid by the cloud user. The received compensation may however be negligible compared to the losses caused by the insufficient QoS. In many cases, cloud providers offer similar or identical characteristics of services such as service availability, reliability, performance and so on, but they exhibit differences in terms of price, quality of service, service delivery and customer experience. In cloud computing, there is not a standardized format nor terminology [63] for cloud contract, and do not abide by any precise definition, notwithstanding some recent attempts [17] towards standardization. So, it always adds extra burden to cloud users and cloud brokers for selecting cloud services from appropriate cloud providers [70], [132].

A cloud brokering architecture [61], [95] in order to deal with the interactions between users and providers in a inter-cloud environment [26] can help users to find appropriate services but service performance verification against the commitments of CSPs [134], [136] and awareness with current regulatory compliance [127],[41] are still missing in the current cloud brokering architecture. In this section, we identify the major the problems in cloud service brokering as an independent 3rd party cloud service recommender from legal and technical perspective.

Problem 1:

Due to the recently emerged technology, there is not a standardized format nor terminology for cloud contract [63] in cloud computing except some recent attempts [17] towards standardization. Moreover, recent cloud service brokering architecture is not aware of current legal/regulatory compliance check [127],[41] to recommend services to cloud users.

Cloud service contract (agreement) offered by CSPs should be fair and transparent to both parties. Cloud users are not yet convinced with current practiced standard Terms of service provided in Cloud contracts. However cloud contract documents have neither standardized format nor terminology [63], and do not abide by any precise definition, notwithstanding some recent attempts [17] towards standardization[1], terms and conditioned mentioned in the contract document should be clear and transparent between both agreed parties. Contract document offered by majority of the cloud provider do not follow the existing regulations and contract law [47]. In most of the cases, Cloud Service User/Customers (CSUs) should be relied on SLA to search appropriate service search but there is not a standard cloud SLA template in cloud computing. Majority of the cloud providers offer monthly uptime in percentage as the main Quality of Service (QoS) indicator, which is an advantage for cloud provider because of missing standard SLA template in cloud computing.

Cloud service brokering framework can play and important role in law/regulation compliance management of cloud services [41]. However, current cloud service brokering framework only consider the service performance commitments of the CSPs to recommend services to the users [37], [36], [59], [82], [40], [131], [19], [56], [113], [22] and some recently proposed brokering frameworks to consider legal/regulatory compliance check [41] are in preliminary phase and do not consider service performance status together with legal/regulatory compliance of CSPs.

Problem 2:

Lack of verification of delivered service performance against the committed SLA by cloud providers to the CSPs.

In practice, cloud providers commit various service performance indicators in SLA document. SLA document is the main source either for cloud service users to select services according to their preference or for cloud service broker to recommend services to the end users [37]. In reality, it is seen that all the cloud provider may not fully comply the service performance commitments mentioned in their SLA [136]. In such situation, cloud service end users may not receive appropriate service according to their expectation. Real status/log of service delivery of CSPs monitored [4] by unbiased and

[1] https://ec.europa.eu/digital-single-market/en/news/cloud-service-level-agreement-standardisation-guidelines

independent 3rd party auditor/verifier may help cloud users or service broker to decide the appropriate cloud service of CSP according to their requirements.

Problem 3:

Due to lack of efficient 3rd party mechanism to collect service performance status of CSPs to choose the cloud services from multiple cloud service providers [83], cloud users should follow the complex manual searching method to decide the cloud services

It is not possible to get cloud services from single cloud provider exactly according to the cloud users preferences because of different nature of business need of cloud users. To select appropriate services from multiple cloud providers, cloud users should access their individual website to choose the services according to their preferences [83]. It consumes extra time and money of the cloud users. Various cloud services collected from different cloud provider may be expensive to the cloud users [136]. There are few cloud brokering parties, which mediate between cloud users and cloud providers [56], [113], [22], but these cloud brokering framework only considers the committed SLA by cloud providers and do not consider delivered service performance of cloud providers [134].

Problem 4:

Lack of recommendation model, which consider all the perspectives of CSPs to select the cloud services from multi-cloud environment

As mentioned in Problem 3, in the current cloud brokering framework, Cloud Service Brokers (CSBs), only consider the service committed in the SLA document of the cloud service providers [56], [113], [22], but do not consider the actual service delivered service performance of the cloud service providers in recommending cloud services to the cloud service users. In addition of this, as service performance of cloud provider is dynamic in nature, it is also necessary to have past, current and future service delivery pattern of cloud provider to judge the appropriate cloud providers. This information (past, current and future service delivery pattern) of CSP add extra confidence to the users to select services from multiple cloud providers [90], [65], [42], [96],[144], [149], [145],

[146], [110], [125], [39].

1.2 Research Questions

The main research question of the thesis is how proposed framework, SLA Assured Service Brokering (SLaB), ensures to the cloud users to select the cloud services according to their requirements with optimal set of available solutions from multi-cloud environment. This section describes our research questions raised in problem section 1.1.

Research Question 1:

What are the legal issues to be considered by Cloud Service Provider and Cloud Service Broker to provide cloud services as a public cloud provider according to the current legal framework and how SLA attributes can be defined to monitor or to select appropriate cloud services in multi-cloud environment?

Under this research question, we do provide answers of the following questions: 1) What are the major missing points in the current cloud contracts offered by majority of the cloud providers? CSPs and CSBs should respect the legal issues according to the current legal framework to provide cloud services as a public cloud service provider, 2) How can SLA attributes be defined to monitor/select service performance (including functional parameters and non-functional parameters) of the cloud providers?, and 4) How can regulatory compliance issues be considered by CSBs during recommendation of cloud servicesof particular cloud provider to the users ? These research questions address Problem 1.

Research Question 2:

How can Cloud Auditor/Verifier framework be designed to resolve the conflict between cloud service provider and cloud users ?

The real status/log of service performance delivery pattern of cloud provider may resolve the conflict between provider and users in case of SLA violation. It has two objectives: 1) it ensures that cloud providers are delivering services according to the committed SLA in their contract document, and 2) overall result of the auditor/verifier affects the position of the cloud provider in recommending cloud services to the end users. In particular, the module, auditor/verifier, provides a status/log report of service performance delivery of cloud providers, which will be acceptable for all the stakeholders of the cloud architecture as an independent 3rd party auditor. This report will be also applicable for penalty calculation under the eligibility of "service credit" mentioned in the SLA agreement of cloud provider. This research question addresses the Problem 2.

Research Question 3:

How can new approach be implemented in cloud service brokering framework, which considers both committed and delivered SLA of CSPs to recommend cloud services to the cloud users?

CSB intermediates cloud users and multiple cloud providers to provide the cloud services according to the users' requirements. To do so, CSB should collect the following information; service preference of CSUs, service performance commitment of CSP mentioned in SLA document and monitored real data of delivered service performance record of cloud providers. In service recommendation, the framework should be able to consider both functional and non-functional SLA parameters/attributes. Generally, measurement of non-functional SLA parameter can be covered by user feedback. So, there should be a common mechanism to receive the user feedback so that both measurable and non-measurable parameters can be considered to sort/rank CSPs according to their service performance commitment and delivery to the cloud users. This research question addresses the Problem 3.

Research Question 4:

How can SLA Assured service brokering framework be designed to recommend optimal set of solutions to the cloud users realizing a dynamic nature of service performance *behavior of CSPs?*

Since the dynamic nature of service performance behavior of cloud providers, it is a vital to consider past, present and future service performance behavior of the cloud providers. In the current cloud service brokering framework, CSB only considers committed SLA by CSPs. So, critical question under this research question is how can past, present and future service performance behavior of the cloud providers be considered in SLA assured service brokering framework to recommend services to the users. This research question addresses the problem raised in Problem 4.

1.3 Scientific Contributions

In this section, we highlight our scientific contributions to the research on SLA Violation Detection Model and SLA Assured Service Brokering (SLaB) in Multi-Cloud Architecture, thereby concretely answering the research questions addressed in the section 1.2. As our first contribution, we analyze the contract document provided by cloud service providers and identify some missing points according to the current legal framework, which is very important to make cloud contract safe and fair to both parties. To make legal/regulatory compliance aware SLA Assured Service Brokering, Heat Map technique is implemented, which is the most efficient performance evaluation technique to evaluate the service performance of the CSPs. With the European General Data Protection Regulation (GDPR) there will be a legal obligation to companies/projects to conduct a Data Protection Impact Assessement (DPIA) to analyze the data privacy risk due to establishment of companies/projects. We also analyse the possible major data privacy risks due to our proposed decision recommendation tool and identified necessary precautions to be taken to minimize the possible data privacy risks due to the decision recomendation tool [119]. An independent 3rd party cloud auditor/verifier is designed to monitor service performance of the cloud service providers and to check the compliance against the service performance commitment in the SLA document of cloud service provider as a second contribution [138], [132]. We propose two-service performance evaluation technique to evaluate the service performance of the cloud service providers as a third contribution [134], [136]. These two evaluation techniques are further compare with each other for the feasibility check to implement as the best performance evaluation technique in the cloud brokering framework [137]. Our final contribution is to identify the current and future service performance behavior of the cloud providers. This information is vital for CSBs due to dynamic nature of service performance behavior of cloud providers [135]. Overall, the following contributions have been achieved:

Contribution 1:

Defining SLA Metrics to monitor/select CSPs including both measurable and non-measurable parameters, and regulatory compliance status analysis of international cloud providers to enhance the provision of legal/regulatory compliance check in current cloud service brokering framework

Most of the incumbent international cloud providers offers the terms of service and SLA agreement in their website. Terms of service and SLA commitments committed by cloud providers are analyzed and important issues to be included in the proposed contract document are proposed to make fair, acceptable and transparent service commitment of CSPs from the regulatory perspective [119]. The method proposed to evaluate the service performance of cloud providers has been also implemented to check and analyze the regulatory compliance status of the cloud providers. The main source of these information is information provided in manifests including documents related to terms of service, Service Level Agreements (SLAs), security practices, privacy policies, the cloud documentations on getting started and other user guides and FAQs by cloud service providers. It helps cloud broker to recommend cloud services to the service users considering service performance status and regulatory compliance status of the cloud providers. Moreover, SLA attributes are also defined to include measurable and non-measurable parameters to monitor/select CSPs [134], [132]. This contribution addresses the Research Question 1.

Contribution 2:

An independent 3rd party cloud auditor/verifier framework design

The designed cloud auditor/verifier framework acts as an independent 3rd party, which collects the real status of the services delivered by cloud providers premises, and compares against the service performance committed in their SLA document [138], [119], [132]. Based on the service performance data obtained by service monitoring, cloud auditor/verifier verifies the service performance against SLA commitment or not. Non-verified service performances of cloud providers are subjected to penalty calculation according to the terms and conditions mentioned in SLA agreement [136]. This contribution addresses the research question raised in Research Question 2.

Contribution 3:

CSP Sorting/Ranking and Evaluation Module

The proposed cloud service provider sorting/ranking module provides the sorting/ranking of the CSPs based on their service performance delivery [134] according to the SLA commitment to the cloud users. It provides the sorting/ranking order considering functional and non-functional parameters of cloud service monitoring. In decision making, directly monitored data is used as a functional parameters and cloud users feedback is used to cover the non-functional requirements of the cloud users. For the evaluation, two evaluation techniques: Heat Map [136] and IFL [134] techniques are proposed and compared with each other for the adaptability in the cloud brokering framework [137]. In the overall evaluation, Heat Map technique returned more convincing result than the IFL technique. This contribution addresses the Research Question 3 presented in the previous section.

Contribution 4:

Service performance pattern analysis and prediction of future behavior of CSPs to recommend cloud services to the cloud users according to their preference

The objective of this work is to provide an optimal set of solutions of the cloud services to the users considering service performance, (past and future service performance behavior), price of the services, and regulatory compliance status of the cloud providers. In this contribution, we extracted the service delivery pattern of commercially available cloud providers and predicted the future service performance behavior of those cloud providers using appropriate forecasting techniques. Past, current and future service performance pattern of CSPs help cloud users in decision making to select appropriate cloud services. Similarly, cloud service broker can take advantage of those information of service performance pattern to recommend cloud services to the users. In this thesis, we could collect service delivery pattern of only 20 commercially avalable cloud providers [135]. In large number of alternatives, highly optimized methods can be implemented to provide optimal set of solutions including price of the cloud services. This contribution addresses the Research Question 4.

1.4 List of Publications

1. Shyam S. Wagle, Mateusz Guzek, Pascal Bouvry, and Raymond Bisdorff. Comparisons of Heat Map and IFL Technique to Evaluate the Performance of Commercially Available Cloud Providers. In IEEE 9th International Conference on Cloud Computing, pages —–, San Francisco, USA, June 2016(to appear).

2. Shyam S. Wagle, Mateusz Guzek and Pascal Bouvry. Service Performance Pattern Analysis and Prediction of Commercially Available Cloud Providers. In IEEE 8th International Conference on Cloud Computing (CloudCom), pages —, Luxembourg City, Luxembourg, December 2016(to appear).

3. Shyam S. Wagle, Mateusz Guzek, Pascal Bouvry, and Raymond Bisdorff. An

evaluation model for selecting cloud services from commercially available cloud providers. In IEEE 7th International Conference on Cloud Computing (CloudCom), pages 107 114, Vancouver, Canada, November 2015.

4. Wagle, S. S., Guzek, M., and Bouvry, P. Cloud service providers ranking based on service delivery and consumer experience. In 2015 IEEE 4th International Conference on Cloud Networking (CloudNet) (CLOUDNET'15), pages 202-205, Niagara Falls, Canada.

5. Shyam S. Wagle, "Cloud Service Optimization Method for Multi-Cloud Brokering", IEEE International Conference on Cloud Computing for Emerging Markets(CCEM), Banglore, India, November 2015

6. Shyam S. Wagle, "Optimized SLA Assured Service Brokering (SLaB) and Service Verification in Multi-Cloud Environment ", Workshop on Mathematical and Engineering Methods in Computer Science, Telc, Czech Republic, October 2015.

7. Shyam S. Wagle, "SLA Assured Brokering (SAB) and CSP Certification in Cloud Computing", IEEE/ACM 7th International Conference on Utility and Cloud Computing (UCC), London, United Kingdom, 2014.

8. Shyam S. Wagle, " Cloud Computing Contracts Regulatory Issues and Cloud Providers Offer: An Analysis", IFIP conference on Privacy and Identity Management for the Future Internet in the Age of Globalization, Karlstad, Sweden, 2016.

9. Shyam S. Wagle, "Regulatory Challenges in Cloud Computing in VM Migration outside EEA", IFIP conference on Privacy and Identity Management for the Future Internet in the Age of Globalization, Patras, Greece, 2014.

10. Shyam S. Wagle "Security Framework for VM Migration in Cloud Computing"

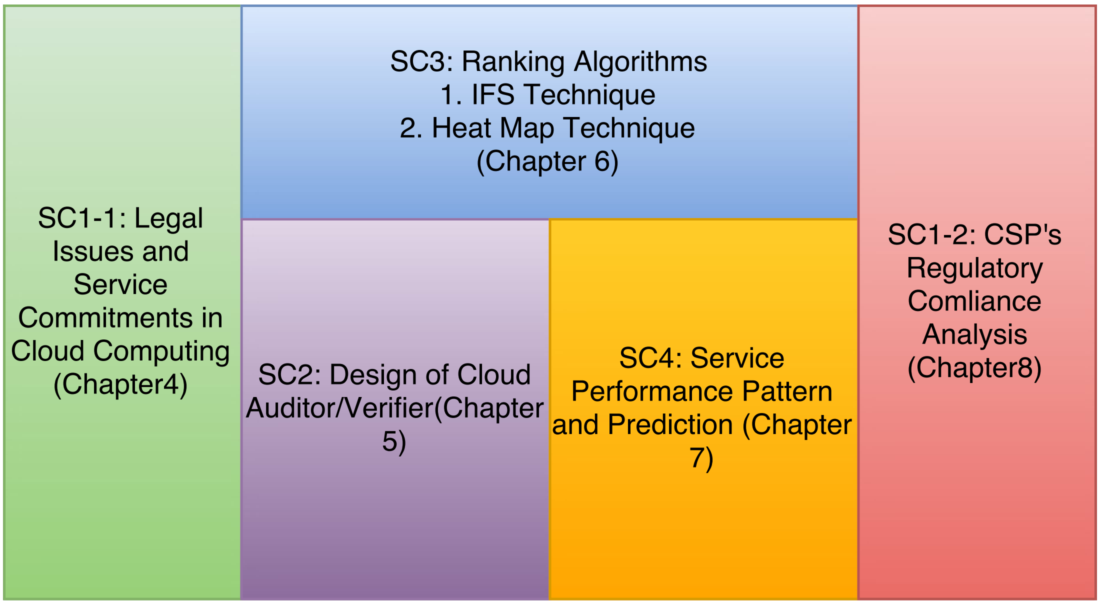


Figure 1.1: Structure of Thesis and Scientific Contributions

IFIP conference on Privacy and Identity Management for the Future Internet in the Age of Globalization, Patras, Greece, 2014.

1.5 Thesis Structure

Figure 1.1 presents the structure of the thesis from scientific contribution perspective. SC1-1: General overview of legal issues in cloud according current legal framework are presented in Chapter 4 and SC1-2: regulatory compliance status of some international cloud providers and DPIA of proposed decision recommendation tool are presented in Chapter 8. SC2: Design of cloud auditor/verifier, SC3: ranking/sorting algorithm and SC4: Service performance analysis with future behavior prediction are presented in Chapter 5, Chapter 6 and Chapter 7 respectively. The overall outline of the entire thesis work is structured as follows:

Chapter 2 presents the background information relevant to the research conducted within the thesis work. It gives overview of cloud computing including multi-cloud architecture. Then, a brief introduction of cloud computing contracts and Service Level Agreement SLA committed by cloud providers are presented. Some theoretical background of cloud brokering concepts, multi-criteria decision-making is also included in this chapter.

Chapter 3 presents the related works addressed in this work. It provides comparisons of their contributions and our contributions in the proposed scientific contributions in the chapter 2. Related Works are divided in three sections: 1) Legal issues, Cloud contract and SLA standardization; 2) Cloud Service Measurement/Monitoring, Verification; and 3) Service Evaluation, Recommendation for cloud users and cloud brokers and performance characteristics analysis of commercially available cloud providers

Chapter 4 presents the contractual terms committed by commercially available cloud providers. Regulatory issues to be considered by CSPs in the service commitments and analysis of current limitations of commitments committed by commercially available cloud providers are briefly analyzed in this chapter.

Chapter 5 presents the design and implementation of proposed service performance monitoring, verification and evaluation of multiple cloud providers. It provides the performance monitoring using commercially available cloud providers.

Chapter 6 presents the algorithms implemented to evaluate the performance of cloud providers. For the performance evaluation we used two approaches: IFL technique and Heat Map Technique.

Chapter 7 presents the verification of performance measurement according to service level commitments of cloud providers. Then, it provides the performance evaluation using IFL and Heat Map technique and comparisons of both techniques from the implementation aspect by cloud brokers. This chapter also provides the service performance delivery pattern of the cloud providers with future behavior of the service performance of the cloud providers.

Chapter 8 presents the compliance status of the cloud providers in their terms of service and SLA document from the legal perspective as mentioned in chapter 4. This chapter also provides the Data Protection Impact Assessment (DPIA) of proposed decision recommendation tool.

Chapter 9 concludes the summary of the thesis including experimental constraints and future research directions.

Chapter 2

Background

This chapter describes the background information on essential concepts necessary for the understanding of the research presented in this thesis. We first present in Sections 2.1 and 2.3 the concepts of Cloud and multi-cloud computing. In Sections 2.4 and 2.5 , we provide the current issues in cloud contracts and current SLA standardization approaches. Then, we discuss in Section 2.6 the concepts of cloud service brokering, on which the thesis contributions presented in Chapter 2 are based. After that, we define in Section 2.7 about the multi-criteria decision making approach, which is one of the contribution of the thesis to evaluate the performance of CSPs based on multiple criteria performances. Finally, Section 2.8 gives a short introduction to prediction methods, on which basis our future prediction of performance of cloud providers are predicted.

2.1 Cloud Computing

Cloud computing is a on-demand internet based computing, where shared resources, data and information are provided to computers and other devices on-demand. It extends the resource-sharing concept recently used in utility and grid computing with a business model, where resources are provisioned as services to customers. Based on the web services [78] and virtualization technology, cloud computing provides on-demand customized computing environments with a simple access interface to private and enterprise users. It is hard to define cloud computing using single sentence. We refer to the National Institute of Standards and Technology (NIST) [95] definition to define the cloud computing:

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

The NIST Definition of cloud computing lists five essential characteristics of cloud computing. It is reasonable to assume that missing any one of these essential characteristics means a service or computing capability cannot be considered as cloud computing:

- *On-demand self-service*: An automatic ubiquitous access over the Internet to the resources.
- *Broad network access*: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms.
- *Resource pooling*:A multi-tenant access to shared resources
- *Rapid elasticity*: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
- *Measured service*: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the

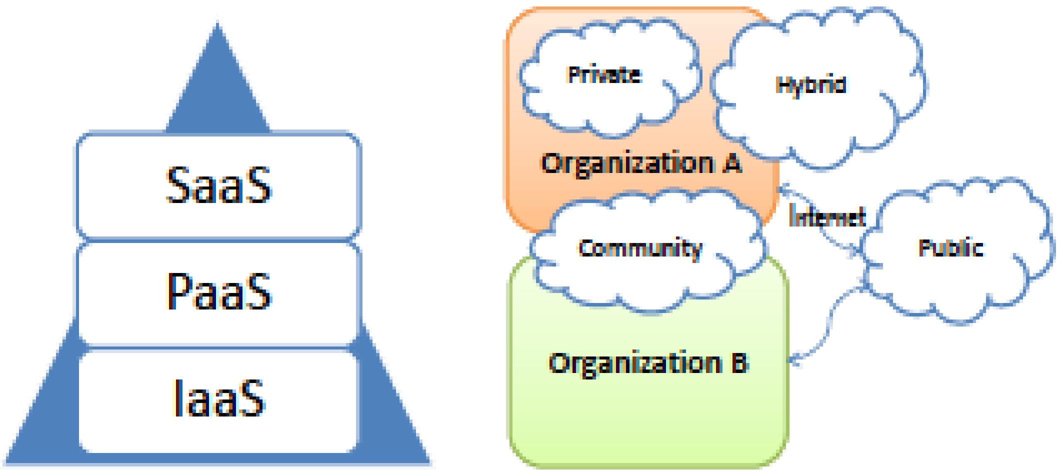


Figure 2.1: Cloud Computing delivery and deployment(right) models

type of service (e.g., storage, processing, bandwidth, and active user accounts). Typically this is done on a pay-per-use or charge-per-use basis. Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

- *On-demand access*: An automatic ubiquitous access over the Internet to the resources.

- *Pay-per-use*: The requested resources are charged only when used.

As shown in Figure 2.1, according to the NIST definition, Cloud services are classified into three delivery models:

- *Infrastructure as a Service (IaaS)* Provides customers with on-demand computational resources in the form of Virtual Machine (VM), storage or network. Customers can install operating systems and software packages on the machines to establish their own computing environments.

- *Platform as a Service(PaaS)* Provides users an entire hosting environment to develop their applications. The customer uses the environment without control over the operating system, hardware, or network infrastructure on which they are running. Examples of PaaS featured clouds are the Google App Engine [66] and Microsoft Azure [92].

- *Software as a Service (SaaS)* provides the customers a functionality of using the providers applications that run centrally on its Cloud in the form of web services. The applications are accessible from various client devices through a thin client interface. A well-known example of SaaS is Google Doc [106], which provides a platform to produce and work with on-line documents.

Furthermore, as depicted on the right side of Figure 2.1, the NIST definition identifies four possible Cloud deployment models:

- *Public Cloud*: provides on-demand services via the Internet to the general public.
- *Private Cloud*: provides services restricted to the organization that owns and manages the infrastructure.
- *Community Cloud*: provides services to a group of organizations that have shared interests.
- *Hybrid Cloud*: provides services owned by public and private Clouds.

The understanding about Cloud computing has become more comprehensive since Amazon published its Elastic Compute Services (EC2) [92] in 2006, the first worldwide commercial computing Cloud, and its storage Cloud - the Simple Storage System (S3) [**?**]to allow users to rent a server and store data on Amazons hosted computing and storage infrastructures. In addition, many commercial and research institutions are developing middleware stacks to build IaaS Clouds. Examples include Eucalyptus [97], Zimory [150], OpenNebula [107], Nimbus [94] and Openstack [108].

As previously mentioned in Chapter 1, this work focuses on cloud services offered by public IaaS Clouds. Nevertheless, the developed concepts and approaches can be easily propagated to PaaS and SaaS Clouds. Throughout this thesis, we refer to IaaS by the Cloud provider or the Cloud unless otherwise specified.

2.1.1 Cloud IT Infrastructure Forecast

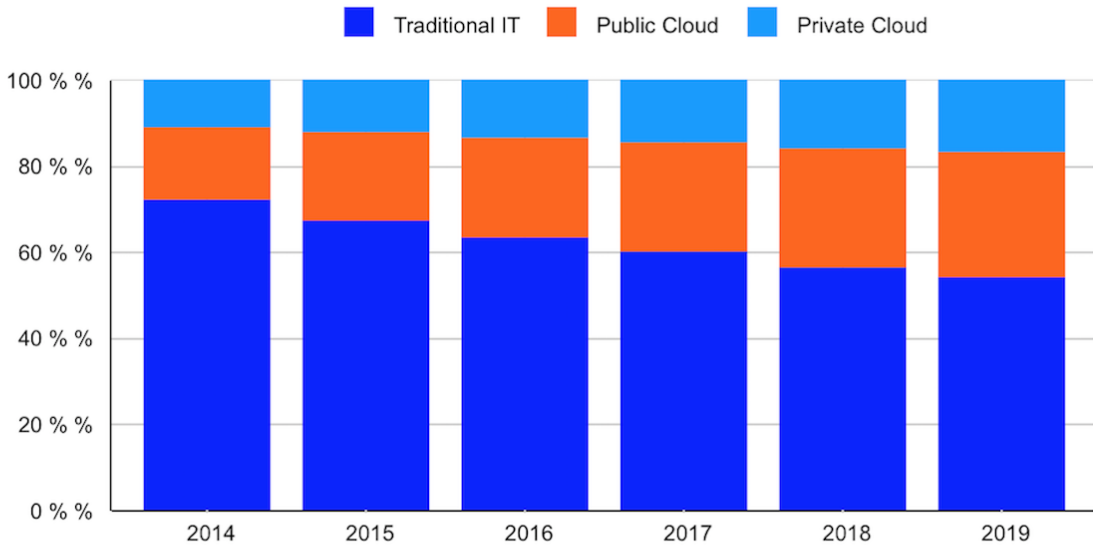


Figure 2.2: Worldwide Cloud Computing IT Infrastructure Market Forecast by Deployment Type 2014-2019 [80]

Total spending on cloud IT infrastructure, for the five-year forecast period, International Data Corporation (IDC) [80] expects that cloud IT infrastructure spending will grow at a compound annual growth rate (CAGR) of 15.1% and will reach \$53.1 billion by 2019 accounting for 46% of the total spending on enterprise IT infrastructure. At the same time, spending on non-cloud IT infrastructure will decline at -1.7% CAGR. Spending on public cloud IT infrastructure will grow at a higher rate than spending on private cloud IT infrastructure at 16.3% Vs 13.2% CAGR. In 2019, IDC expects service providers will spend \$33.6 billion on IT infrastructure for delivering public cloud services, while spending on private cloud IT infrastructure will reach $19.4 billion.

2.2 The NIST Cloud Reference Architecture

The NIST cloud reference architecture consists of five major actors (See Figure 2.3) and three types of cloud services [121]. Each actor performs a set of assigned tasks and interacts with other actors to provide, maintain, and manage cloud services.

- *Cloud Service User*:

  The cloud service user represents an individual or organization that can request services from one or more cloud service providers using a cloud broker as intermediary. The architecture supports three types of users consistent with the three types of services.

  - SaaS users request applications
  - PaaS users develop, test, deploy, and manage applications hosted in the cloud
  - IaaS users install, manage and monitor services

- *Cloud Service Provider*: The cloud service provider represents an organization responsible for making a service available to cloud service users. A cloud service provider sets up SLAs with cloud carriers and cloud service users:

  - Deploying the cloud infrastructure in one of four models: private, public, hybrid or community
  - Managing the cloud infrastructure: coordinating and managing VMs, virtual data storage, hypervisors, hardware resources and service applications and supporting network managing tools

  - managing cloud services: supporting external interfaces and client applications to help manage accounts, users, contracts, inventory and SLA and supporting provisioning, metering, migration, portability and security
  - Managing the network by configuration, accounting, performance and security management

- *Cloud Service Broker*: The cloud service broker represents an individual or organization that manages the use, performance and secured delivery of cloud services to users. It negotiates relationships between cloud providers and cloud service users and can customize services based on users requirements. Figure 2.3 illustrates high-level interactions between the major actors in the NIST framework. The communication between cloud broker and cloud service user is optional. So, this communication is represented by dashed line.

- *Cloud Auditor*: The cloud auditor represents an individual or organization that performs independent assessments of the cloud provider's services, information systems operations, performance and security on behalf of the cloud service users.

- *Cloud Carrier*: The cloud carrier represents an organization that provides an access network to the cloud infrastructure for hardware and storage devices. It also ensures consistent SLAs for cloud service offerings.

2.3 Multi-Cloud Computing

Inter-cloud [26] is a recently introduced vision of globally interconnected Clouds (Cloud of Clouds), much like the Internet as a network of networks. This vision addresses interoperability across Clouds, focusing on the use of open Cloud standards. Hereby, Cloud consumers should be able to freely choose and effortlessly switch between different Clouds. On the other hand, providers should be able to distribute their load

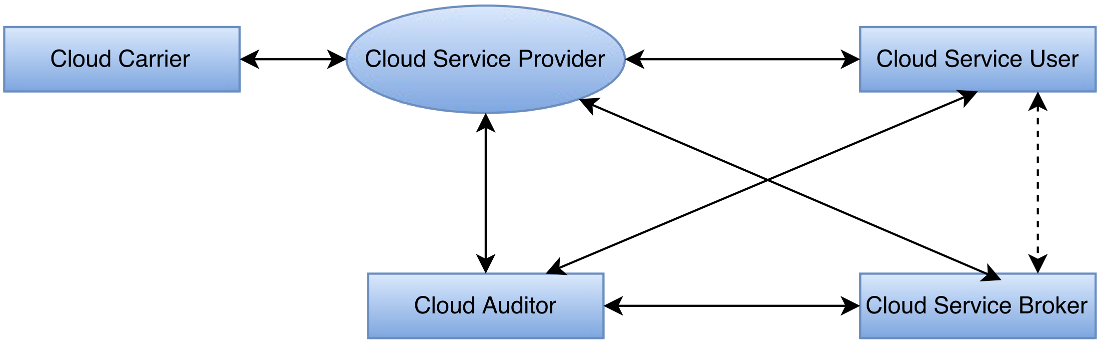


Figure 2.3: NIST Cloud Reference Architecture

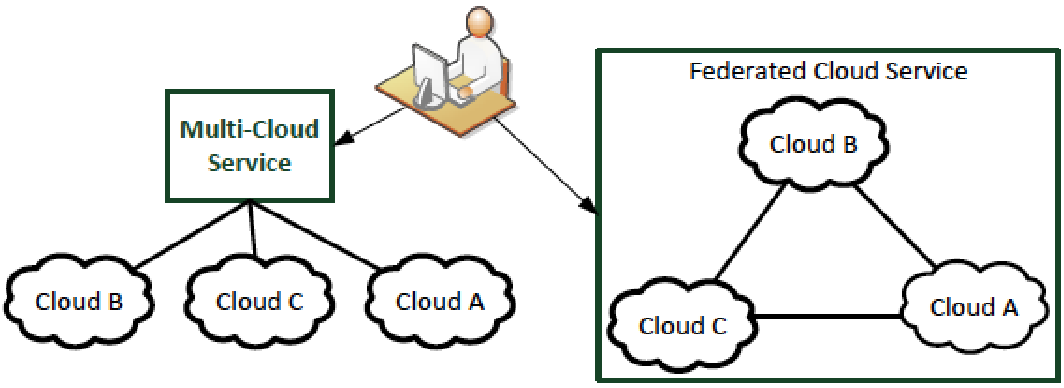


Figure 2.4: Multi-Cloud/Inter-Cloud Architecture

among geographically distributed datacenters in case of workload spikes or outages in order to meet the availability agreed upon with their customers [130]. The common future use cases and functional requirements for Inter-cloud computing are published in a white paper by the Global Inter-Cloud Technology Forum (GICTF) [64], which is an initiative started to foster the development of Inter-cloud technologies in industry and academia.

Based on the strength of the relation between the participating Clouds in an Inter-cloud environment, we distinguish between two usage scenarios: multi-Cloud and federated Clouds. While in the former the Clouds are used independently of one another,

Table 2.1: Top 10 reasons for using multiple cloud

Type of use	Reason
Serial usage	Optimize cost or improved quality of service React to the changes of the offers by the providers Follow the constraints, like new locations or law Avoid the dependence on only one external provider Ensure back-ups to deal with disasters or scheduled inactivity
Simultaneous usage	Deal with the peaks in service and resource requests using external ones, on demand basis Replicate applications/services consuming services from different clouds to ensure their availability Act as intermediary Enhance own cloud resource and service offers, based on agreement with the other providers Consume different services for their particularities not provided anywhere

in the latter case the Clouds establish agreements with each other in order to use the resources of the other Cloud [139]. An example of a Cloud middleware supporting Cloud federations is RESERVOIR [118]. The main difference between a multi-Cloud and a federated Cloud architecture is illustrated in Figure 2.4. In this thesis we address multi-Cloud environments formed by independent public Clouds. However, many of the proposed concepts can easily be adapted to federated Clouds.

2.3.1 Use of Multi-Clouds

Use of multi cloud helps to consume resources and services from different cloud providers. Table 2.1 and Figure 2.5 provides the use of multiple cloud from different stakeholder's perspective. D. Petcu [112] has pointed out top 10 reasons for multiple cloud from four cloud stakeholders' perspectives: cloud user, cloud provider, cloud broker, cloud application developer (See Figure 2.5).

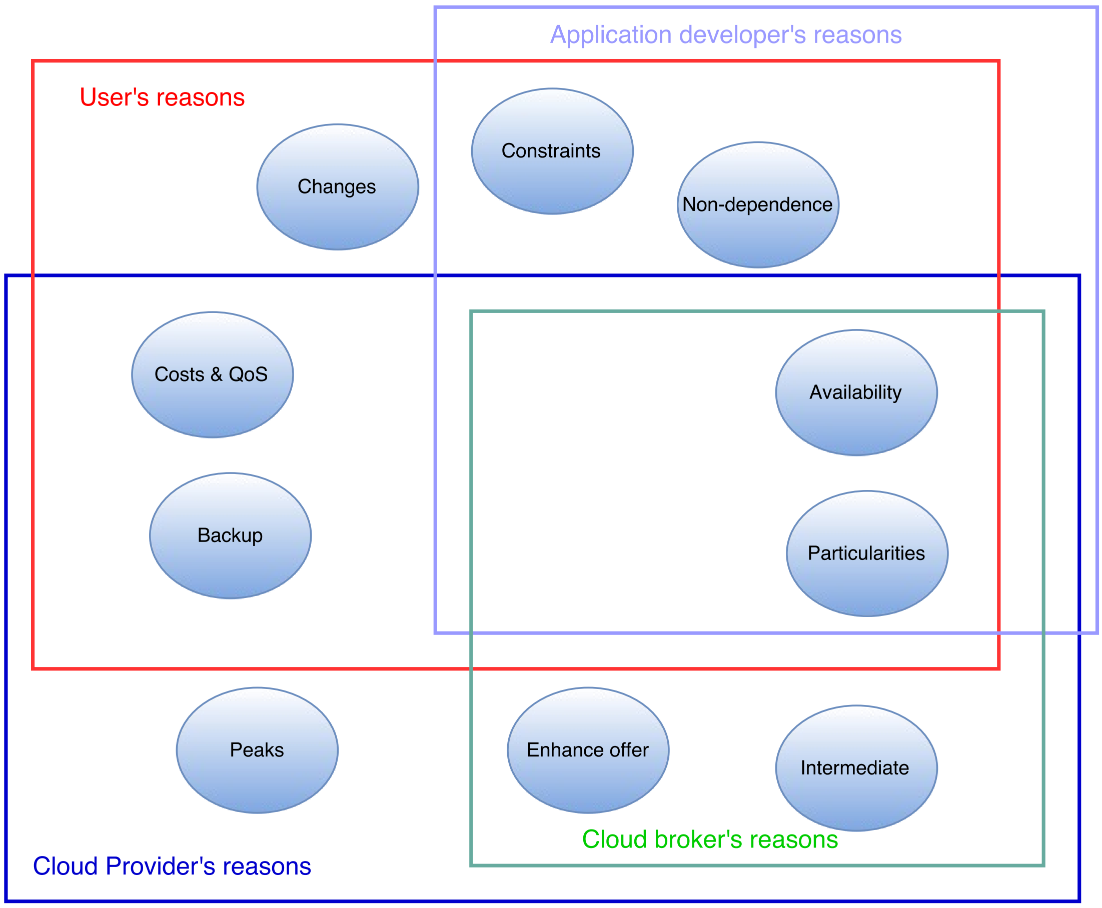


Figure 2.5: Resasons of Use of Multi-Cloud

2.4 Cloud Computing Contracts

A contract is a legally binding agreement between two or more parties. In cloud contract possible parties in the agreement are only cloud providers and cloud users or other mediators (cloud broker, sub-contractors) including cloud providers and cloud users. In practice, there are two contracting models [35] under which cloud providers provide services to the cloud users: 1) The online agreement is a click wrap agreement where user agrees the terms and conditions of the cloud providers as an "I agree" box or similar at the moment of service initiation. Online agreement is not subject to negotiation by cloud users. This model is most commonly followed model by cloud provider where cloud users do not have any bargaining power to negotiate the standard agreement offered by cloud providers. This analysis is limited to an online agreement model because all the information mentioned here are taken from CSPs' website; (2) The second contract is standard, negotiated, signature based agreement, which generally occurs when larger companies want to move their critical data or applications to the cloud (for instance public cloud). In such agreement cloud users are free to push their terms and conditions as well as requirements according to them in the contract document.

Most of the small cloud users are not allowed to negotiate the cloud contract according to their requirements. Cloud users should feel comfortable and safe with in the agreement rather than blindly accept the terms and conditions proposed by CSPs. Cloud users and providers are often reluctant to take advantage of cloud computing services because they think either terms and conditions are unclear or are unbalanced in the favor of cloud providers [99]. More often cloud providers try to avoid their responsibilities like in security and data protection on the users to be in safe side from any legal obstacles but these are the current big issues in cloud computing contract from the legal point of view. In our observation, most of the cloud providers provides contractual issues under Terms of service and SLA section in their website and few of them include SLA agreement in the Terms of service agreement.

2.5 Service Level Agreement(SLA)

Service level agreement (SLA) is a formal, negotiated document that defines (or attempts to define) in quantitative and qualitative terms the service being offered to the cloud users. Cloud service providers offer SLA with performances and service availability promises for their services. It is a documented agreement between the cloud service provider and cloud user that identifies services and cloud service level objectives. It should include minimum level objectives what cloud providers can provide to the cloud users and what happens when cloud provider failed to provide agreed minimum level objectives. Cloud Select Industry Group - Subgroup on Service Level Agreement (C-SIG-SLA) has presented a set of SLA standardization guidelines for cloud service providers and professional cloud users, while ensuring the specific needs of the cloud market and industry are taken into account [100]. This document is specifically targeted for European cloud market. We highlight here the major issues to be included in the SLA agreement.

2.5.1 Cloud SLA Metrics

Metrics provide knowledge about characteristics of a cloud property through both its definition (e.g. expression, unit, rules) and the values resulting from the observation of the property [102]. So, it is necessary to define a specific metrics in which basis cloud services are selected and ranked. However, there is not a standard defined SLA metrics in cloud computing, some initiatial works have been already conducted out to define the SLA metrics in cloud computing. Guide to Cloud SLA [48], Service Measurement Index (SMI) defined by CSMIC, TM Forum [129], NIST Cloud Computing Standards Roadmap [95], Cloud Computing Service Level Agreements [105], OCCI working group [98] have provided their important contributions to standardize the SLA metrics in cloud computing. Taking as a reference from CSMIC and QoS properties for web services proposed by [91] we list some of important SLA attributes with corresponding sub-attributes to be consider in cloud computing service monitoring (See Figure 2.6).

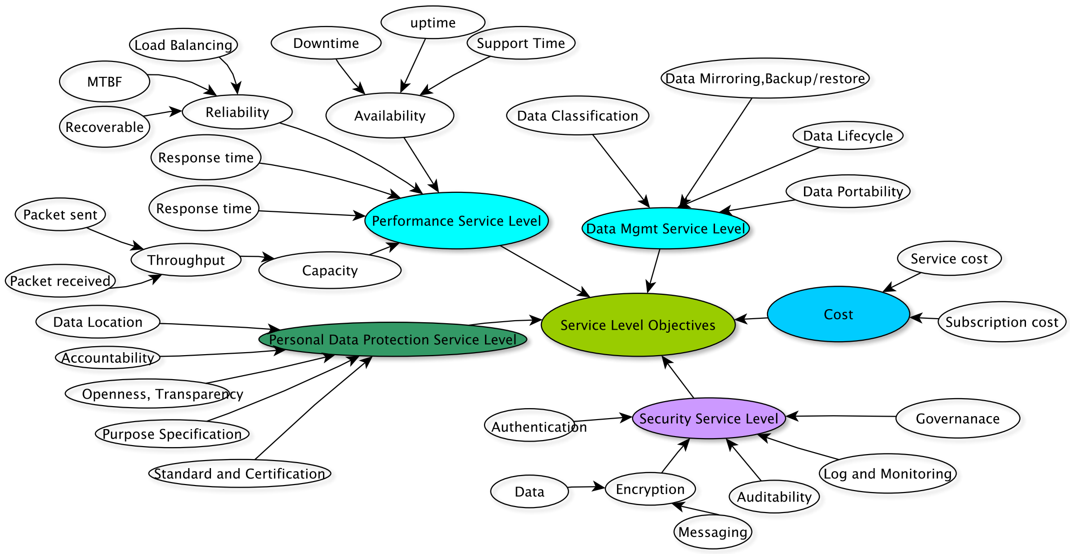


Figure 2.6: SLA Metrics in Cloud Computing

2.5.1.1 Performance Service Level

Performance service level includes availability of the services (uptime, percentage of successful requests, percentage of timely service provisioning requests), response time of the service, capacity parameters (Number of simultaneous connections, Number of simultaneous cloud service users, Maximum resource capacity, Service Throughput) and support (Support hours, Support responsiveness, Resolution time).

2.5.1.2 Security Service Level

In Security service level, main important point to be include are: Service Reliability, Authentication and Authorization, Cryptography, Security Incident management and reporting, Logging and Monitoring, Auditing and security verification, Vulnerability Management and security control governance. Service reliability which is directly interconnected with level of redundancy that cloud provider can provide, user authentication and identity assurance level should be mentioned to for Authentication and authorization. How a cloud service provider handles information security incidents is of great concern to cloud service customers, since an information security incident relating to the cloud service is also an information security incident for the cloud service customer. Incident reporting is also important in security Incident management. Logging is the recording of data related to the operation and use of a cloud service. Monitoring means determining the status of one or more parameters of a cloud service. Logging and monitoring are ordinarily the responsibility of the cloud service provider.

2.5.1.3 Data Management Service Level

From security and regulatory point of view it is necessary to classify data for example user's data, provider's data, cloud service derived data and so on. It is also necessary to mention about data backup, mirroring and restore, lifecycle of data and data portability with different formats and interfaces.

2.5.1.4 Personal Data Protection Service Level

In SLA agreement, it is tthe most important part to define cloud provider acts as a data processor or data controller or joint controllers (notably by processing personal data for their own purposes, outside of an explicit mandate from the user). It is also necessary describe applicable data protection codes of conduct, standards, certifications. If personal data are processed, it is necessary to define purposes of processing, openness, transparency o/f subcontractors, special categories of data. Document should define who is accountable on personal data breach. Another important point in data management service level is detail list about geographical location(s) where user data may be stored and/or processed and preferred geographical location for the storage of the user data. Last but not least, SLA agreement must define the access request response time period within which the provider shall communicate the information necessary to allow the user to respond to access requests by the data subjects.

2.5.2 Detail Analysis of Performance Service Level

In the previous section, we presented the standard SLA guideline proposed by OCCI working group. Basically, there are two types of SLA parameters: functional which are directly measurable and non-functional which are not directly measurable. In the thesis work, measurement of non-functional data are collected through user feedback or CSPs' SLA commitments mentioned in their website. Low-level performance parameters are measured from the CSP's premises. To compare these low level parameters either with SLA commitments provided by CSPs or service level requested from cloud users, we use mapping table to convert low level to SLA parameter and vice-versa. Table 2.2 shows the general concept of parameter mapping how low level parameter converted in to SLA parameters.

Table 2.2: Funtional Parameter Mapping to SLA Parameter

Functional Parameters	SLA Parameters	Mapping Rule
Uptime(t_U), Downtime(t_D)	Availability (A_v)	A_v=$t_U/(t_U$+t_D
I/p bytes, o/p bytes, packet size, BW_{in}, BW_{out}	Response Time (R_{tot})	R_tot= R_{in}+R_{out} (ms)
Packet sent, received packet, total packet	Throughput (T_r)	packet sent/total data
$MTTF$, λ	Reliability(R)	$R_{e(t)} = e^{-}\lambda t$

In the mapping rules the downtime variable represents the mean time to repair (MTTR), which denotes the time it takes to bring a system back online after a failure situation and the uptime represents the mean time between failure (MTBF), which denotes the time the system was operational between the last system failure to the next. R_{in} is the response time for a service request and is calculated as packet size/($BW_{in} - I/p$ bits) in milliseconds. R_{out} is the response time for a service response and is calculated as Packet size/(BW_{out} - o/p bits) in milliseconds. Throughput is mapped as packet sent/total data sent, where total data is the sum of the packet sent and packet loss. The reliability reflects how a service operates without failure during a given time and condition [141]. This characteristic is thus based upon the functioning duration before failure or the functioning duration between failure of the service, denoted MTTF, but also on the basis of the users failures. Therefore, λ which represents the failure rate is equal to: $\lambda = \frac{1}{MTTF}$. If failures are considered as unpredictable and randomly occurring, then the reliability of the service in time can be expressed as follows: $R_{e(t)} = e^{-}\lambda t$.

To cover functional and non-functional parameters in decision making process we have selected five SLA attributes; Performance, Availability and Reliability as functional attributes, Security and Cost as a non-functional attributes (See Table 2.2). To map parameters from measured values to SLA parameter we use mapping rule for converting into functional value. For example, if service downtime, uptime of particular cloud provider is known then it is mapped in to availability:

$$A_v = \frac{uptime}{uptime + downtime} \tag{2.1}$$

Mapping to SLA parameter from measured value depends on nature of services and types of service used. Definitions [101] and mathematical formula provided in [109], [140], [122] are used in parameter mapping.

These are the some example of parameter mapping. It can be extended in mapping rules from functional parameters to SLA parameters to make all of them are measurable and comparable with offered SLA by CSPs. Mapping to SLA parameter from measured value depends on nature of services and types of service used. Few parameters mapping has also presented in LoM2HiS [53] but these rules are not sufficient to compare all the SLA attributes. Some of the defined mapping rules are presented in Table 2.2. Definitions mentioned in QoS modeling for Green Cloud [73] and mathematical formula provided in [109], [140], [122] are also can be used in parameter mapping.

2.5.3 SLA Standards

The international standard for Information Technology Service Management, ISO/IEC 20000-1:2011 [81], formally defines an SLA to be a documented agreement between the service provider and customer that identifies services and service targets. It further elaborates that an SLA can also be established between providers and suppliers etc., can be included in a contract or other form of documented agreement. Cloud SLAs obviously relate to services provided by a cloud service provider, and in practical terms often include not just definitions of services and service targets, but also details of things such as the recourse in the event of an SLA being broken, the nature of support available for the service, and any requirements that may be imposed on the consumer of the cloud. In SLAware [13] the author Keven Kearney describes that SLAs are negotiated agreements between service providers and customers specifying their respective responsibilities and obligations in respect of service delivery and service usage. In addition to providing details of agreement parties, services and SLA duration, SLAs may, among other things, specify prices and costs, quality of service and other performance objectives, help-desk details, schedules for regular maintenance, penalties for SLA violations, exclusion clauses and termination conditions.

The ISO sub-committee responsible for Cloud Computing standards, ISO/IEC JTC 1/SC 38 Distributed application platforms and services (DAPS) [50], is at the time of writing drafting a vocabulary for cloud computing which may include a formalized cloud-specific SLA definition. In any event, commercial SLAs such as those for Amazon EC2 [92], Windows Azure [92] and Google Apps [66] are today arbitrary in nature. They are typically verbose, complex, static documents sometimes nested and of several pages in length. They are published by the cloud provider and describe details of services being offered from the cloud provider point of view.

The development of standards for SLAs has the potential to help automate discovery, negotiation, composition and monitoring of SLAs. The disposition of violations can also be automated. Cloud Consumers can be empowered with the ability to negotiate personalized SLAs tuned to their precise needs against a selection of providers. Cloud providers can propose flexible offerings and appeal to a wider customer base. Given that various terms in each SLA can be automatically tracked and monitored, providers also have the opportunity to maximize internal efficiencies, safe in the knowledge that their myriad of SLA commitments are being met.

2.5.3.1 SLA Standardization Initiatives

- *TM Forum*

  The TM Forum [129] have published numerous SLA-related documents including *GB917 SLA Management Handbook*, *TR178 Enabling End to End Cloud SLA Management* and *TR197 Multi-Cloud Service Management PackSLA Business Blueprint*. All are specifically designed to meet the particular SLA needs of the Telecommunications industry.

- *NIST*

  The recently published NIST Cloud Computing Standards Roadmap [95] discusses the potential for standardized SLAs. Version 2.0 of the NIST Cloud Computing Taxonomy, a work in progress, is expected to include a newly defined SLA taxonomy to support US Government procurement of Cloud Computing. Version 1.0 of the NIST Cloud Computing Technology Roadmap [103] includes SLA concept maps.

- *EU/ETSI*

  The European Commission has recently published a report summarizing SLA related results from numerous research projects it has funded: Cloud Computing Service Level Agreements - Exploitation of Research Results [105]. It includes recommendations for the Commissions Cloud Select Industry Group on

SLAs to consider, for potential rollup to the ETSI Cloud Standards Coordination (CSC) [54] initiative. The report details outputs from more than 21 projects and provides 11 specific recommendations for progressing SLAs. The ETSI CSC is coordinating the European strategy to address cloud standards.

- *OGF*

  The WS Agreement and WS-Agreement Negotiation standards can provide the basis for an SLA negotiation protocol. The OCCI working group [98] is planning to develop SLA extensions to the OCCI standard during 2014.

- *ISO*

  A New Work Item on SLA Framework and Terminology has been proposed. The scope for this work includes an overview of SLAs for Cloud Services, the relationship between a master agreement and SLAs, SLA components, commonly used terms, definitions and contexts. Note that a technically rich standard structure for SLAs is currently not in scope.

2.6 Cloud Service Brokering

Service brokering is a business model where services are delivered to the consumer through a third party entity or company called a broker, who acts as mediator between the two parties. This concept has already been used in Grid computing to distribute computing jobs to the Grid sites and monitor their status on behalf the user [106], [115]. With the emergence of Cloud computing, service brokering has been adopted to add new business values to Cloud services. Among them is the support of the user in selecting the provider that better meets his SLA requirements. The basic interactions needed between the broker, user, and provider during the selection process are depicted in Figure 2.7.

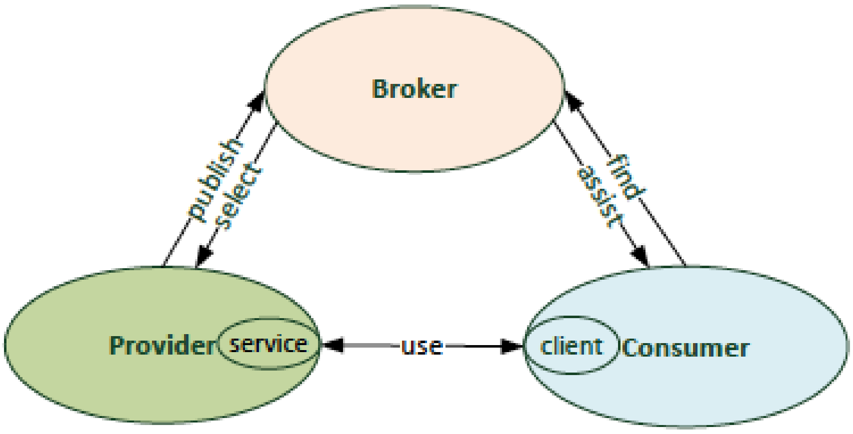


Figure 2.7: Cloud Service Brokering

The market research company Gartner [104] has defined three opportunities to use a Cloud broker:

- *Cloud Service Intermediation*: Building services on top of an existing cloud platform, such as additional security or management capabilities
- *Cloud Service Aggregation*: Deploying customer services over multiple Cloud platforms.
- *Cloud Service Arbitrage*: Brokers supply flexibility and opportunistic choices and foster competition between Clouds.

The lack of standardization and interoperability across Cloud providers makes the deployment of Cloud service brokers on current production Clouds a challenging task. Therefore most existing commercial companies offering Cloud brokering solutions use proprietary adapters to interface the Clouds that are limited in their functionality. The service-brokering life cycle for Cloud consists of the following steps:

1. Request Formulation: The user defines at design time the functional and non-functional SLA requirements for the requested Cloud service.

2. Discovery and Monitoring: The broker discovers the candidate service offers and stores their monitored SLA metrics and pricing information in different data repositories.

3. Matchmaking: The broker selects the suitable Clouds for provisioning the requested service by matching the SLA requirements to the candidate computing and storage resources.

4. Deployment: The broker deploys the service components on the selected providers. Cloud Service Brokering Life Cycle.

5. Execution: The service is executed and its status is continually monitored at the runtime.

6. Termination: The service can be terminated upon user request or by the broker (e.g., in case of repeated SLA violations).

2.7 Multi-Criteria Decision-Making(MCDM)

The Multi-Criteria Decision-Making (MCDM) [143], [1] theory is a research field related to operations research concerned with solving decision problems involving multiple, and often conflicting, criteria. Based on the goal of the decision maker, decision problems are classified into choosing, ranking and sorting problems. In the literature there are three basic methods for solving MCDM problems: Multi Attribute Utility Theory (MAUT), outranking, and the Analytic Hierarchy Process (AHP). These methods differ in the amount of input required from the decision maker and in their used objective functions, however their input and output parameters are similar. The basic input parameters (i.e., criteria and alternatives) and the required inputs from the decision maker to perform a MCDM process are depicted in Figure 2.8.

In MAUT [84], the preferences of the decision maker for or against each criterion are

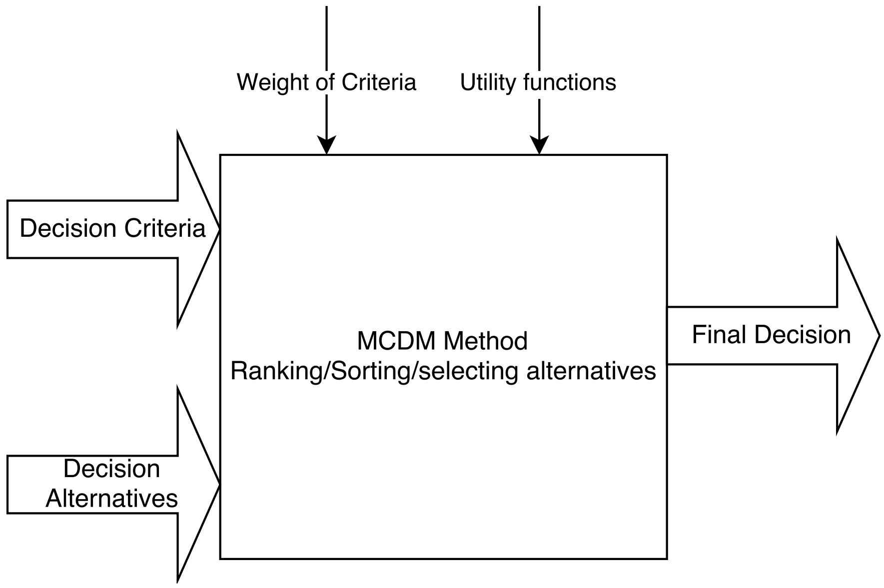


Figure 2.8: MCDM process

quantified using utility functions and their weight values. The decision problem is then simplified into a single objective function by aggregating the weighted utility functions of the decision criteria. Thus, the best solution should maximize this objective function.

The outranking MCDM method [57] checks the degree of dominance of one alternative over another by comparing its performance against all decision criteria. Unlike the other methods, the scaling and weighting of criteria is not required for the decision process. Since the outranking method is in some cases unable to find a non- dominant alternative, it is usually combined with other MCDM methods as a pre-step to reduce the number of alternatives. The AHP [120] methods solve decision problems by arranging the criteria and their alternatives into a hierarchy structure. Unlike MAUT, AHP is based on pairwise comparisons of decision criteria (using a numerical scale ranging from 1 (equal) to 9 (extremely important)) rather than using utility and weighting functions [60]. The unique features of AHP compared to other MCDM methods are the capabilities to support the interdependence among criteria and to check inconsistencies in the solutions found.

In this thesis, we follow a decision aiding approach proposed by Bisdorff [30], which involves the following steps:

1. Sorting the potential cloud providers into marginal performance quantiles classes;

2. Ranking the providers with multiple ordinal performance criteria;

3. Sorting the performance criteria in decreasing order of correlation with the previous ranking;

4. Visualizing the results in a performance heat map, ordering the potential CSPs from the best to the worst alternative.

2.8 Prediction Methods

Prediction methods are broadly divided into qualitative and quantitative. Qualitative forecasting techniques are subjective, based on the opinion and judgment of consumers, experts; they are appropriate when past data is not available. Quantitative predictions are applicable when past data are available. Due to many drawbacks in simple and weighted moving average of quantitative prediction, exponentially smoothing methods are widely used to predict the future data. The choice of prediction method is often constrained by data availability and data pattern. The pattern in the data will affect the type of forecasting method selected. The pattern in the data will also determine whether a time-series method will suffice or whether casuals model are needed. If the data pattern is unstable over time, a qualitative method may be selected. Thus the data pattern is one of the most important factors affecting the selection of a forecasting method [68]. Data may not follow the specific pattern in all the cases. In these circumstances, an automatic forecasting method is essential which determine an appropriate time series model, estimate the parameters and compute the forecasts [76]. The most popular automatic forecasting algorithms are based on either exponential smoothing or ARIMA methods.

2.8.1 Exponential Smoothing

The exponential method involves the automatic weighting of past data with weights that decrease exponentially with time, i.e. the most current values receive a decreasing weighting. For example in each increment in the past is decreased by (1-α), where $\alpha \in$ (0,1) is the smoothing parameter. Generally, there are three exponential smoothing are in practice: Simple, Double and Triple exponential smoothing. The triplet (E,T,S) refers to the three components: error, trend and seasonality. So the model ETS (A,A,N) has additive errors, additive trend and no seasonality and so on. ETS can also be considered an abbreviation of ExponenTial Smoothing [76].

2.8.2 ARIMA

It is a generalization of an autoregressive moving average (ARMA) model where data show evidence of non-stationarity. ARIMA models are generally denoted ARIMA(p, d, q)(P,D,Q)$_m$ where parameters p, d, and q are non-negative integers, p is the order of the autoregressive model, d is the degree of differencing, and q is the order of the Moving-average model. Furthermore, m refers to the number of periods in each season, and the uppercase P, D, Q refer to the autoregressive, differencing, and moving average terms.

2.9 Summary

This chapter presented the general background of cloud computing. Multiple cloud providers and performance measurement from multiple cloud providers base the thesis work on identification of SLA agreements offered. So, a brief introduction of multi-cloud architecture is presented including cloud computing. Basic idea of cloud contracts, Cloud SLA. Then, introduction of multi-criteria decision making (MCDM) including the Heat Map performance ranking method in the next section. Finally, short descriptions of prediction methods applied for performance prediction in the thesis is presented in the last section.

Part II

Related Works

Chapter 3

Related Works

In this thesis works, the contributions are divided in to three parts: 1) Cloud service monitoring, verification of delivered cloud services with offered SLA; 2) Performance evaluation and recommendation as an independent 3rd party (including as a cloud broker) to the cloud users and 3) Service pattern analysis of cloud providers including future performance prediction. Related works of each parts are provided in different sections. Section 3.1 gives the overview of research works in SLA Monitoring/Measurement and Service Verification. Similarly, section 3.2 provides the overview of works related to service performance evaluation and cloud service recommendation to users as an independant cloud service broker. Related research works in service performance prediction of CSPs according to current status of the CSPs to collect the future behavior of the cloud providers in section3.3.

3.1 SLA Monitoring/Measurement, Service Verification

This section provides the related works in service monitoring/measurement and service verification according to CSP's SLA commitments. Firstly, initiation of different bodies, for the standard guidelines to be included in SLA document, to define the SLA attributes to measure the cloud services are provided and then, monitoring/measurement techniques.

3.1.1 SLA Standarization

It is a documented agreement between the cloud service provider and cloud user that identifies services and cloud service level objectives. It should include minimum level objectives what cloud providers can provide to the cloud users and what happens when cloud provider failed to provide agreed minimum level objectives. Cloud Select Industry Group - Subgroup on Service Level Agreement (C-SIG-SLA) has presented a set of SLA standardization guidelines for cloud service providers and professional cloud users, while ensuring the specific needs of the cloud market and industry are taken into account[1].

- *TM Forum* The TM Forum [129] have published numerous SLA-related documents including GB917 SLA Management Handbook, TR178 Enabling End to End Cloud SLA Management and TR197 Multi-Cloud Service Management Pack-SLA Business Blueprint. All are specifically designed to meet the particular SLA needs of the Telecommunications industry.

- *NIST* The recently published NIST Cloud Computing Standards Roadmap [95] discusses the potential for standardized SLAs. Version 2.0 of the NIST Cloud Computing Taxonomy, a work in progress, is expected to include a newly defined SLA taxonomy to support US Government procurement of Cloud Computing. Version 1.0 of the NIST Cloud Computing Technology Roadmap [103] includes SLA concept maps.

- *EU/ETSI* The European Commission has recently published a report summarizing SLA related results from numerous research projects it has funded: Cloud

[1] https://ec.europa.eu/digital-single-market/en/news/cloud-service-level-agreement-standardisation-guidelines

Computing Service Level Agreements - Exploitation of Research Results [105]. It includes recommendations for the Commissions Cloud Select Industry Group on SLAs to consider, for potential rollup to the European Telecommunications Standard Institute (ETSI) Cloud Standards Coordination (CSC) [54] initiative. The report details outputs from more than 21 projects and provides 11 specific recommendations for progressing SLAs. The ETSI CSC is coordinating the European strategy to address cloud standards.

- *Open Grid Forum (OGF)* The WS Agreement and WS-Agreement Negotiation standards can provide the basis for an SLA negotiation protocol. The OCCI working group [98] is planning to develop SLA extensions to the OCCI standard during 2014.

- *International Organizations for Standardization (ISO)* A New Work Item on SLA Framework and Terminology has been proposed. The scope for this work includes an overview of SLAs for Cloud Services, the relationship between a master agreement and SLAs, SLA components, commonly used terms, definitions and contexts. Note that a technically rich standard structure for SLAs is currently not in scope.

3.1.2 SLA Monitoring/Measurement and Verification

To the best of our knowledge, there are very few works in service monitoring/measurement considering the SLA commitments of cloud providers. Some initial works have been performed in LoM2HiS [53] with few mapping rules to map the functional values to the SLA parameters. Lin et. al [142] have proposed SLA verification framework but this verification framework is limited to memory allocation in Virtual Machines (VMs). This framework provides a Third Party Auditor (TPA) to facilitate the SLA verification for untrusted CSPs instead of verification of SLA attributes. The authors in [16],

[74] and [62] provide the general concept of service monitoring but they do not consider the non-functional parameters in service verification.

In this section, we review the list of few commercially available monitoring tools [14], which are primarily focused on providing the service performance of functional parameters:

- CloudWatch[7]:

  It is a monitoring service for AWS cloud resources and the applications run on AWS. It can be used to collect and tract metrics, collect and monitor log files, set alarms, and automatically react to changes in the resources of AWS.

- AzureWatch[3]:

  AzureWatch monitors and aggregates key performance metrics form the different Azure resources like instances, databases, storage, websites and applications. It further supports user-defined performance counters related to quantifiable application metrics. Now, CloudMonix is repacing AzureWatch.

- CloudKick [79]

  Rackspace provides it users with monitoring data like CPU utilization and traffic volume. It also provides a cloud tools, which is able to build a complete monitoring solution with specific focus on virtual machines and alerting mechanisms.

- CloudStatus [6]

  It is one of the first independent cloud monitoring tool for AWS and Google App Engine, which is built on top of Hyperic-HQ. It provides monitoring of user application performance, a methodology for evaluating the root cause analysis of performance changes and degradations, and both real time and weekly trends of monitored metrics.

- NimSoft [10]

  Nimsoft Monitoring Solutions (NMS) is able to monitor data centers of both private and public clouds. It provides a single view on the IT infrastructures and services provided by Google Apps, RackSpace Cloud, Amazon, Salesforce.com and others through a unified monitoring dashboard.

- Monitis [9]

  It adopts agents installed on the resources to be monitored to inform users about the service performance and to send alerts when resource are considered scarce.

- LogicMonitor [8]

  It allows monitoring virtualized infrastructures by adopting an elastic multi-layer approach. Ranging from web servers or databases running on VMs to the underlying hypervisors, it automatically discovers and monitors newly added or deleted resources as they are provisioned by properly grouping them and sending related notifications.

- Aneka [2]

  It is a framework for the development, deployment, and management of Cloud applications. Aneka consists of a scalable Cloud middleware that is deployed on top of heterogeneous computing resources, and an extensible collection of services, coordinating the execution of applications, monitoring the status of the Cloud, and providing integration with existing Cloud technologies.

- CloudHarmony [5]

  It provides a wide set of performance benchmarks of public Clouds. The tests consider the common OS-layer metrics (related to CPU, disk and memory I/O), a wide set of application-layer benchmarks, such as Unixbench and IOzone (considering completion times for tasks like integer and floating point operations, file system access, system call overhead, etc.), and user- layer tests (RTT and throughput experienced by a web application).

3.2 Service Evaluation and Service recommendation of cloud providers

3.2.1 Cloud Service Provider Ranking

For the selection of the best web services according to consumers' opinion is introduced by Wang [11] for the web service selection based on consumer's vague perception. Practically, web services and cloud services can not be evaluated only the basis of consumers' perception because, user may not receive actual service delivered by CSP due to network problem, limited bandwidth and other problems. The authors in SMICloud [60] have proposed a framework for comparing and ranking cloud services based on AHP [87]. It considers only quantifiable SLA attributes defined by CSMIC (https://csmic.org). It does not consider the qualitative attributes and consumer's perception. Cloud users cannot be involved in decision-making process for the service recommendation. CloudCmp [88] has proposed framework to compare the performance of different cloud services but it only compares very low level performance metrics of Cloud services such as CPU utilization and network throughput etc. To the best of our knowledge, there is no selection model which selects and ranks the CSP based on both service delivered by CSPs and cloud user experience.

3.2.2 Cloud Service Performance Analysis

In the current growing cloud-computing business, selecting the best cloud service from appropriate cloud providers is very complex and challenging for the cloud users. There is a multitude of works that employ optimization to achieve this goal [69], however they usually require certain input data, and their solutions are applicable for the current situation. The multi-objective optimization attempts [71] overcome some of these limitations, but in turn they provision a Pareto front of optimal solutions, which creates a consecutive problem of the selection of the final solution .

The selection of the best web services according to consumers' opinion for the web service selection based on consumer's vague perception is introduced by Wang [11]. Practically, web services and cloud services can not be evaluated only on the basis of consumers' perception, because user may not receive actual service delivered by cloud provider due to network problem, e.g. limited bandwidth, or other problems.

For the ranking of cloud services SMICloud [60] has proposed a framework for comparing and ranking cloud services. It considers only quantifiable SLA attributes defined by Cloud Service Measurement Index Consortium (CSMIC) [49], and does not consider the qualitative attributes. SMICloud is based on an analytic hierarchy process (AHP) [87]. The main difficulty in the provider ranking based on the AHP technique is assigning the hierarchy of SLA attributes. In practice, each SLA attributes are important and dependent on each user's preferences.

The authors in CloudCmp [89] have proposed a framework to compare the performance of different Cloud services such as Amazon EC2, Windows Azure and Rackspace, but it only compares the low-level performance metrics of Cloud services such as Computer Processing Unit (CPU) utilization and network throughput etc. Such low-level performance metrics could be further used to create models of high-level system properties, such as power consumption or performance [72], but it has not been tackled.

Hoi Chan et. al [43] have proposed ranking and mapping of cloud computing applications. It is limited to few SLA attributes and does not provide a basis on which the weights of cloud services are assigned to each cloud provider. Service Ranking System [45] searches SLA offers provided by cloud providers rather than the quality of delivered services to rank the cloud providers. The authors in CloudRank [148] propose a cloud ranking algorithm based on greedy method which considers few functional parameters to rank the cloud providers and does not consider the delivered services in their framework. The cloud service selection process based on consumer experience and involving the third party to avoid a biased assessment of cloud services from users has been proposed by Qu et. al [116], however it does not cover the performance measurements from cloud providers. To the best of our knowledge, there is no evaluation framework, which selects and ranks the commercially available cloud providers based on their delivery of service compared with the SLAs offered by them.

3.2.3 Multi-Cloud Architecture

As the first industry driven project, the TM Forum[2] Cloud Service Broker Catalyst explored the role of a value-added service broker by demonstrating a proof of concept for a trusted and transparent Cloud management platform. Here, we classify related work into i) SLA based brokering and ii) Service verification. In our study we found that academic research are focused on service brokering and rarely tackles SLA-based brokering. There are very limited works in service verification delivered by cloud service providers.

Cloud brokering is a new architectural framework, which integrates the resources from different cloud service providers. Recently, cloud brokering is receiving a lot of attention to the research industry. Most of the works are focused on different scheduling methods to manage the resources from CSP's perspective then from cloud user's perspective. The authors in SLA based brokering [20] have proposed the SLA based service brokering in inter-cloud environment which propose the conceptual model for SLA management and interoperability feature, but SLA matching mechanism is missing in their work.

The CloudBus research project [36] provides an architecture for market-oriented Cloud computing. The three key components of this architecture are a Cloud broker, a

[2] http://www.tmforum.org

market maker and an Inter-Cloud. The Cloud broker schedules applications on behalf of the user by specifying the desired QoS requirements, whereas the market maker acts as a mediator bringing together Cloud providers and customers. It aggregates infrastructure demands from the Cloud broker and matches them against the available resources published by the Cloud providers. The Inter-Cloud [37] provides a scalable, federated computing environment composed of heterogeneous, interconnected Clouds, enabling Inter-cloud resource sharing. It is concentrated on optimizing cost and execution time from cloud users' perspective. The authors presented a flexible framework for multi-level SLA management within Clouds [128] developed in context of the SLA@SOI[3] EU project. The core framework consists of a Business Manager and an SLA Manager. The Business Manager controls all relations between customers and providers, whereas the SLA Manager deals with all the SLA related issues including negotiation, provisioning and monitoring. Besides the core framework, a domain-specific Service Manager provides management functionalities for the SLA Manager by interfacing the native provisioning system. The main contribution of the SLA@SOI framework is that the service quality can be predicted and enforced at run-time through an automated SLA management.

The authors implemented a prototype broker architecture [126] based on a combination of the core SLA@SOI framework and the RESERVOIR[4] framework. This latter allows an easy and on-demand provisioning of virtualized infrastructure resources within a federated Cloud platform. In their presented architecture, the core SLA@SOI framework acts as an SLA-based broker, whereas the RESERVOIR sites act as SLA@SOI third party providers and candidates for SLA provisioning. The SLA based brokering and provisioning is performed from the cloud provider's perspective instead of cloud user's perspective. The interoperability between the two Cloud frameworks is achieved by implementing a standardized Service Manager interface using the Open Cloud Com-

[3] http://sla-at-soi.eu
[4] http://www.reservoir-fp7.eu

puting Interface (OCCI) API[98].

In the study, it is found that academic researches are focused on optimization techniques in service brokering by efficiently placing cloud resources in different servers or in different locations. Current research works rarely tackle SLA-based brokering to provide the SLA assured optimal solutions to the CSUs. In cloud brokering, most of the works are focused on different scheduling methods to manage the resources from CSP's perspective rather than from CSUs' perspective. The authors in SLA based brokering [83] have proposed the conceptual SLA based service brokering model in inter-cloud environment, but SLA based optimization according to service delivery is missing in their work.

The authors in [59], [82] and [40] propose genetic algorithms to solve the QoS- aware service composition problem. Since they use single- objective genetic algorithms, they can provide only a single optimal solution. Also, they define aggregate functions to combine multiple objective values into a single objective value, and the quality of solutions highly depends on the design of the aggregate functions. For example, a weighted sum is widely used as an aggregate function, however it is not easy to define weight values for each objective in a fairly manner since objectives have different value ranges and priorities. Hiroshi et. al [131] provides SLA aware service composition with multi-objective optimization but does not consider the service delivered by CSPs. However, implementation of proposed algorithm in the multi-cloud brokering has been left in their work, Amato et. al [19] provides the general concept of multi-cloud brokering using multi-objective genetic algorithm. They provide the single optimum solution rather than set of multiple optimum solutions.

Owl-s based semantic cloud service broker [93] address the problem of cloud service matching and OWL-S based cloud service broker. It considers location of service, bandwidth, storage, cost and usage. OPTIMIS[5] describes the concepts of cloud bursting and

[5]http://www.optimis-project.eu

cloud brokerage along with security issues associated with two models[56]. OPTIMIS project has also now realized the requirements of various level of legal information that is necessary for automating the process of cloud provider selection and data outsourcing [86]. mOSAIC [113] is a vendor agnostic cloud broker, which consider SLA offered by CSPs but does not consider the service performance of them to recommend cloud services to the users.

The authors in QBROKAGE [22] propose a genetic approach for Cloud Brokering, focusing on finding Infrastructure-as-a-Service (IaaS) resources for satisfying Quality of Service (QoS) requirements of applications. It is more focused on to find near-optimal solutions even when dealing with hundreds of providers, trying at the same time to mitigate the vendor lock-in. Broker@Cloud[6] is another example of brokering framework, which is planned to allow cloud intermediaries to equip their platforms with advanced methods and mechanisms for continuous quality assurance and optimization of software-based enterprise cloud services.

Authors [41] have proposed conceptual framework for Legal Compliance Checking of cloud services and have planned to define a reference architecture for a self-adaptable and legislation-aware cloud service broker, however, service performance analysis and SLA commitments are missing in their work.

3.3 Performance Pattern Analysis and Performance Prediction

Increasing number of cloud providers with similar service offer, similar SLA commitments, similar service price makes complicated to the cloud user to choose best cloud providers according to their requirements. To differentiate cloud providers according to their service performances Wagle et al. [134], [136] proposed service evaluation tech-

[6]http://www.broker-cloud.eu

niques to evaluate the performance of cloud providers. Beside the current performance behavior of the cloud service provider, it is also important to know the historical and future performance behavior of them due to dynamic nature of cloud computing environment. Recent performance predictions are more based on Quality of Service (QoS) of web based services forecasting as an efficient technique to predict future QoS values in order to support QoS-based service selection and composition [90], [65], [42] and QoS management [96],[144], [149] in dynamic environments. These approaches have proposed time series ARIMA models to forecast the future values of QoS attributes. Simply, the key idea of these models is to fit the past QoS measures and forecast their future values.

In the domain of QoS-based service selection and composition, several researchers have investigated various approaches for QoS forecasting. Li et al. [90] propose a web service selection algorithm based on QoS prediction mechanism. Their algorithm uses time series modeling based on structural equations to fit QoS values of web services, and dynamically predicts their future changes to support adaptive services selection. Godse et al. [65] propose a method that combines monitoring and extrapolation methodologies based on ARIMA models to predict service performance. This method is used to support automating dynamic service selection methodology, which is robust in the face of varying QoS. Recently, Cavallo et al. [42] present an empirical study aimed at comparing different approaches for QoS forecasting, namely the use of average and current values, linear models, and ARIMA models. The study is performed on QoS data obtained by monitoring the execution of 10 real services for 4 months. It claims that the use of ARIMA forecasting has the best compromise in ensuring a good prediction error, being sensible to outliers, and being able to predict likely violations of QoS constraints.

In the context of QoS management, Nobile et al. [96] propose an architecture of QoS proxy for RT-RPCs (Real Time Remote Procedure Calls) that uses ARIMA models in order to predict future traffic characteristics of RT-RPCs that pass through the proxy. The architecture is based on allowing the anticipated allocation of the necessary resources to attend the predicted demand and the choice of policies aimed at the adaptation of the proxy to the states of its network environment. Zhu et al. [149] present a Grid-based framework that uses a time series prediction algorithm to forecast the future performance of parallel/distributed discrete event simulation (PDES). Zeng et al. [144] have investigated that performance metrics can be predicted based on their historical data and using ARIMA models. Their work introduces the design and implementation of an event- driven QoS prediction system, which can process operational service events in a real-time fashion, in order to predict or refine the prediction of performance metrics.

In the domain of cloud computing, Zhang et al. [145], [146] have proposed prediction approach for user's cloud component QoS usage experiences. It provides the performance prediction approaches of cloud users' end. Similarly, Panneerselvam et. al [110] analyzed the workload demand of users to reduce the excess resource consumptions of cloud providers. Amin et al. [21] propose a forecasting approach considering the high volatility of QoS measures and have claimed that it improves the forecasting accuracy of QoS attributes and violations. A. Biswas et al. [33], [32] proposes an auto-scaling framework to control enterprises resources coming in to cloud but it does not consider itself the prediction of performances of cloud providers. Syu et al. [125] has applied Genetic Programming for time-aware dynamic QoS prediction. Calheiros et al. [39] have proposed workload prediction method using ARIMA method and have analyzed impact of it in QoS prediction in cloud computing.

To the best of our knowledge, service performance pattern analysis including future performance prediction of cloud providers using real monitoring data is missing in the current research. Recent and future behavior of cloud provider helps in decision making to select appropriate cloud services to cloud users. These research works mentioned in this section show that it is crucial research issue to aware the cloud users with the current and future service performance pattern of cloud providers to select appropriate cloud services by cloud users. In this thesis work, ETS and ARIMA forecasting methods have been implemented to predict the future behavior in the service performance of the cloud providers.

3.4 Summary

This chapter provides the research works related to this thesis. Basically, we covered the works performed regarding the performance measurement, monitoring and SLA verification according to the SLA committed by CSPs in the first section. Then, the works related with the cloud contracts and SLA standardization initiatives taken by different bodies and organizations are presented in the next section. The third section provides the works related to performance evaluation techniques are presented in the next section. The last section provides the works related with performance pattern analysis and future service performance prediction.

Part III

Regulatory Issues in Cloud Computing

Chapter 4

Legal Issues and Service Commitments in Cloud Computing

This chapter is mainly focused on Legal issues and SLA commitments committed by cloud providers. Section 4.1 gives the overview of cloud contract and SLA. Section 4.2 is mainly based on regulatory issues from EU's General Data Protection Directive (GDPR) perspective.

4.1 Cloud Contract and SLA

A contract is a legally binding agreement between two or more parties. In cloud contract there might be the agreement between cloud service providers and cloud users or together with other mediators (cloud broker, sub-contractors). SLA is a formal, negotiated document that defines (or attempts to define) in quantitative and qualitative terms the service being offered to the cloud users. CSPs offer SLA with performances and service availability promises for their services. In practice, there are two contracting models [35] under which cloud providers provide services to the cloud users: 1) The online agreement is a click wrap agreement where user agrees the terms and conditions of the cloud providers as an "I agree" box or similar at the moment of service initiation. Online agreement is not subject to negotiate by cloud users. This model is the most commonly followed model by cloud provider where cloud users do not have any bargaining power to negotiate the standard agreement offered by cloud providers. This analysis is limited to an online agreement model because all the information mentioned here are taken from CSPs' website; (2) The second contract is standard, negotiated, signature based agreement, which generally occurs when larger companies want to move their critical data or applications to the cloud (for instance public cloud). In such agreement cloud users are free to push their terms and conditions as well as requirements according to them in the contract document.

Cloud users should feel comfortable and safe with in the agreement rather than blindly accept the terms and conditions proposed by CSPs, however, most of the small cloud users are not allowed to negotiate the cloud contract according to their choice. Cloud users and providers are often reluctant to take advantage of cloud computing services because they think either terms and conditions are unclear or are unbalanced in the favor of cloud providers[1]. More often cloud providers try to avoid their responsibilities like in security and data protection on the users to be in safe side from any legal obstacles but these are the current big issues in cloud computing contract from the legal point of view. In our observation, most of the cloud providers provides contractual issues under terms of service and SLA section in their website [119].

In the survey conducted by W. K. Hon et al. [12] pointed out major six terms included in standard cloud computing contracts in which cloud users are most interested to negotiate:

1. Limitation of liability in data integrity and disaster recovery,

[1] $http://ec.europa.eu/justice/contract/cloud-computing/index_en.htm$

2. Service Level Agreement (SLA)

3. Security and privacy

4. Vendor lock-in and exit

5. Provider's ability to change the service features and

6. IPR

Third and fourth terms are roughly equally negotiated terms depends on type of user and service. It shows that cloud users are not yet convinced with current practiced standard cloud contracts. However cloud contract documents have neither standardized format nor terminology [63], and do not abide by any precise definition, notwithstanding some recent attempts [17] towards standardization[2]. The paper categorizes following major issues in cloud contracts which causes legal issues:

- Regulatory Issues
  a. Data Privacy
  b. Location of Data
  c. Processor and Sub-processor Agreement
  d. Governing Laws and Jurisdiction
- Data Security
- Service Level Agreement
- Suspension and Termination of the Services

[2]https://ec.europa.eu/digital-single-market/en/news/cloud-service-level-agreement-standardisation-guidelines

4.2 Regulatory Issues from cloud computing contractual point of view

As data of various cloud users is stored in a shared infrastructure environment, it is the possibility of accessing confidential data by un-authorized users or media. This causes many technical issues to protect data from unwanted access as well as it creates the legal issues due to dynamic nature of service access in cloud computing.

4.2.1 Data Privacy

The recently enacted EU's GDPR[3] repealing EU's Data Protection Directive 95/46/EC[4] gives fundamental rights to the data users(data subject) with respect to their personal data while requiring "data controllers" to follow rules and restrictions with respect to their data processing operations [85]. The Regulation is designed to further addressing new technological developments. Cloud users are entitled to inform the identity of any data controller and the purposes for which personal data are being collected or processed. According to EU's GDPR, data controllers should follow these main privacy protection principles of data protection that define the individual rights of the users and the responsibilities of data controllers that process personal data: fair and lawful processing, collection and processing only for a proper purpose, should be adequate, relevant and not excessive, should be accurate and up to date, should be retained no longer than necessary, giving the data subject access to his or her data, keeping data secure and no transfer of personal data to a country that does not provide an adequate level of privacy and personal data protection. New penalties (including fines of up to the greater of 100 million, or 2-5% of annual worldwide turn over) in the new regulation make cloud providers serious in regulatory compliance.

In the U. S., there is no comprehensive federal legislation to protect consumer's

[3] $http://ec.europa.eu/justice/data-protection/reform/index_en.htm$

[4] http://eur-lex.europa.eu/legal-content/

personal data and privacy. There is also not generally applicable regulations to limit the export of personal data outside U. S. considering as a sensitive data but sensitive data is to be considered for the data collected by online services about children under the age of 13; data collected by financial institutions about their customers; data collected by credit reporting agencies about consumers; and data collected by health care providers about patients [85].

In Australia, privacy issue is regulated by Privacy Act1988(Cth). It is also applicable even it is done outside Australia if it relates to personal information about an Australian citizen, resident or related to Australia. This Privacy Act outlines national privacy principles, including a requirement that where personal information is collected, the record must be protected by reasonable security measures[5] and that generally information collected for one purpose should not be used for another[6] but it is not as strict as EU's data protection regulation related to the data privacy.

4.2.2 Trans-boarder Data Flow

Cloud service providers provide services to the users located in one or several countries; also, the first provider may outsource a portion of the processing to another cloud provider or may in turn be renting its cloud infrastructure from a bigger cloud provider [114]. All of these providers may be located in different countries or under different jurisdictions. There are three commonly used cloud computing deployment models: Private, Public and Hybrid which is the combination of private and public cloud. An additional model is a community cloud, which is less commonly used. From judiciary point of view, there are two cloud models: 1) Domestic Clouds: If a cloud is physically located under the same jurisdiction, it is a domestic or mono-jurisdictional cloud. In European Union (EU), a cloud is "domestic" or "mono-jurisdictional" if the conditions laid down by Article 4 of the GDPR are satisfied: either the controller is

[5] S14, National Privacy Principle 4.
[6] S14, National Privacy Principle 10.

located within the EU or, it uses equipment located in the EU for purposes other than those of transit; 2) Trans-border clouds: If a cloud is not physically located under the same jurisdiction, it is a Trans-border or trans-jurisdictional cloud. In other words, the cloud, which does not fulfill the provision of domestic cloud it, is trans-border cloud.

The EU GDPR prohibits the transfer of personal data to countries, which do not ensure an adequate level of protection within the meaning of Article 25(2). Unless the data subject has given the previous consent unambiguously to the proposed transfer or under the condition that other procedures are in place, as per Article 26, data transfer outside European Economic Area (EEA) is not acceptable. Model Contracts, Safe Harbor Principle, Binding Corporate Rule (BCR) are the provisions for the personal data transfer outside EU.

4.2.3 Processor and Sub-processor Agreement

According to EU GDPR, processor of personal data must comply certain requirements when engaging in processing of personal data. There is still issue in cloud computing, cloud provider is data processor or data controller[25]. Many providers are silent on the point or try to take their responsibility only as data processor. Many providers try to ensure they are not regarded as controllers (with greater obligation and liabilities) [12]. In cloud computing, there are many other service providers who act as cloud providers. Big cloud providers outsource multiple channels to sell their services. These multiple channels are also called reseller or service provider or outsourcer or cloud broker, which acts as mediator of cloud provider and cloud users. Cloud broker may act as both cloud provider and cloud user because it can provide service to the end users integrating from multiple cloud providers as well as get cloud services form multi-cloud environment as a cloud users.

4.2.4 Governing Laws and Jurisdiction

As discuss in previous sections, cloud providers may have data center and service providing channels in different locations around the world. Cloud providers should comply and respect all the legal issues according to their national law to provide the cloud services to the users.

4.2.5 Data Subject Rights

It is a responsibility of cloud provider, to respond to data subject, if sh/e requests access to his/her personal data [12]. Behaving as a data processor, sometimes cloud providers want to skip such obligation of data subject. In such case, cloud provider points out users have direct access to and control their data and cloud provider does not have any role because they chose provider to process. This issue most often arrives because of unclear definition of cloud provider whether it is processor or controller.

4.3 Important Issues to be considered in Cloud Computing Contracts

The objective of the cloud contract is defining safe and fair term and conditions in the agreement, which is clear and transparent to every parties involved in the agreement. This section provides the most essential points to be included in cloud contracts.

4.3.1 Liabilities

Providers try to exclude liability altogether or restrict liability as much as possible because they provide commoditized services[12]. It is also true that it is not always practical to expose unlimited liabilities to the CSPs for small deal. Liabilities of data loss of IaaS providers, liability for intellectual property rights infringement of software of SaaS providers are some examples conflicting issues mostly in between user and provider [12].

4.3.2 Provider Lock-In and Exit

Lock-in is one of the top concern of cloud users. Most of the cloud users may not wish to be locked-in for long time with an initial contract. Users should be free to leave the service after short specific time. User should be allowed to leave the service when s/he feels service is not appropriate to her/him or same service is available in the market in the cheaper price from other CSP. This is somehow commercial issue but main concern is how user's data and metadata can be recovered once service is terminated for whatever the reason. Data formats should be easily accessible, readable and importable into other applications of other CSPs independently. Data retention and deletion are also important issues in cloud contract. Users should be assured about retention of their data and complete deletion of their data after contract termination[12].

4.3.3 Terms and Conditions

As usual like in other contracts there should be minimum term, renewals and notice periods. Long initial terms may be one of the issues of provider lock-in. Many of the CSP set automatic renewal provision, which may mislead cloud users if there is not a fix, notice periods. These terms and conditions depend on type services and types of business scale. Suspension rights must be also clearly mentioned in agreed contract document.

4.3.4 Service Level Agreement(SLA)

It is a documented agreement between the cloud service provider and cloud user that identifies services and cloud service level objectives (SLOs). It should include minimum level objectives what CSPs can provide to the cloud users and what happens when CSP failed to provide agreed minimum level objectives. Cloud Select Industry Group - Subgroup on Service Level Agreement (C-SIG-SLA) has defined a set of SLA standardization guidelines for CSPs and professional cloud users, while ensuring the specific needs of the cloud market and industry are taken into account. This document is specifically targeted for European cloud market. We have highlighted some major points, which are important to be included in the SLA agreement in Section 2.5.

4.3.5 Changing Service Features

CSPs should not be entitled to change terms without consent, or at least should give users notice and allow them to terminate[7]. Any changes in service must not adversely affect the previous commitment. Users must be notified with sufficient time mentioning the key changes and impact of changes.

4.3.6 IPR

Intellectual property rights issues arise frequently on cloud processed data and, or applications. This generally happens due to not addressing properly who owns data in the cloud contract document.

4.4 Summary

This chapter provides the some important legal issues related to our thesis work. Firstly, we mention about what is cloud contract and how SLA should be included in cloud contract. Secondly, we included the important issues to be considered in cloud contract from recent General Data Protection Regulation (GDPR).

[7] https://www.cloudindustryforum.org/search/site/CIF3

Part IV

Design Implementation and Evaluation

Chapter 5

Design and Implementation

5.1 Overall Implementation Framework

Figure 5.1 shows the entire framework of our thesis work to implement in SLA assured service brokering. According to cloud reference architecture mentioned in section 2.2 of chapter 2, SLA assured brokering framework is proposed to assign different task to multiple actors in the reference architecture. In SLA assured service brokering, cloud users request the cloud services to the cloud broker according to their requirements. Cloud broker accesses the multiple cloud providers and offers the cloud services to the cloud users according to their requirements or priority. Cloud broker receives the cloud users request with priority list of requirements from the cloud users. Then, cloud broker discovers the services from multiple cloud service providers according to service request from cloud users. The cloud broker matches the services requests from different cloud providers and provides the services to the users, however, in this thesis, end to end service offer from cloud broker perspective is out of limit. The general concept of the proposed SLA assured service brokering shown in Figure 5.1 with the role of different modules are presented here:

1. Cloud Service Providers (CSPs)

They are composed of multiple data centers with different cloud resources and SLA templates. Cloud broker can access the cloud services offered by cloud service providers and provide the services to the customers according to their requirements using different matching algorithms. Generally, cloud service providers provide the information about the status of the data centers like uptime, downtime, response time, server load, CPU utilization etc. However, these values may not be trustable without third party verifier. For that purpose, we implement monitoring agents in CSP's premises to receive the exact and trusted status of

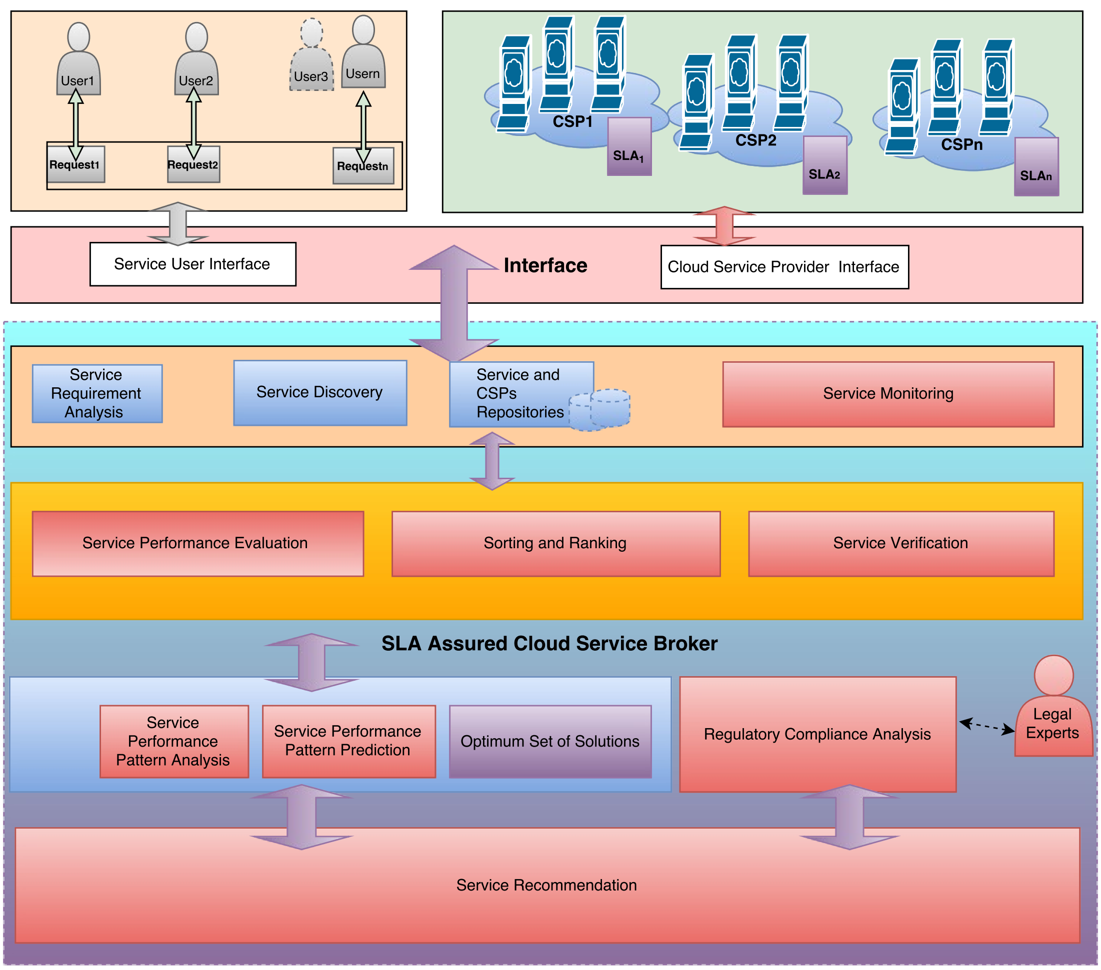


Figure 5.1: SLA based brokering and Service Verification Framework

the services offered by service providers. These values are compared with parameters mentioned in SLA template. Details of service measurement and verification are mentioned in Section 5.2.

2. Cloud Users

   Figure 5.4 shows service requirements from cloud users. For example cloud users might be:

   General users: The user who does not need high security requirements but prefer cheaper services,

   Banking users: The users who need high degree of security requirement and high accessibility with the system even the service price is higher.

   Gaming and Medical Users: In this category, the users are more concerned with accessibility(availability) of the system than other cloud users.

3. Interfaces

   Through service user interface, cloud user accesses the service of cloud service providers and cloud broker and cloud user use cloud service provider interface to access the services of the cloud service providers.

4. Service Requirement Analysis

   This module analyzes the requests from cloud users to access the cloud services from different cloud providers according to the users request.

5. Service Discovery This module discovers the services offered by cloud providers to match the services requested from cloud users.

6. Service and CSPs Repositories

   It stores all the information of cloud providers including SLA commitment, service delivery status of the cloud provider and service request of cloud users with priority lists.

7. Service Monitoring This module collects the SLA committed by CSPs and SLA delivered by CSPs. SLA template contains both functional and non-functional parameters. We perform manual operation in data collection.

8. Service Verification This module compares the exact services offered by cloud service providers with SLA agreement between cloud service provider and consumer. If measured values meet with the SLA parameters, CSP will be verified according the service delivered. Otherwise feedback will be sent to the corresponding service providers for the correction according to the SLA template.

9. Sorting and Ranking After comparing the measured values with SLA parameters, this module provides scoring to each cloud providers based on sum of deviation in offered services. This ranking information of each cloud service providers will be usable for the cloud users and cloud brokers to select the services based on users' requirements. Regulatory bodies can utilize this information for the regulatory enforcement to the cloud providers. Cloud service providers can also get benefited from this scoring value so that they can improve their service quality.

10. Service Performance Evaluation

    This module evaluates the performance of CSPs using quantifiable parameters, which are converted from non-quantifiable parameters measured in CSPs' premises. Based on the parameters evaluated by this module, service verification module verify the services with SLA committed by CSPs and sort and rank the CSPs according to their performance by sorting and ranking module.

11. Regulatory Compliance Analysis

    CSPs contain data center locations in different places. To deliver the cloud services to the cloud users, CSPs should comply the national and international laws.

This module analyzes the regulatory compliance status of the CSPs before recommending the services to the users. Legal experts are associated with this module to assess the regulatory compliance.

12. Service Performance Pattern Analysis

    To select the appropriate cloud services according to their requirements it is also important to know the current service delivery pattern and future service delivery pattern. We provide service delivery patterns of the CSPs and predict the future performance of CSPs based on current performance data.

13. Service Performance Patten Prediction

    This module predicts the service performance of the cloud provider based on current service performance of the cloud provider, which provides the future service performance delivery pattern of the cloud providers.

14. Optimum Set of Solutions

    The basic concept this module is to provide the combination of optimal set of solutions according the cloud users' priority requirements [132]. It provides the set of solutions from the cost perspective. In general, user has to pay high service cost for the high performance and comparatively low cost for low performance.

15. Service Recommendation

    Considering all the aspects (SLA committed by CSP, service performance delivered by CSPs and regulatory compliance status of CSPs), SLA assured cloud service broker recommends the services to the cloud users according to users' requirements and priority lists.

The details of each modules implemented in this thesis work will be provided in the next sections.

5.2 Cloud Performance Monitoring Framework

To provide the actual services delivered from CSPs, we monitor the services delivered cloud providers. Monitoring all the services delivered by CSPs is a complex task. For instance Ganglia distributed monitoring system[1] can be used as a cloud service monitoring tool which is a scalable distributed monitoring system for high-performance computing systems such as clusters and Grids. It is based on a hierarchical design targeted at federations of clusters. It leverages widely used technologies such as Extensible Markup Language (XML) for data representation, External Data Representation (XDR) for compact, portable data transport, and RRD tool for data storage and visualization. It has low per-node overheads and high concurrency. The implementation is robust, has been ported to an extensive set of operating systems and processor architectures, and is currently in use on thousands of clusters around the world. It has been used to link clusters across university campuses and around the world and can scale to handle clusters with thousands of nodes. Figure 5.2 shows the extraction of actual functional matrix from cloud service provider premises. The monitoring agent embedded with virtual host (VH1) measures the resource metrics from cloud infrastructure. For the disaster recovery, VH2 also measures the resource metrics from the same cloud infrastructure so that results will be accessed in case of VH1 fails. Similarly, it collects the resource metrics from another cloud infrastructure. All resource metrics measured from individual cloud infrastructure are collected in data collection. These functional parameters are converted to SLA mapping to map to SLA parameters as mentioned in section 2.5.2 of chapter 2.

5.2.1 SLA Commitment Verification

There are two types of requirements of every user: functional requirements and non-functional requirements. Requirements, which are directly measurable, are called func-

[1] http://ganglia.sourceforge.net

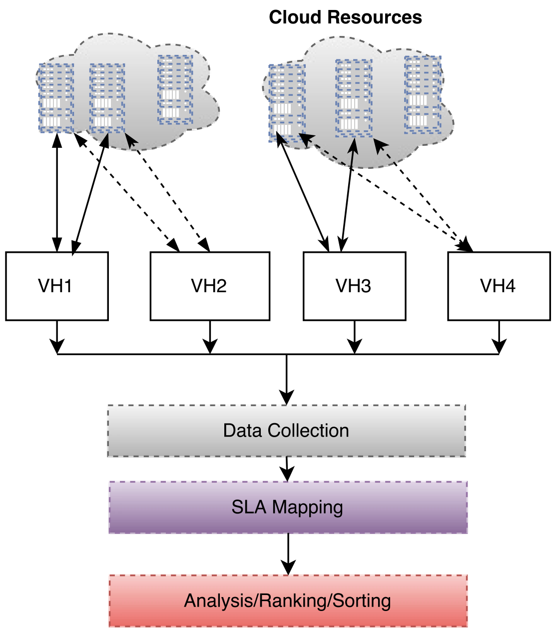


Figure 5.2: Extracting the status from CSP's premises

tional requirements and those, which are not directly measurable, are non-functional requirements. CSPs do not provide all the low level information of service delivery status. It is assumed that CSPs provide their SLA commitments in high level performance matrices like *Availability*, *Reliability* etc. Table 2.2 shows the general concept how measured SLA parameters from CSPs' premises are converted to SLA parameters to compare with SLA commitments by CSPs.

5.3 Service Performance Ranking and Evaluation

In the entire work to evaluate the performance of the cloud provider, we used the two commercially available cloud monitoring tools for the cloud service recommendation and CSP ranking and Cloud Harmony for pattern analysis of the CSPs.

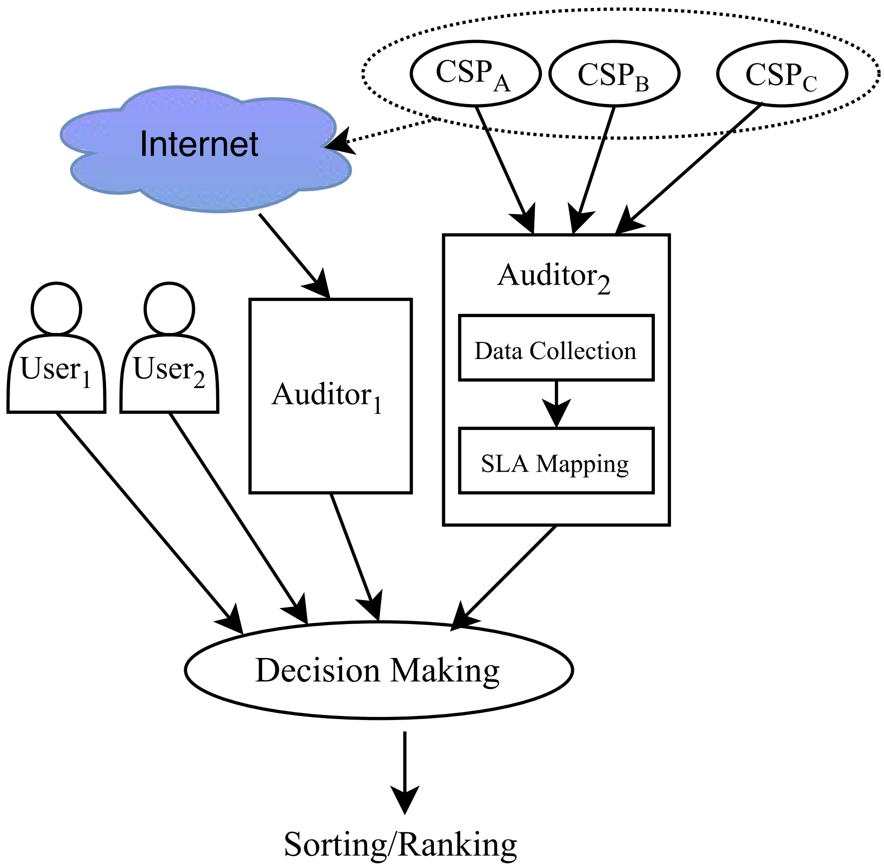


Figure 5.3: CSP Performance Measurement Model

5.3.1 Experiment Setup for Service recommendation and CSP Ranking

Figure 5.3 shows the performance measurement model to collect the performance of commercially available CSPs and feedback of the cloud users. To provide the ranking/sorting of of cloud providers, cloud auditors collect the service performance of cloud providers. $Auditor_1$ is designed for collecting service performance information of cloud providers through internet (using commercially available monitoring tools) and $Auditor_2$ is designed for collecting service performance internally as mentioned in section 5.2. $User_1$ and $User_2$ provide the customer experience of cloud services to participate in decision-making.

5.4 General Overview of Cloud User's Request and Relations with Stakeholders

In this section, we have defined the different attributes including functional and non-functional parameters from different cloud service entities' perspective and their relationship with each other.

5.4.1 Cloud Users

Figure 5.4 shows service requirements from cloud users. For example cloud users might be:

1. General users: The users who does not need high security requirements but prefer cheaper services,
2. Banking users: The users who need high degree of security requirement and high accessibility with the system even the service price is higher.
3. Gaming and Medical Users: In this category, the users are more concerned with accessibility(availability) of the service than other cloud users.

5.4.2 Cloud Broker

Figure 5.5 shows the relations and different attributes from cloud broker's perspective. Each cloud service provider has name, identification number (Csp-ID), and SLA template. Cloud users request the cloud services from the cloud broker. Cloud broker identifies the best cloud service providers among multiple cloud providers according to SLA offered by them and delivers the cloud services to the users according to their request and willingness to pay for the services.

Cloud Auditor/Verifier (Figure 5.6 gather the service commitments offered by cloud providers and service performance delivered by cloud providers in the service reposito-

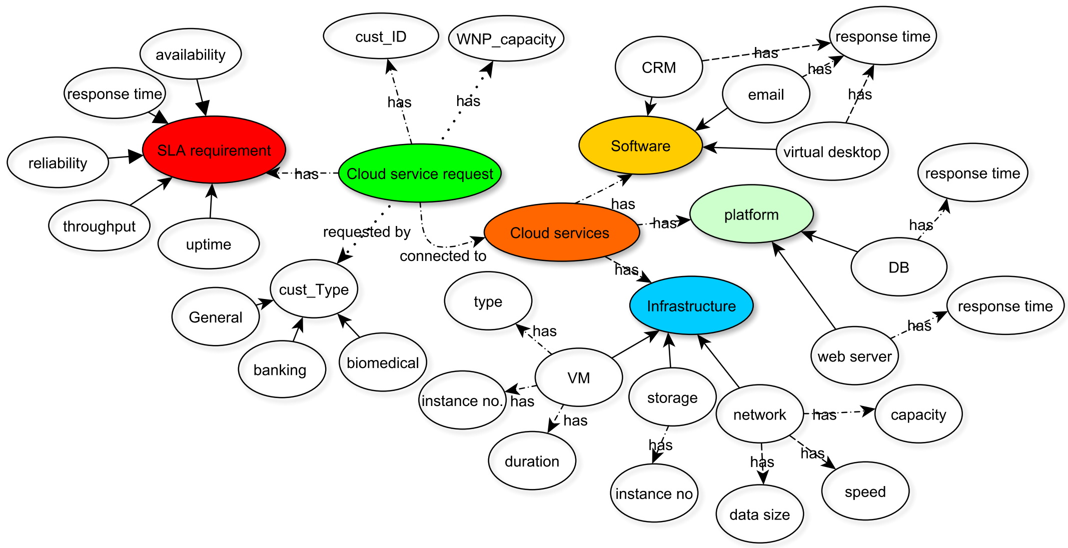


Figure 5.4: Service Request from different Cloud Users

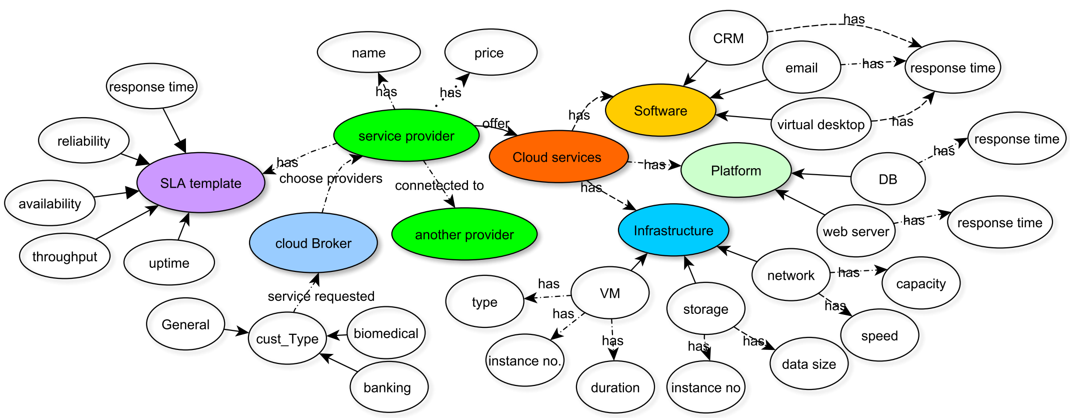


Figure 5.5: Cloud Broker Relation with Cloud Users and Cloud Service Providers

ries with identical csp_{name} and csp_{ID}. This information collected in service repositories is used to verify the service committed by cloud providers and rank/sort the cloud providers according to their service performance to the cloud users.

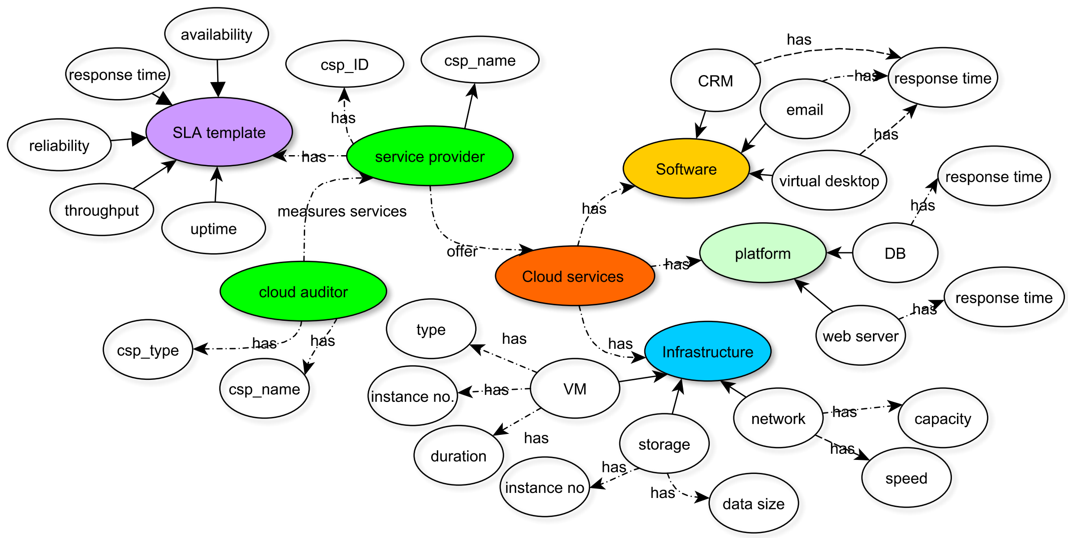


Figure 5.6: Cloud Service Auditor/Verifier

5.5 Summary

In this chapter, overall SLA assured cloud service brokering framework is provided. It provides the general overview of stakeholders and entities involved in cloud service brokering. The first section describes the details of modules used in SLA assured service brokering. Then, next section provides the service performance monitoring techniques from cloud providers. Another section provides the overview of ranking/sorting framework based on service performance of cloud providers. The last section provides the overview of cloud user's request, relation of cloud broker and cloud auditor with other stakeholders in cloud computing environment.

Chapter 6

Cloud Service Provider Ranking/Sorting Algorithm

To evaluate the performance of cloud service providers, we have to consider both measurable and non-measurable parameters. For example, *Availability(Uptime, Downtime)* is directly measurable and level of *Security* is not directly measurable. It is the feeling of users' experience. So, to include both measurable and non-measurable parameters in the performance evaluation, we propose IFL (Intuinistic Fuzzy Logic) method which was first introduced by Ping [11] for the web service selection and Heat Map technique based on quantile class proposed by Bisdorff [30] for choosing best poster in a conference.

6.1 IFL Concept

As cloud service providers (CSPs) offer similar kind of cloud services, searching the appropriate cloud services according to consumers' requirements in the increasing number of CSPs is becoming a complex task. CSPs offer SLA commitment to the cloud users but there are little or no verification mechanisms, which ensure that CSPs are delivering cloud services according to service committed. We propose a CSP ranking model based on service delivery of CSPs and user experience. To rank and select the appropriate cloud providers, an intuitionistic fuzzy group decision-making is used, as it can include both measurable and non-measurable value in selection process. It also provides the position of CSP on the basis of particular SLA parameter, which helps cloud users to select the CSP according to their specific requirements [134].

6.1.1 Algorithm

With the increasing number of cloud service providers (CSPs), selecting the appropriate cloud services according to their requirements is a complex and tedious job for the cloud users. CSPs commit their service offer to the users through *Service Level Agreement* (SLA). SLA is composed of different Quality of Service (QoS) rules, which are obligations that have to be followed by CSPs [73]. In many cases, CSPs offer similar or identical characteristics of services, which makes more complex for cloud users to choose services according to their exact requirements. Major challenge of cloud users nowadays is the practical difficulty in trusted and objective assessment of the fulfillment of SLA terms offered by CSPs [134].

The current techniques and tools for measurement are more suitable to quantify functional properties than non-functional properties of the SLA attributes. Practically, non-functional SLA properties rely heavily on the perceptions of service providers by consumers. These perceptions are not easy to assess due to their complexities, vagueness, and the involvement of ill-structured information [11]. We propose an integration of an auditor module (two cloud auditors of different nature: internal auditor ($auditor_{int}$ or $auditor_1$) and external auditor ($auditor_{ext}$ or $auditor_2$) that measures the services delivered by CSPs. Cloud users provide their assessment according to their user experience. The opinions of cloud auditors measurement and users are expressed in linguistic terms for the performance rating of each criterion. The proposed model ranks the cloud providers in terms of all the SLA attributes in cloud computing as well as in terms of particular SLA attributes (like in terms of *Availability*, *Reliability*, *Performance*, *Cost* and *Security*) which will be very helpful to the users to choose the appropriate CSP according to their requirements. In this section, we introduce the basic of Intuinistic Fuzzy Set (IFS) introduced by Atanassov et al. [23] and [24] and algorithm to provide the group decision based on auditors' service measurement and consumer's perception [11].

6.1.2 Cloud Service Ranking Algorithm

Let a set X = $x_1, x_2, ..., x_n$ be a finite universal set. An IFS A on X is an object with the form $A = (x, \mu_A(x), \nu_A(x))|x \in X$ where the functions $\mu_A : X \rightarrow [0,1]$ and $\nu_A : X \rightarrow [0,1]$ assign the degree of membership and the degree of non-membership to the element $x \in X$. Functions $\mu_A(x)$and $\nu_A(x)$are constrained by $0 \leq \mu_A(x) + \nu_A(x) \leq 1$

$$0 \leq \mu_A(x) + \nu_A(x) \leq 1 \tag{6.1}$$

A third parameter of IFS $\pi_A(x)$, known as the intuitionistic fuzzy index or hesitation degree of whether x belongs to A or not: $\pi_A = 1 - \mu_A(x) - \nu_A(x)$.

$$\pi_A = 1 - \mu_A(x) - \nu_A(x) \tag{6.2}$$

It is obviously seen that for every $x \in X : 0 \leq \pi_A(x) \leq 1$

$$0 \leq \pi_A(x) \leq 1 \tag{6.3}$$

If $\pi_A(x)$ has small value, knowledge about x is more certain and vice-versa. We apply the following algorithm to rank the cloud provider based on complete SLA criteria and individual criteria.

1. We first select the evaluation criteria with different sub-criteria under each criteria.

2. Decision makers involved in decision making use the linguistic terms defined in Table 6.1 to define the importance of criteria in linguistic term. The aggregated importance of the criterion, $w(c_j)$ which is agreed by group of decision makers, is computed applying Eq.6.4.

$$w(c_j) = [\mu_w(c_j), \nu_w(c_j)] \tag{6.4}$$

   Where $w(c_j)$ is calculated using intersection operator of IFN defined by Atanassov[24] with all the IFN value provided by decision makers.

3. To compare each SLA attributes from alternative cloud provider, we aggregate the weights of subcriteria under the same criteria using Eq.6.5 to calculate $W(c_j)$

$$W(c_j) = c_{i1} \cap c_{i2} \cap .... \cap c_{in} \tag{6.5}$$

   where i belongs to the same SLA criteria. $W(c_j)$ is the aggregated weight of the importance of all sub-critera to criteria.

4. Decision makers evaluate each of the alternatives and gives the corresponding score for each alternatives. Let the $D_k(k = 1, ..., q)$ decision makers employ the symbolic linguistic terms defined in second column of Table 6.1 to evaluate the performance of cloud provider under each criterion $(c_j)(j = 1; 2; ...; n)$ which is

expressed in the form of the matrix.

$$X = [x_{ij}^k] \begin{bmatrix} x_{11}^k & x_{12}^k & \dots & x_{1n}^k \\ x_{21}^k & x_{22}^k & \dots & x_{2n}^k \\ \dots & \dots & \dots & \dots \\ x_{m1}^k & x_{m2}^k & \dots & x_{mn}^k \end{bmatrix}$$

Where k is number of decision makers, n is the number of decision criteria and m is the number of alternatives. Using Max-Min-Max composition (T) defined by Biswas [34] and De et. al [51], $Z^k(CSP_i)$ is calculated from x_{ij}^k and $w(c_j)$ in Eq.6.6.

$$Z^k(CSP_i) = T(x_{ij}^k, w(c_j)) \tag{6.6}$$

And average of $Z^k(CSP_i)$ is as denoted as $Z(CSP_i)$, to aggregate the score of the decision makers. To evaluate the performance and rank the order of alternatives, we calculate the score function $S(C_j)$ and $S(CSP_i)$ using Eq.6.7 and Eq.6.8 respectively.

$$S_w(C_j) = \mu_w(C_j) - \pi_w(C_j) * \nu_w(C_i) \tag{6.7}$$

$$S_{CSP}(CSP_i) = \mu_z(CSP_i) - \pi_z(CSP_i) * \nu_z(CSP_i) \tag{6.8}$$

The Highest value of $S_{CSP}(CSP_i)$ gives the highest rank and lowest value gives lowest rank for that particular SLA parameter.

6.1.2.1 Interpretation of Auditors' Measurement in IFS

According to service commitment by cloud provider, we define multiple breaking points considering service credit offered by cloud provider according to service violation (e.g., see Amazon-EC2 SLA template (http://aws.amazon.com/ec2/sla). We set minimum value (min_{value}), maximum value (max_{value}) and threshold value (th_{value}) to compare

Table 6.1: Linguistic terms for the Importance of a Criteria and Performance Rating

Importance of Criteria	Performance Rating	IFNs	Measured Value
Very unimportant (VU)	Very Poor (VP)	[0.1 0.9 − π]	$<min_{value}$
Unimportant (U)	Poor (P)	[0.3 0.7 − π]	min_{value}
Medium (M)	Fair (F)	[0.5 0.5 − π]	th_{value}
Important (I)	Good(G)	[0.7 0.2 − π]	max_{value}
Very Important (VI)	Very Good (VG)	[0.9 0.1 − π]	$>max_{value}$
I do not know (N)	I do not know (N)	[0.0 0.0]	Data not received

SLA offer of cloud providers. If a measured value is greater than max_{value}, it is interpreted as Very Good (VG). If measured value is less than min_{value} it is interpreted as very poor (VP). If cloud provider does not allow to collect the service status or some parameters are missing from cloud provider, it is interpreted as I do not know (N) (See Table 6.1).

6.1.2.2 Ranking/Sorting

To select the best cloud provider among alternatives, different cloud providers are selected. Then, alternatives are assessed by a group of 4 decision makers (2 cloud auditors and 2 cloud users), based on defined SLA criteria (See Table 8.1). According to the importance of each criteria, cloud auditors and cloud users assigns the importance of weight of each parameter. All the weight ratings provided by decision makers are aggregated to common weight using Eq. 6.4. For the calculation, we have randomly selected certain weight for each decision makers based on their nature. For example most of the SLA parameters are very important for cloud auditors except *Cost* whereas *Cost* is the most important for the cloud users. In our real framework, real weight for each attributes should be defined by decision makers and obtained by means of user surveys and based on service status measured by $auditor_1$ and $auditor_2$. According to the service status of the cloud provider, and according to the service experienced by cloud user, they assign the performance rating for each alternative CSP (See Table 6.1).

6.2 Performance Heat Map Table

Selecting the appropriate cloud services and cloud providers according to the cloud users requirements is becoming a complex task, as the number of cloud providers increases. Cloud providers offer similar kinds of cloud services, but they are different in terms of price, quality of service, customer experience, and service delivery. The most challenging issue of the current cloud computing business is that cloud providers commit a certain *Service Level Agreement* (SLA), with cloud users, but there is little or no verification mechanisms which ensure that cloud providers are providing cloud services according to their commitment. In the current literature, there is a lack of an evaluation model, which provides the real status of cloud providers for the cloud users. In this paper, an evaluation model is proposed, which verifies the quality of cloud services delivered for each service and provides the service status of the cloud providers. Finally, evaluation results obtained from cloud auditors are visualized in an ordered performance heat map, showing the cloud providers in a decreasing ordering of overall service quality. In this way, the proposed service quality evaluation model represents a visual recommender system for cloud service brokers and cloud users [136].

6.2.1 CSP Selection aiding Approach

The primary goal of this work is to help cloud users and cloud brokers with selection of the best cloud providers based on the service offer, delivery and user experience according to the defined SLA criteria. We follow a decision aiding approach proposed by Bisdorff [30], which involves the following steps:

1. Sorting the potential cloud providers into marginal performance quantiles classes;

2. Ranking the providers with multiple ordinal performance criteria;

3. Sorting the performance criteria in decreasing order of correlation with the previous ranking;

4. Visualizing the results in a performance heat map, ordering the potential CSPs from the best to the worst alternative.

6.2.1.1 Sorting marginal performances into quantile classes

Let X be the set of n potential cloud providers evaluated on a single real performance criteria. We denote $x, y, ...$ the performances observed of the potential decision actions in X. We call quantile $q(p)$ the performance such that $p\%$ of the observed n performances in X are less or equal to $q(p)$. The quantile $q(p)$ is estimated by linear interpolation from the cumulative distribution of the performances in X. Consider a series: $p_k = k/q$ for $k = 0, ...q$ of $q + 1$ equally spaced quantiles, like

- *quartiles*: 0, 0.25, 0.5, 0.75, 1.0
- *quintiles*: 0, 0.2, 0.4, 0.6, 0.8, 1.0
- *deciles*: 0, 0.1, 0.2, ..., 0.9, 1.0

The upper closed[1] q^k class corresponds to the interval $]q(p_{k-1}); q(p_k)]$, for $k = 2, ..., q$, where $q(p_q) = max_X x)$ and the first class gathers all data below p_1 $:] - \infty; q(p_1)]$. We call q-tiles a complete series of $k = 1, ..., q$ q_k quantile classes. For the performance heat map visualization, we associate to each of such p^k quantile class a color from *dark red* (worst) to *dark green* (best). See for instance the color legend for 7-tiles.

6.2.1.2 *q-tiles* Sorting on a Single Criteria

If X is a measured performance, it may be distinguished in three sorting:

[1]The lower closed q_k class corresponds to the interval $[q(p_{k-1}); q(p_k)[$.

- $x \leq q(p_{k-1})$ and $x < q(p_k)$: The performance x is lower than the q^k class
- $x > q(p_{k-1})$ and $x \leq q(p_k)$: The performance x belongs to the q^k class
- $x > q(p_{k-1})$ and $x > q(p_k)$: The performance x is higher than the q^k class

If the relation $<$ is the dual of $\geq$, it will be sufficient to check that both, $q(p_{k-1}) \not\geq x$, as well as $q(p_{k-1}) \not\geq x$, are vefified for x to be a member of the $k-th$ $q-tiles$ class.

6.2.1.3 Multi-Criteria Extension

The single criteria is extended to multiple criteria by the following way:

- Let $A = \{x, y, z, ...\}$ is a finite set of n objects to be sorted
- $F = \{1, ..., m\}$ is a finite and coherent family of m performance criteria
- For each criterion j in F, the objects are evaluated on a real performance scale $[0; M_j]$, supporting an indifference threshold ind_j and a preference threshold pr_j such that $0 \leq ind_j < pr_j \leq M_j$
- The performance of object x on criterion j is denoted x_j
- Each criterion j in F carries a rational significance w_j such that $0 < w_j < 1.0$ and $\sum_{j \in F} w_j = 1.0$

6.2.1.4 Interpretation of Auditors' Measurement in Heat Map

As mentioned in IFS technique, multiple breaking points will be considered. The only difference in Heat Map technique is: ordinary level 0 to 4 will be assigned instead of IFN number (See in Table 6.2).

Table 6.2: Ordinal Level and Interpretation of auditor measurement in Ordinal Value

Linguistic terms	Ordinal Value	Measured Value
Very poor(VP)	0	$<min_{value}$
Poor (P)	1	min_{value}
Fair (F)	2	th_{value}
Good(G)	3	max_{value}
Very Good(VG)	4	$>max_{value}$
No Value	NA	Data not received

6.3 Summary

In this chapter, two performance evaluation techniques: IFL and Heat Map are introduced to evaluate the performance of commercially available cloud providers. This chapter also provides the way to assign measurement/feedback of evaluators in linguistic terms either in IFN number or in ordinary level.

Chapter 7

Evaluation

In the entire work to evaluate the performance of the cloud provider, we used the two commercially available cloud monitoring tools: Cloud Harmony [5] and Monitis [9] for the cloud service recommendation and CSP ranking and Cloud Harmony for pattern analysis of the CSPs.

7.1 Experiment Setup for Service recommendation and CSP Ranking

Figure 7.1 shows the performance measurement model to collect the performance of commercially available CSPs and feedback of the cloud users.

To include both measurable attributes and non-measurable attributes, five main performance criteria are chosen; *Availability*, *Reliability*, *Performance* as a functional criteria, *Cost* and *Security* as a non-functional criteria to measure the quality of cloud computing services as the most important requirements for the cloud users [134]. Under each main criteria, sub-criteria are defined (See Table 8.1) in both evaluation techniques.

$CloudAuditor_1$ uses CloudHarmony monitoring tool [5] and $CloudAuditor_2$ uses

Table 7.1: Criteria and Subcriteria for evaluating cloud services

Criteria	Sub-criteria	Short Name
Availability (C1)	Uptime(c11)	upT
	Downtime(c12)	dwT
	Outage Frequency(c13)	ouT
Reliability (C2)	Load Balancing(c21)	LB
	MTBF(c22)	$MTBF$
	Recoverable(c23)	Rcv
Performance (C3)	Latency(c31)	Lat
	Response time(c32)	rsT
	Throughput (c33)	tpT
Cost (C4)	Storage Cost (c41)	stC
	VM instance cost(c42)	snC
Security (C5)	Authentication (c51)	auT
	Encryption(c52)	enC
	Audit-ability(c53)	auD

Table 7.2: Internet connection between Local Test Environment and Cloud Providers

SN	Cloud Provider	Short Name	Website	Downlink (256 Kbps-10 Mbps) (Mbps)	Latency (ms)
1	Microsoft Azure	MS	https://www.azure.microsoft.com	28.15	46.5
2	GMOCloud -US	GMO	https://www.us.gmocloud.com	1.31	506
3	HP Cloud	HP	https://www.hpcloud.com	22.64	16
4	Amazone S3	Amz	https://www.aws.amazon.com/s3/	36.3	40.5
5	Rackspace	Rsp	https://www.rackspace.com	3.07	630
6	GoogleCloud Storage	Ggl	https://www.cloud.google.com	270.05	35
7	City Cloud	Cit	https://www.citycloud.com	8.62	89
8	Cloud Sigma	Sig	https://www.cloudsigma.com	24.13	215
9	Elastic Host	Ela	https://www.elastichosts.com	12.53	34
10	Centurylink	Cent	https://www.centurylinkcloud.com	254.79	36
11	Digital Ocean	Dig	https://www.digitalocean.com	4.22	190

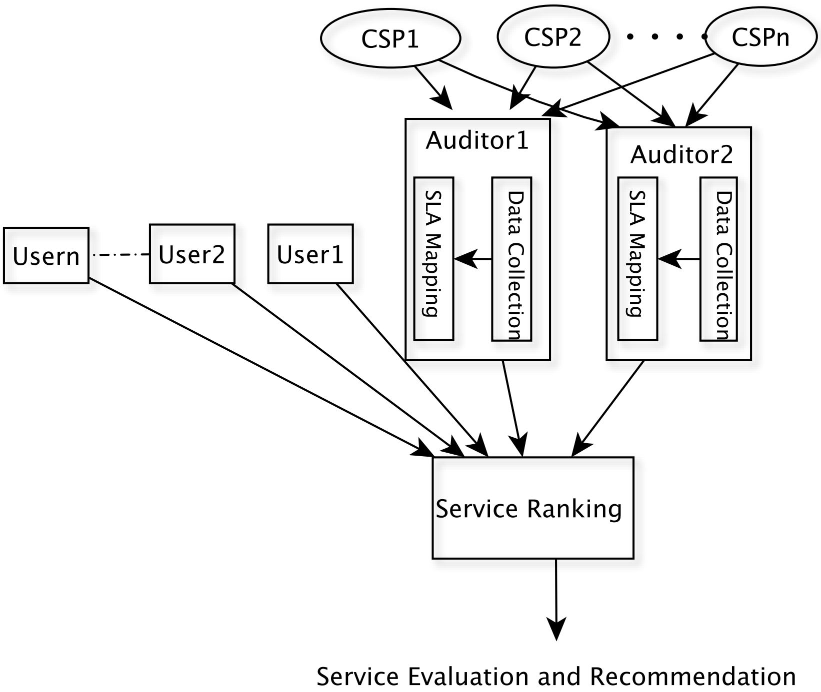


Figure 7.1: CSP Performance Measurement Model

Monitis monitoring tool [9]. Service performance is measured for all cloud users based in Luxembourg. The verification of cloud services of a cloud provider with a committed SLA is difficult because cloud providers often do not provide sufficient information in their SLA and they are not legally obliged to provide all the information in their SLA. The selected cloud providers provide only monthly uptime of service delivery.

All services are measured on the basis of SLA attributes defined in Table 8.1. Missing data are represented as 'NA'. Measurements of cloud service performance of each cloud provider are different for each cloud auditor because of different monitoring environment. In some cases the results are conflicting. The cost is directly referred from their websites. Service measurement from all selected cloud providers covers only the computing and storage services. Ranking order is based on the data gathered over a period of seven days. The actual ranking could change when considering another or longer observation period or using input from other auditors. As a result, the presented results are only for explanatory purposes and should not be considered in any case as conclusive regarding the real QoS of the service providers.

Besides the evaluations of auditors, service experience by cloud users may be similarly included in the overall evaluation of cloud providers by the way of user surveys. This part is yet to be completed in our ongoing research work [134]. In this work, performance evaluation ratings of cloud users are randomly assigned.

7.1.1 Performance Evaluation by IFL Technique

Using performance matrix assigned from decision makers from Table 7.6 and weight rating of each criteria $W(c_j)$ presented in Table 7.5, $Z(CSP_i)$ is calculated to assign the scoring value for each criteria (See Table 7.7). The corresponding values of $Z(CSP_i)$ with each SLA criteria C_j signifies the group decision provided by 4 decision makers for 3 alternative CSPs. To evaluate the performance of the CSPs, average value of all the criteria is calculated. Scoring values of each SLA criteria are calculated in Table 7.8 which provide the scoring for each SLA parameter under different CSPs. On the basis of scoring value, cloud user selects the appropriate cloud provider according to his/her requirement in each SLA parameter. Average value of $Z(CSP)$ is high in CSP *Ela* and *GMO* and low in CSP *Amz* (See Table 7.7). So, the overall ranking is of the selected CSPs is: *Amz* >*Ela* $\geq$ *GMO*. Performance Criteria *Availability*, *Performance* in CSP *Ela* *Availability*, *Cost* and *Security* in CSP *AMZ* show better performance than other. But, performance of CSP *GMO* is very low in comparision with *Ela* and *AMZ*(See Table 7.8) in most of the performances.

7.1.2 Performance Evaluation by Heat Map Technique

Unless cloud providers commit to all selected quality criteria services in their SLA, which is not the case in practice, it is not possible to provide the verification of service

Table 7.3: Service Measurement by $CloudAuditor_1$

Cloud Provider	SLA offered	SLA delivered														
		Auditor 1 (Measurement)														
		Availability (C1)			Reliability (C2)			Performance (C3)			Cost (C4)		Security (C5)			SLA Verification
	Uptime %	Uptime (c11) %	Downtime (c12) (min)	Outage (c13) (frequency)	Loadbalancing (c21)	MTBF (c22) (min)	Recoverable (c23)	Latency (c31) (ms)	Response Time (c32)(ms)	Throughput(c33) (Mbps)	Storage Cost (c41) (GB/month) $	Snapshot cost (c42) $	Authentication (c51)	Encryption (c52)	Auditability (c53)	
Microsoft Azure	99.900	100.00	2.2	1	Yes	H	G	85.41	NA	41.82	0.048	NA	Yes	Yes	Yes	V
GMOCloud -US	99.900	44.70	2.3	1	Yes	10	G	210	NA	4.24	0.17	NA	Yes	Yes	Yes	NV
HP Cloud	99.950	100.00	0	0	Yes	VH	VG	21.38	NA	40.34	0.1	0.1	Yes	Yes	Yes	V
Amazon S3	99.990	100.00	1	1	Yes	H	G	47.73	NA	40.81	0.041	NA	Yes	Yes	Yes	V
Rackspace Cloud	99.900	100.00	0	0	Yes	VH	VG	84.59	NA	38.84	0.15	0.11	Yes	Yes	Yes	V
Google Cloud	99.000	100.00	1.15	1	Yes	H	G	45.42	NA	73.59	0.01	0.13	Yes	Yes	Yes	V
City Cloud	100.000	99.97	84	3	Yes	1 day	VP	93.19	NA	9.17	0.12	0.12	Yes	Yes	Yes	NV
Cloud Sigma	99.990	100.00	16.1	1	Yes	H	G	89.2	NA	8.45	0.13	0.13	Yes	Yes	Yes	V
Elastic Host	99.990	99.97	18.52	7	Yes	18hr	VP	84.05	NA	10.07	0.1	0.03	Yes	Yes	Yes	NV
CenturylinkCloud	99.999	99.99	12.9	10	Yes	3hr	P	83.73	NA	9.44	0.15	NA	Yes	Yes	Yes	NV
Digital Ocean	99.990	100.00	0.81	3	Yes	10hr	P	90.77	NA	10.15	0.2	NA	Yes	Yes	Yes	V

Table 7.4: Service Measurement by $CloudAuditor_2$

Cloud Provider	SLA offered	SLA Delivered														
		Auditor 2(Measurement)														
		Availability (C1)			Reliability (C2)			Performance (C3)			Cost (C4)		Security (C5)			SLA Verification
	Uptime %	Uptime (c11) %	Downtime (c12) (min)	Outage (c13) (frequency)	Loadbalancing (c21)	MTBF (c22) (min)	Recoverable (c23)	Latency (c31) (ms)	Response Time (c32)(ms)	Throughput (C33)(Mbps)	Storage Cost (c41) (GB/month) $	Snapshot cost (c42) $	Authentication (c51)	Encryption (c52)	Auditability (c53)	
Microsoft Azure	99.900	100	0	0	Yes	VH	VG	NA	179.6	NA	0.05	NA	Yes	Yes	Yes	V
GMOCloud -US	99.900	98.9	5	4	Yes	H	F	NA	282.1	NA	0.17	NA	Yes	Yes	Yes	NV
HP Cloud	99.950	99.9	3	2	Yes	VH	G	NA	176.49	NA	0.1	0.1	Yes	Yes	Yes	NV
Amazon S3	99.990	98.8	8	6	Yes	H	G	NA	505.71	NA	0.04	NA	Yes	Yes	Yes	NV
Rackspace Cloud	99.900	NA	NA	NA	Yes	NA	G	NA	NA	NA	0.15	0.11	Yes	Yes	Yes	V
Google Cloud	99.000	99.8	38	10	Yes	1day	G	NA	1190	NA	0.01	0.13	Yes	Yes	Yes	V
City Cloud	100.000	99.9	1	2	Yes	H	VG	NA	950.33	NA	0.12	0.12	Yes	Yes	Yes	NV
Cloud Sigma	99.990	100	0	0	Yes	VH	VG	NA	456.76	NA	0.13	0.13	Yes	Yes	Yes	V
Elastic Host	99.990	100	0	0	Yes	VH	VG	NA	59.81	NA	0.1	0.03	Yes	Yes	Yes	V
CenturylinkCloud	99.999	100	0	0	Yes	VH	VG	NA	949.91	NA	0.15	NA	Yes	Yes	Yes	V
Digital Ocean	99.990	99.3	35	5	Yes	1hr	G	NA	777.47	NA	0.2	NA	Yes	Yes	Yes	NV

Table 7.5: The ratings of importance weight of each criteria by decision makers

Criteria	Sub-criteria	Auditor1	Auditor2	User1	User2	w(cj)	W(cj)
Availability(C1)	Uptime(c11)	VI(0.0)	VI(0.0)	I(0.1)	M(0.1)	[0.5,0.4]	[0.5,0.5]
	Downtime(c11)	VI(0.0)	VI(0.0)	I(0.1)	M(0.1)	[0.5,0.4]	
	Outage(c13)	VI(0.0)	VI(0.0)	I(0.1)	M(0.0)	[0.5,0.5]	
Reliablity(C2)	Loadbalancing(c21)	VI(0.0)	VI(0.0)	I(0.0)	I(0.2)	[0.7,0.3]	[0.5,0.4]
	MTTB(c22)	VI(0.0)	VI(0.0)	I(0.0)	I(0.0)	[0.7,0.3]	
	Recoverable(c23)	VI(0.0)	VI(0.0)	I(0.0)	M(0.1)	[0.5,0.4]	
Performance(C3)	Latency(c31)	VI(0.0)	VI(0.0)	I(0.0)	M(0.0)	[0.5,0.5]	[0.5,0.5]
	Responsetime(c32)	VI(0.0)	VI(0.0)	I(0.1)	I(0.0)	[0.7, 0.3]	
	Throughput(c33)	VI(0.0)	VI(0.0)	VI(0.0)	VI(0.0)	[0.9,0.1]	
Cost(C4)	Installation cost(c41	U(0.1)	U(0.1)	VI(0.0)	VI(0.0)	[0.3,0.6]	[0.3,0.6]
	Running cost(c42)	U(0.1)	U(0.1)	VI(0.0)	VI(0.0)	[0.3,0.6]	
Security(C5)	Authentication(51)	VI(0.0)	VI(0.0)	M(0.1)	M(0.1)	[0.5,0.4]	[0.3,0.7]
	Encryption(c52)	I(0.0)	U(0.1)	U(0.1)	U(0.0)	[0.3,0.7]	
	Auditability(c53)	VI(0.0)	VI(0.0)	M(0.2)	U(0.1)	[0.3,0.6]	

Table 7.6: Performance Matrix

Performance Evaluator	Cloud Provider	Performance Measurement													
		Availability (C1)			Reliability (C2)			Performance (C3)			Cost (C4)		Security (C5)		
		Uptime (c11) %	Downtime (c12) (min)	Outage (c13) (frequency)	Loadbalancing (c21)	MTBF (c22) (min)	Recoverable (c23)	Latency (c31) (ms)	Response Time (c32)(ms)	Throughput (c33) (Mbps)	Storage Cost (c41) (GB/month) $	Snapshot cost (c42) $	Authentication (c51)	Encryption (c52)	Auditability (c53)
Auditor1	Amazon S3	VG(0,0)	P(0,0)	G(0,0)	VG(0,0)	G(0,0)	G(0,0)	VG(0,0)	N(0,0)	VG(0,0)	VG(0,0)	N(0,0)	VG(0,0)	VG(0,0)	VG(0,0)
	GMOCloud -US	VP(0,0)	G(0,0)	G(0,0)	VG(0,0)	P(0,0)	G(0,0)	F(0,0)	N(0,0)	P(0,0)	G(0,0)	N(0,0)	VG(0,0)	VG(0,0)	VG(0,0)
	Elastic Host	VG(0,0)	F(0,0)	G(0,0)	VG(0,0)	F(0,0)	P(0,0)	G(0,0)	N(0,0)	F(0,0)	G(0,0)	VG(0,0	VG(0,0)	VG(0,0)	VG(0,0)
Auditor2	Amazon S3	F(0,0)	F(0,0)	P(0,0)	VG(0,0)	G(0,0)	G(0,0)	N(0,0)	G(0,0)	N(0,0)	VG(0,0)	N(0,0)	VG(0,0)	VG(0,0)	VG(0,0)
	GMOCloud -US	P(0,0)	G(0,0)	G(0,0)	VG(0,0)	G(0,0)	F(0,0)	N(0,0)	VG(0,0)	N(0,0)	G(0,0)	N(0,0)	VG(0,0)	VG(0,0)	VG(0,0)
	Elastic Host	VG(0,0)	VG(0,0)	VG(0,0)	VG(0,0)	VG(0,0)	VG(0,0)	N(0,0)	VG(0,0)	N(0,0)	VG(0,0)	G(0,0)	VG(0,0)	VG(0,0)	VG(0,0)
User1	Amazon S3	P(0,1)	F(0,2)	G(0,0)	G(0,0)	VP(0,1)	VG(0,0)	G(0,1)	G(0,0)	VG(0,0)	G(0.0)	G(0.1)	F(0.0)	G(0.0)	G(0.0),
	GMOCloud -US	G(0.0)	VG(0.0)	G(0,0)	P(0,0)	P(0.1)	G(0.1)	F(0.1)	G(0.0)	VG(0.0)	F(0.0)	F(0.2)	G(0.1)	VG(0.0)	F(0.0)
	Elastic Host	F(0.0)	G(0.0)	G(0,0)	F(0,0)	VG(0.1)	G(0.1)	G(0.0)	VG(0.0)	VG(0.0)	G(0.0)	G(0.0)	F(0.1)	VP(0.1)	VP(0.1)
User2	Amazon S3	VG(0.0)	VG(0.0)	P(0,0)	G(0,0)	P(0.1)	G(0.1)	G(0.0)	VG(0.0)	VG(0.0	VG(0.0)	G(0.0)	G(0.1)	F(0.1)	F(0.0)
	GMOCloud -US	G(0.1)	F(0.0)	G(0,0)	G(0,0)	VP(0.1)	F(0.0)	VG(0.0)	P(0.1)	VG(0.0)	P(0.0)	F(0.0)	VG(0.0)	G(0.0)	G(0.1)
	Elastic Host	G(0.1)	G(0.0)	VG(0,0)	VG(0,0)	F(0.1)	G(0.0)	VG(0.0)	F(0.2)	VG(0.0)	G(0.0)	P(0.0)	VG(0.0)	VG(0.0)	G(0.0)

Table 7.7: Decision Matrix $Z(CSP_i)$

	AMZ	GMO	Ela
Auditor1	[0.9, 0.1]	[0.7, 0.3]	[0.7, 0.3]
Auditor2	[0.7, 0.1]	[0.7, 0.1]	[0.7, 0.1]
User1	[0.9, 0.1]	[0.9, 0.1]	[0.9, 0.1]
User2	[0.9, 0.1]	[0.9, 0.1]	[0.9, 0.1]
Avg	$[0.249925, 3.0e^{-10}]$	$[0.249775, 7.5e^{-5}]$	$[0.249775, 7.5e^{-5}]$

Table 7.8: Scoring Value for CSP based on SLA Paramters $S_{W(C_j)}$

Amz					*GMO*					*Ela*				
C1	C2	C3	C4	C5	C1	C2	C3	C4	C5	C1	C2	C3	C4	C5
0.196	0.179	0.125	0.237	0.2049	0.1098	0.138	0.142	0.044	0.145	0.219	0.215	0.175	0.161	0.12

criteria	**tpt**	**upT**	**MTBF**	**Lat**	**Rcv**	**ouT**	**dwT**	**stC**	**auD**	**enC**	**auT**	**snC**	**rsT**	**LB**
weights	2.00	2.00	2.00	2.00	2.00	2.00	2.00	3.00	2.00	2.00	2.00	3.00	2.00	2.00
tau(*)	0.62	0.59	0.54	0.45	0.43	0.43	0.43	0.36	0.00	0.00	0.00	0.00	0.00	0.00
Amz	4	4	3	4	3	3	3	4	4	4	4	NA	NA	4
MS	4	4	3	3	3	3	3	4	4	4	4	NA	NA	4
HP	4	4	4	4	4	4	4	3	4	4	4	4	NA	4
Rsp	4	4	4	3	4	4	4	3	4	4	4	4	NA	4
Ggl	4	4	3	4	3	3	3	4	4	4	4	4	NA	4
Sig	2	4	3	3	3	3	2	3	4	4	4	4	NA	4
Dig	2	4	3	3	2	2	0	3	4	4	4	NA	NA	4
Ela	2	2	3	3	1	1	2	3	4	4	4	4	NA	4
Cent	2	2	2	3	2	0	1	3	4	4	4	NA	NA	4
Cit	2	1	2	3	1	2	0	3	4	4	4	4	NA	4
GMO	1	0	1	2	3	3	3	3	4	4	4	NA	NA	4

Color legend:

quantile	0.14%	0.29%	0.43%	0.57%	0.71%	0.86%	1.00%

(*) tau: Ordinal (Kendall) correlation of marginal criterion and global outranking relation.

Figure 7.2: Heat map table by Auditor 1

delivery for all SLA parameters. Instead of that, we propose an evaluation model to provide the status of commercial available cloud providers as a performance heat map. The visual performance heat map is used to recommend the cloud services to the cloud brokers and cloud users.

On each criteria we thus associate to the performance x of a cloud provider the color of the $q$tiles class to which belongs x. In Fig 7.12 again, we may thus ob-

Table 7.9: Service Measurement by $CloudAuditor_2$

Cloud Provider	SLA offered	SLA Delivered														
		Auditor 2(Measurement)														
		Availability (C1)			Reliability (C2)			Performance (C3)			Cost (C4)		Security (C5)			SLA Verification
	Uptime %	Uptime (c11) %	Downtime (c12) (min)	Outage (c13) (frequency)	Loadbalancing (c21)	MTBF (c22) (min)	Recoverable (c23)	Latency (c31) (ms)	Response Time (c32)(ms)	Throughput (C33)(Mbps)	Storage Cost (c41) (GB/month) $	Snapshot cost (c42) $	Authentication (c51)	Encryption (c52)	Auditability (c53)	
Microsoft Azure	99.900	100	0	0	Yes	VH	VG	NA	179.6	NA	0.05	NA	Yes	Yes	Yes	V
GMOCloud -US	99.900	98.9	5	4	Yes	H	F	NA	282.1	NA	0.17	NA	Yes	Yes	Yes	NV
HP Cloud	99.950	99.9	3	2	Yes	VH	G	NA	176.49	NA	0.1	0.1	Yes	Yes	Yes	NV
Amazon S3	99.990	98.8	8	6	Yes	H	G	NA	505.71	NA	0.04	NA	Yes	Yes	Yes	NV
Rackspace Cloud	99.900	NA	NA	NA	Yes	NA	G	NA	NA	NA	0.15	0.11	Yes	Yes	Yes	V
Google Cloud	99.000	99.8	38	10	Yes	1day	G	NA	1190	NA	0.01	0.13	Yes	Yes	Yes	V
City Cloud	100.000	99.9	1	2	Yes	H	VG	NA	950.33	NA	0.12	0.12	Yes	Yes	Yes	NV
Cloud Sigma	99.990	100	0	0	Yes	VH	VG	NA	456.76	NA	0.13	0.13	Yes	Yes	Yes	V
Elastic Host	99.990	100	0	0	Yes	VH	VG	NA	59.81	NA	0.1	0.03	Yes	Yes	Yes	V
CenturylinkCloud	99.999	100	0	0	Yes	VH	VG	NA	949.91	NA	0.15	NA	Yes	Yes	Yes	V
Digital Ocean	99.990	99.3	35	5	Yes	1hr	G	NA	777.47	NA	0.2	NA	Yes	Yes	Yes	NV

Table 7.10: Service Mapping to ordinal value measurement by $CloudAuditor_1$

Cloud Provider	SLA offered	SLA delivered														
		Auditor 1 (Mapped)														
		Availability (C1)			Reliability (C2)			Performance (C3)			Cost (C4)		Security (C5)			SLA Verification
	Uptime %	Uptime (c11) %	Downtime (c12) (min)	Outage (c13) (frequency)	Loadbalancing (c21)	MTBF (c22) (min)	Recoverable (c23)	Latency (c31) (ms)	Response Time (c32)(ms)	Throughput (c33) (Mbps)	Storage Cost (c41) (GB/month) $	Snapshot cost (c42) $	Authentication (c51)	Encryption (c52)	Auditability (c53)	
Microsoft Azure	99.900	4.00	3	3	4	3	3	3	NA	4	4	NA	4	4	4	V
GMOCloud -US	99.900	0.00	3	3	4	1	3	2	NA	1	3	NA	4	4	4	NV
HP Cloud	99.950	4.00	4	4	4	4	4	4	NA	4	3	4	4	4	4	V
Amazon S3	99.990	4.00	3	3	4	3	3	4	NA	4	4	NA	4	4	4	V
Rackspace Cloud	99.900	4.00	4	4	4	4	4	3	NA	4	3	4	4	4	4	V
Google Cloud	99.000	4.00	3	3	4	3	3	4	NA	4	4	4	4	4	4	V
City Cloud	100.00	1.00	0	2	4	2	1	3	NA	2	3	4	4	4	4	NV
Cloud Sigma	99.990	4.00	2	3	4	3	3	3	NA	2	3	4	4	4	4	V
Elastic Host	99.990	2.00	2	1	4	3	1	3	NA	2	3	4	4	4	4	NV
CenturylinkCloud	99.999	2.00	1	0	4	2	2	3	NA	2	3	NA	4	4	4	NV
Digital Ocean	99.990	4.00	0	2	4	3	2	3	NA	2	3	NA	4	4	4	V

Table 7.11: Service Mapping to ordinal value measurement by $CloudAuditor_2$

Cloud Provider	SLA offered	SLA Delivered														
		Auditor 2(Mapped))														
		Availability (C1)			Reliability (C2)			Performance (C3			Cost (C4)		Security (C5)			SLA Verification
	Uptime %	Uptime (c11) %	Downtime (c12) (min)	Outage (c13) (frequency)	Loadbalancing (c21)	MTBF (c22) (min)	Recoverable (c23)	Latency (c31) (ms)	Response Time (c32)(ms)	Throughput (c33) (Mbps)	Storage Cost (c41) (GB/month) $	Snapshot cost (c42) $	Authentication (c51)	Encryption (c52)	Auditability (c53)	
Microsoft Azure	99.900	4	4	4	4	4	4	NA	4	NA	4	NA	4	4	4	V
GMOCloud -US	99.900	1	3	3	4	3	2	NA	4	NA	3	NA	4	4	4	NV
HP Cloud	99.950	3	3	3	4	4	3	NA	4	NA	3	4	4	4	4	NV
Amazon S3	99.990	2	2	2	4	3	3	NA	3	NA	4	NA	4	4	4	NV
Rackspace Cloud	99.900	NA	NA	NA	4	NA	3	NA	NA	NA	3	4	4	4	4	V
Google Cloud	99.000	4	1	1	4	2	3	NA	2	NA	4	4	4	4	4	V
City Cloud	100.00	3	3	3	4	3	4	NA	2	NA	3	4	4	4	4	NV
Cloud Sigma	99.990	4	4	4	4	4	4	NA	3	NA	3	4	4	4	4	V
Elastic Host	99.990	4	4	4	4	4	4	NA	4	NA	3	4	4	4	4	V
CenturylinkCloud	99.999	4	4	4	4	4	4	NA	2	NA	3	NA	4	4	4	V
Digital Ocean	99.990	2	1	1	4	2	3	NA	2	NA	3	NA	4	4	4	NV

serve that, for $CloudAuditor_1$, providers Amz, MS, HP, *Rsp* and *Ggl* show on sub-criteria *tpT*:*Performance*, Amz, MS, HP, *Rsp*, *Ggl*, *Sig* and *Dig* show on sub-criteria *upT*:*Availability*, HP and *Rsp* show on sub-criteria $MTBF$:*Reliability*, Amz, HP and *Ggl* show on sub-criteria *Lat*:*Performance* the best performance (4), whereas cloud provider GMO shows the worst performance in all the cases but cloud provider GMO shows worst performance only on sub-criteria *Rcv*:*Reliability* observed by $Auditor_2$ (see Fig 7.15). Similarly, in Fig. 8.3 we observed that, for combining result of both auditors, providers MS, AMZ, HP, *Ggl* and *Rsp* show on sub-criteria *tpT*:*Performance*, HP and *Rsp* show on sub-criteria $MTBF$:*Reliability*, Amz, HP and *Ggl* show on sub-criteria *Lat*:*Performance*, MS, Amz, HP, *Ggl*, *Rsp*, *Sig* and *Gig* show on sub-criteria *upT*:*Availability* and MS, $Cent$, *Sig*, *Ela* and *Cit* show on sub-criteria *Rcv*:*Reliability* the best performance (4), whereas provider GMO shows the worst performance in all the cases.

It is worthwhile mentioning that the quantiles sorting result has not to be taken as a kind of service rating. When observing in the heat map table that a CSP is evaluated best on a criteria, this only means that its performance is to be considered best relatively to the actually given set of potentially available CSPs. That is why, in case of identical evaluation of all potential CSPs, the performance is sorted into the best quantile for all of them (see last rows in Fig 7.12, 7.15 and 8.3).

7.1.3 Multi-Criteria Ranking of the CSPs

In Fig 7.12 and 7.15, the CSPs appear ranked in decreasing order from the overall best to overall worst performing. This overall ranking is computed from bipolar outranking situations [28], where we consider that an alternative x *outranks* an alternative y when there is a *significant majority of criteria* that warrant a '*better than*' relation between them **and** there is no *considerable counter-performance* observed between when considering x in place of y.

When computing these outranking relation, we consider the five main performance criteria, namely *Availability*, *Reliability*, *Performance*, *Cost* and *Security* to be equally important; and all sub-criteria within each criterion are considered to be equi-significant. All criteria has the three sub-criteria except $Cost(C_4)$. Weights are assigned to each sub-criteria to make equally significant for all criteria (see second row in Fig 7.12, 7.15 and 8.3). Thus we obtain the following set of significance weights of the criteria and sub-criteria:

$w_A = w_{c11} + w_{c12} + w_{c13} = w_R = w_{c21} + w_{c22} + w_{c23} = w_P = w_{c31} + w_{c32} + w_{c33} = w_C = w_{c41} + w_{c42} = w_S = w_{c51} + w_{c52} + w_{c53}$ where wc_{ij} represents the significance weight assigned to sub-criterion j under criterion i.

Considering eleven potential commercial cloud providers, alternative AMZ is ranked as the highest ranked cloud provider by $CloudAuditor_1$, whereas MS is ranked as the highest ranked cloud provider by $CloudAuditor_2$ (see Fig 7.12 and 7.15), whereas the alternative GMO, respectively Dig, is ranked lowest by $CloudAuditor_1$, respectively $CloudAuditor_2$. Equally spaced 7 quantiles are considered in these heat maps, where, as mentioned before, dark green color indicates the relatively highest performance, whereas dark red indicates the relatively lowest performance. Collective ranking of the potential eleven cloud providers is shown in Fig 8.3 by grouping the evaluations of the two cloud auditors. In the collective ranking, evidently alternative MS is the highest ranked cloud provider, whereas cloud provider alternative GMO is the lowest ranked.

7.2 Service Verification

For the service verification, the measured value for criteria C_1 (see Table 7.3 and Table 7.9) is used, as all the selected cloud providers offer monthly uptime in SLA commitment. Measured value for criteria C_1 is mapped to criterion *Availability* and compared with SLA offered by cloud providers. A value with red background shows

criteria	ouT	dwT	MTBF	upT	Rcv	rsT	auD	enC	auT	snC	tpT	Lat	LB	stC
weights	2.00	2.00	2.00	2.00	2.00	2.00	2.00	2.00	2.00	3.00	2.00	2.00	2.00	3.00
tau(*)	0.75	0.70	0.60	0.55	0.53	0.42	0.00	0.00	0.00	0.00	0.00	0.00	0.00	-0.07
MS	4	4	4	4	4	4	4	4	4	NA	NA	NA	4	4
Cent	4	4	4	4	4	4	4	4	4	NA	NA	NA	4	3
Ela	4	4	4	4	4	4	4	4	4	4	NA	NA	4	3
Sig	4	4	4	4	4	3	4	4	4	4	NA	NA	4	3
Cit	3	4	3	3	4	2	4	4	4	4	NA	NA	4	3
HP	3	3	4	3	3	4	4	4	4	4	NA	NA	4	3
Rsp	NA	NA	NA	NA	3	NA	4	4	4	4	NA	NA	4	3
GMO	3	3	3	1	2	4	4	4	4	NA	NA	NA	4	3
Ggl	1	1	2	4	3	2	4	4	4	4	NA	NA	4	4
Amz	2	2	3	2	3	3	4	4	4	NA	NA	NA	4	4
Dig	1	1	2	2	3	2	4	4	4	NA	NA	NA	4	3

Color legend:

quantile	0.14%	0.29%	0.43%	0.57%	0.71%	0.86%	1.00%

(*) tau: Ordinal (Kendall) correlation of marginal criterion and global outranking relation.

Figure 7.3: Heat map table by Auditor 2

criteria	tpT	MTBF	Lat	stC	stC	upT	upT	dwT	MTBF	Rcv	rsT	ouT	Rcv	ouT	dwT	auD	enC	auT	snC	tpT	Lat	LB	auD	enC	auT	snC	rsT	LB
weights	2.00	2.00	2.00	3.00	3.00	2.00	2.00	2.00	2.00	2.00	2.00	2.00	2.00	2.00	2.00	2.00	2.00	2.00	3.00	2.00	2.00	2.00	2.00	2.00	2.00	3.00	2.00	2.00
tau(*)	0.50	0.48	0.38	0.36	0.36	0.33	0.32	0.31	0.29	0.23	0.20	0.18	0.16	0.15	0.09	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
MS	4	3	3	4	4	4	4	3	4	3	4	4	4	3	4	4	4	4	NA	NA	NA	4	4	4	4	NA	NA	4
Amz	4	3	4	4	4	4	2	3	3	3	3	2	3	3	2	4	4	4	NA	NA	NA	4	4	4	4	NA	NA	4
Cent	2	3	3	3	3	2	4	1	4	2	4	4	4	0	4	4	4	4	NA	NA	NA	4	4	4	4	NA	NA	4
HP	4	4	4	3	3	4	3	4	4	4	4	3	3	4	3	4	4	4	4	NA	NA	4	4	4	4	4	NA	4
Ggl	4	3	4	4	4	4	4	3	2	3	2	1	3	3	1	4	4	4	4	NA	NA	4	4	4	4	4	NA	4
Rsp	4	4	3	3	3	4	NA	4	NA	4	NA	NA	3	4	NA	4	4	4	4	NA	NA	4	4	4	4	4	NA	4
Sig	2	3	3	3	3	4	4	2	4	3	3	4	4	3	4	4	4	4	4	NA	NA	4	4	4	4	4	NA	4
Ela	2	2	3	3	3	2	4	2	4	1	4	4	4	1	4	4	4	4	4	NA	NA	4	4	4	4	4	NA	4
Cit	2	2	3	3	3	1	3	0	3	1	2	3	4	2	4	4	4	4	4	NA	NA	4	4	4	4	4	NA	4
Dig	2	2	3	3	3	4	2	0	2	2	2	1	3	2	1	4	4	4	NA	NA	NA	4	4	4	4	NA	NA	4
GMO	1	1	2	3	3	0	1	3	3	3	4	3	2	3	3	4	4	4	NA	NA	NA	4	4	4	4	NA	NA	4

Color legend:

quantile	0.14%	0.29%	0.43%	0.57%	0.71%	0.86%	1.00%

(*) tau: Ordinal (Kendall) correlation of marginal criterion and global outranking relation.

Figure 7.4: Heat map table by All Auditors

the non-compliance of an SLA and is a subject to penalty for SLA violation. '*V*' represents a positive verification of a service and '*NV*' represents the negative verification of services. In data observed by $CloudAuditor_1$; *GMOCloud-US*, *City Cloud*, *Elastic Host* and *Centurylink Cloud* did not comply the service commitment as stated in their SLA. There is a significant gap between service offer and service delivered in *GMOCloud-US* and a comparatively less sever violation in the cases of *City Cloud* and *Elastic Host*. The difference is little for *Centurylink Cloud*, but it still did not manage to comply with its SLA. Similarly, *GMOCloud-US*, *HP Cloud*, *Amazon S3 City Cloud* and *Digital Ocean* did not comply the service commitment in service observation by $CloudAuditor_2$. There is a significant difference in offered SLA and delivered availability in *GMOCloud-US*, *Amazon S3* and *Digital Ocean* but it is less significant in *HP Cloud* and *City Cloud*.

7.3 Comparisons of Two Techniques

In this section, we present the comparisons of our two approaches: Instuitionistic Fuzzy Logic (IFL), formulated in [134], initially proposed by Wang [11] for web service selection, and Heat Map Performance Table to evaluate commercially available CSPs based on service performance delivered by them [136]. For the CSP evaluation, we collect the service delivery performance of CSPs using commercially available service monitoring tools. All the SLA offers provided by CSPs are not directly measurable. To include all the measurable and non-measurable parameters while evaluating performance of CSPs, we include CSUs feedback to include non-measurable parameters. In comparison of two performance evaluation approaches, however, IFL evaluation technique can provide the confidentially of their feedback to the CSP evaluation system, Heat Map Table is found better and easy to implement in current cloud service brokering to recommend the cloud services to the users. As IFL technique is not flexible for the multiple alterna-

Table 7.12: Performance Evaluation by $CloudAuditor_1$

criteria	tpT	Lat	upT	stC	MTBF	auD	enC	auT	snC	rsT	Rcv	LB	ouT	dwT
weights	2.00	2.00	2.00	1.00	2.00	1.00	1.00	1.00	2.00	2.00	2.00	2.00	2.00	2.00
tau(*)	1.00	1.00	1.00	0.67	0.67	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Amz	4	4	4	4	3	4	4	4	NA	NA	3	4	3	3
Ela	2	3	2	3	3	4	4	4	4	NA	1	4	1	2
GMO	1	2	0	3	1	4	4	4	NA	NA	3	4	3	3

Color legend:

quantile	0.14%	0.29%	0.43%	0.57%	0.71%	0.86%	1.00%

(*) tau: Ordinal (Kendall) correlation between marginal criterion and global ranking relation.

Table 7.13: Performance Evaluation by $CloudAuditor_2$

criteria	ouT	dwT	rsT	MTBF	Rcv	upT	auD	enC	auT	snC	tpT	Lat	LB	stC
weights	2.00	2.00	2.00	2.00	2.00	2.00	1.00	1.00	1.00	2.00	2.00	2.00	2.00	2.00
tau(*)	1.00	1.00	0.67	0.67	0.33	0.33	0.00	0.00	0.00	0.00	0.00	0.00	0.00	-0.67
Ela	4	4	4	4	4	4	4	4	4	4	NA	NA	4	3
GMO	3	3	4	3	2	1	4	4	4	NA	NA	NA	4	3
Amz	2	2	3	3	3	2	4	4	4	NA	NA	NA	4	4

Color legend:

quantile	0.14%	0.29%	0.43%	0.57%	0.71%	0.86%	1.00%

(*) tau: Ordinal (Kendall) correlation between marginal criterion and global ranking relation.

tives [137], we chose three CSPs for the comparisons of two techniques: *Amz*, *Ela* and *GMO*.

In the overall evaluation including all auditors and cloud users in Figure 7.17, weights are assigned to each sub-criteria to make equally significant with weight assigned in IFL evaluation (See Table 7.5) to make comparable with both techniques. Average weights are assigned for combined evaluations of all cloud auditors and users. We obtain the following sets of significance weights of the criteria and sub-criteria for cloud auditors and users:

1. For cloud auditors

   $w_A = w_{c11}+w_{c12}+w_{c13} = 6.0$; $w_R = w_{c21}+w_{c22}+w_{c23} = 6.0$; $w_P = w_{c31}+w_{c32}+w_{c33} =$

Table 7.14: Performance Evaluation by $User_1$

criteria	dwT	upT	auT	enC	rsT	MTBF	tpT	ouT	auD	snC	stC	Lat	Rcv	LB
weights	2.00	2.00	1.00	1.00	2.00	2.00	2.00	2.00	1.00	2.00	1.00	2.00	2.00	2.00
tau(*)	1.00	1.00	0.67	0.33	0.33	0.33	0.00	0.00	-0.20	-0.67	-0.67	-0.67	-0.67	-1.00
Amz	4	3	3	4	3	1	4	3	2	2	2	2	3	1
Ela	3	2	2	0	4	4	4	3	0	3	3	3	3	2
GMO	2	0	2	3	0	0	4	3	3	3	3	3	4	3

Color legend:

quantile	0.14%	0.29%	0.43%	0.57%	0.71%	0.86%	1.00%

(*) tau: Ordinal (Kendall) correlation between marginal criterion and global ranking relation.

Table 7.15: Performance Evaluation by $User_2$

criteria	MTBF	Rcv	LB	enC	stC	rsT	ouT	dwT	auD	auT	tpT	Lat	upT	snC
weights	2.00	2.00	2.00	1.00	1.00	2.00	2.00	2.00	1.00	1.00	2.00	2.00	2.00	2.00
tau(*)	1.00	0.67	0.67	0.33	0.33	0.33	0.33	0.33	0.00	0.00	0.00	0.00	0.00	-0.33
Ela	2	3	4	4	3	2	4	3	3	4	4	4	3	1
GMO	1	3	3	2	4	4	1	4	2	3	4	3	4	3
Amz	0	2	3	3	1	1	3	2	3	4	4	4	3	2

Color legend:

quantile	0.14%	0.29%	0.43%	0.57%	0.71%	0.86%	1.00%

(*) tau: Ordinal (Kendall) correlation between marginal criterion and global ranking relation.

Table 7.16: Performance Evaluation by all Auditors

criteria	tpT	Lat	MTBF	upT	stC	stC	Rcv	upT	auD	enC	auT	snC	tpT	Lat
weights	2.00	2.00	2.00	2.00	2.00	2.00	2.00	2.00	1.00	1.00	1.00	2.00	2.00	2.00
tau(*)	1.00	1.00	1.00	1.00	0.67	0.67	0.33	0.33	0.00	0.00	0.00	0.00	0.00	0.00
Amz	4	4	3	4	4	4	3	2	4	4	4	NA	NA	NA
Ela	2	3	2	2	3	3	4	4	4	4	4	4	NA	NA
GMO	1	2	1	0	3	3	2	1	4	4	4	NA	NA	NA

criteria	MTBF	LB	auD	enC	auT	snC	rsT	Rcv	LB	ouT	dwT	ouT	dwT	rsT
weights	2.00	2.00	2.00	1.00	1.00	2.00	2.00	2.00	2.00	2.00	2.00	2.00	2.00	2.00
tau(*)	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	-0.33	-0.33	-0.67
Amz	3	4	4	4	4	NA	NA	3	4	3	3	2	2	3
Ela	4	4	4	4	4	4	NA	1	4	1	2	4	4	4
GMO	3	4	4	4	4	NA	NA	3	4	3	3	3	3	4

Color legend:

quantile	0.14%	0.29%	0.43%	0.57%	0.71%	0.86%	1.00%

(*) tau: Ordinal (Kendall) correlation between marginal criterion and global ranking relation.

Table 7.17: Performance Evaluation of All Auditors and Users

criteria	dwT	upT	tpT	Lat	MTBF	upT	auD	enC	auT	Lat	upT	auT	stC	stC	ouT	enC	rsT	MTBF	Rcv	upT	tpT	LB	tpT	ouT	auD	enC	auT	snC
weights	1.75	1.75	1.50	1.50	1.50	1.75	1.00	1.00	1.00	1.50	1.75	1.00	2.00	2.00	1.75	1.00	1.50	1.50	1.50	1.75	1.50	1.50	1.50	1.75	1.00	1.00	2.00	2.00
tau(*)	1.00	1.00	1.00	1.00	1.00	1.00	0.67	0.67	0.67	0.67	0.67	0.67	0.67	0.67	0.33	0.33	0.33	0.33	0.33	0.33	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Amz	4	3	4	4	3	4	3	4	4	4	3	3	4	4	3	4	3	1	3	2	4	3	4	3	4	4	4	NA
Ela	3	2	2	3	2	2	3	4	4	4	3	2	3	3	4	0	4	4	4	4	4	4	4	3	4	4	4	4
GMO	2	0	1	2	1	0	2	2	3	3	1	2	3	3	1	3	0	0	2	1	4	3	4	3	4	4	4	NA

	tpT	Lat	MTBF	LB	auD	enC	auT	snC	rsT	Rcv	LB	ouT	dwT	snC	MTBF	auD	ouT	dwT	Rcv	dwT	stC	Lat	Rcv	rsT	stC	rsT	snC	LB
	1.50	2.00	1.50	1.50	1.00	1.00	1.00	2.00	1.50	1.50	1.50	1.75	1.75	2.00	1.50	1.00	1.75	1.75	1.50	1.75	2.00	1.50	1.50	1.50	2.00	1.50	2.00	1.50
	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	-0.33	-0.33	-0.33	-0.33	-0.33	-0.67	-0.67	-0.67	-0.67	-0.67	-0.67	-1.00	-1.00	-1.00	-1.00
	NA	NA	3	4	4	4	4	NA	NA	3	4	3	3	2	0	2	2	2	2	2	2	2	3	3	1	1	2	1
	NA	NA	4	4	4	4	4	4	NA	1	4	1	2	1	2	0	4	4	3	3	3	3	3	4	3	2	3	2
	NA	NA	3	4	4	4	4	NA	NA	3	4	3	3	3	1	3	3	3	3	3	3	3	4	4	4	4	4	3

Color legend:

quantile	0.14%	0.29%	0.43%	0.57%	0.71%	0.86%	1.00%

(*) tau: Ordinal (Kendall) correlation between marginal criterion and global ranking relation.

$6.0; w_C = w_{c41} + w_{c42} = 4.0;\ w_S = w_{c51} + w_{c52} + w_{c53} = 3.0$

2. For $user_1$

   $w_A = w_{c11}+w_{c12}+w_{c13} = 3.0;\ w_R = w_{c21}+w_{c22}+w_{c23} = 3.0;\ w_P = w_{c31}+w_{c32}+w_{c33} = 3.0; w_C = w_{c41} + w_{c42} = 4.0;\ w_S = w_{c51} + w_{c52} + w_{c53} = 3.0$

3. For $user_2$

   $w_A = w_{c11}+w_{c12}+w_{c13} = 6.0;\ w_R = w_{c21}+w_{c22}+w_{c23} = 3.0;\ w_P = w_{c31}+w_{c32}+w_{c33} = 3.0; w_C = w_{c41} + w_{c42} = 4.0;\ w_S = w_{c51} + w_{c52} + w_{c53} = 3.0$

4. Average of cloud auditors and users for combined evaluations

   $w_A = w_{c11}+w_{c12}+w_{c13} = 5.25;\ w_R = w_{c21}+w_{c22}+w_{c23} = 4.5;\ w_P = w_{c31}+w_{c32}+w_{c33} = 4.5; w_C = w_{c41} + w_{c42} = 4.0;\ w_S = w_{c51} + w_{c52} + w_{c53} = 3.0$

where wc_{ij} represents the significance weight assigned to sub-criterion j under criterion i.

7.3.1 Result Analysis

Both Heat Map and IFN technique provided evaluation of three potential cloud service providers with the same measuring data. In the overall evaluation, IFN techniques gives the ranking order of CSPs: *Amz >Ela* $\geq$ *GMO* whereas Heat Map technique gives the overall rakning order: *Amz*> *Ela*> *GMO* by both auditors. Same performance evaluation is assigned in Heat Map for $User_1$ and $User_2$ as in IFN technique. Overall position of CSPs remained same. Cloud provider *Ela* and *GMO* give the similar performance ranking in overall evaluation (See Table 7.7) but performance evaluation in individual criteria is clearly seen different than overall evaluation in IFN technique in *Ela* and *GMO*. Individual evaluation of cloud provider *GMO* is comparatively very lower than overall position provider *Ela*.

Performance evaluation by Heat Map technique not only provides the performance ranking of the CSPs but also provides the transparent visual performance view of individual criteria with overall evaluation of individual decision makers and combined result of all the decision makers. In overall performance ranking (see for instance in Table 7.17), it gives the convincing results according to the performance measured by cloud auditors. For instance, cloud provider *Amz* and *Ela* look comparatively close performance ranking position in performance measurement, *Performance* factor subs-criteria *Throughput* (tpT) and *Latency* (Lat), *Reliability* factor subs-criteria *MTBF* (MTBF), *Availability* factor subs-criteria *Uptime* (upT), played dominating role (See Table 8.3, highest *tau* value). In case of cloud provider *GMO* it is clearly seen that it has comparatively lower performance than other cloud providers.

Positions of cloud provider *Ela* and *GMO* are the same by IFL and 2nd and 3rd in Performance Heat Map Table. IFL technique is less convincing, because individual performance is in fact very low in provider *GMO* (See Table 7.8). In our observation, it is because the IFL technique is heavily guided by the opinion of the most critical performance evaluators. If any of the users provides very bad feedback of a CSP, it has strongly negative impact on the final position of that CSP. Even if other decision makers judge this CSP as the one with the best performance, the position of that CSP may be lower due to single inconsistent performance evaluator. Beside the fact that IFL can include hesitation degree, it does not increase the precision of the ranking. In spite of high multiple decision alternatives, a new HPC linear ranking algorithm for very big performance tables (up to several thousand of decision alternatives) gives the results less than 3 seconds [31] in Heat Map Technique. So, performance Heat Map technique is highly computationally scalable for the multiple decision alternatives.

In both performance evaluation techniques (see Table 7.5 and section 7.1.3) decision makers can provide the importance of their requirements in specific selection criteria; however, it is easy to allocate specific importance of each criteria in IFL evaluation technique. In Table 7.6 feedback of cloud service users randomly considered to evaluate the performance of the cloud providers in IFL technique. Position of provider *Ela* and *GMO* almost same by IFL and 2nd and 1st in Performance Heat Map Table but result is not convincing in IFL technique because individual performance is very low in provider *GMO* (See Table 7.8). In the observation, it is clearly seen in IFL technique that it is extremely guided by the opinion of the most critical performance evaluators. If any user provides very bad feedback, it extremely changes the position of the CSP.

7.4 Experiment Setup for Pattern Analysis of CSPs

In the previous section, performance of the CSPs analyzed and ranked cloud providers according their service delivery in committed SLA. It is also important to analyze the service delivery pattern of the cloud providers while selecting cloud services from multi-cloud environment. Future behavior of the performance patterns of cloud providers helps cloud users in decision making to choose cloud services [135].

Wide ranging choices of cloud services of growing number of cloud service providers (CSPs) have made challenging decision making problem for cloud service users (CSUs) to select cloud services. CSUs are more concerned with the actual performance delivery of cloud service providers (CSPs) rather than the documented service level agreement (SLA) commitments in their SLA agreement. Cloud providers may not provide actual services according to documented SLA commitments [136]. Service performance pattern of CSPs helps cloud users to select appropriate cloud services from multi-cloud architecture according to their quality of service (QoS) requirements. Detail information (historical, current and future performance) of cloud providers adds confidence to cloud users in decision making to select appropriate cloud providers. Due to dynamic nature of service performance in cloud computing, there are considerable fluctuations in the QoS which results performance of cloud providers unpredictable in the time series. In cloud service selection, historical performance and future performance predictions are equally important as current performance of cloud providers. So, capturing all the performance variability in different performance metrics is important to select the right one among the multiple alternatives of cloud services [147],[44].

Usually, cloud users expect to receive a certain level of service performance as specified in SLA document. In order to provide the long-range performance information of cloud providers, service performance of cloud providers should be continuously monitored. Due to technical limitations and high monitoring cost may not allow cloud users for continuously monitoring service performance of the cloud providers. Efficient prediction method to forecast future performances of cloud providers based on current data helps to solve this problem.

In this work, performance of commercially available cloud providers is measured during a month on a daily basis using cloud-monitoring tool. Performance metrics *Uptime*, *Downtime*,*Outage Frequency*, *Latency*, *Response Time* and *Throughput* are considered to observe the performance of the cloud providers. These time series data do not follow the specific trend pattern and is unique for each cloud provider. In such case automatic forecasting method can create appropriate time series models [76]. We applied ETS and ARIMA prediction methods as automatic prediction methods, which gave very convincing cloud performance predictions according to the performance data collected from cloud providers. Comparison of error measures in both methods reveals that both techniques are appropriate for future performance prediction of cloud providers. In overall performance prediction, ARIMA method produced better result than ETS for our dataset collected from multiple cloud providers during one-month period.

7.5 Prediction Methods and Prediction Accuracy

Prediction methods are broadly divided into qualitative and quantitative. Qualitative forecasting techniques are subjective, based on the opinion and judgment of consumers, experts; they are appropriate when past data is not available. Quantitative predictions are applicable when past data are available. Due to many drawbacks in simple and weighted moving average of quantitative prediction, exponentially smoothing methods are widely used to predict the future data. The choice of prediction method is often constrained by data availability and data pattern. The pattern in the data will affect the type of forecasting method selected. The pattern in the data will also determine whether a time-series method will suffice or whether casuals model are needed. If the data pattern is unstable over time, a qualitative method may be selected. Thus the data pattern is one of the most important factors affecting the selection of a forecasting method [68]. Data may not follow the specific pattern in all the cases. In these circumstances, an automatic forecasting method is essential which determine an appropriate time series model, estimate the parameters and compute the forecasts [76]. The most popular automatic forecasting algorithms are based on either exponential smoothing or ARIMA methods.

7.5.1 Exponential Smoothing

The exponential method involves the automatic weighting of past data with weights that decrease exponentially with time, i.e. the most current values receive a decreasing weighting. For example in each increment in the past is decreased by (1-α), where $\alpha \in$ (0,1) is the smoothing parameter. Generally, there are three exponential smoothing are in practice: Simple, Double and Triple exponential smoothing. The triplet(E,T,S) refers to the three components: error, trend and seasonality. So the model ETS(A,A,N) has additive errors, additive trend and no seasonality and so on. ETS can also be considered an abbreviation of ExponenTial Smoothing [76].

7.5.2 Autoregressive integrated moving average(ARIMA)

It is a generalization of an autoregressive moving average (ARMA) model where data show evidence of non-stationary. ARIMA models are generally denoted ARIMA (p, d, q)(P,D,Q)$_m$ where parameters p, d, and q are non-negative integers, p is the order of the autoregressive model, d is the degree of differencing, and q is the order of the Moving-average model. Furthermore, m refers to the number of periods in each season, and the uppercase P, D, Q refer to the autoregressive, differencing, and moving average terms.

7.5.3 Prediction Accuracy

Let y_t denotes the observation at time t and f_t denote the forecast of y_t. Then define the forecast error $e_t = y_t - f_t$. The forecasts may be computed from a common base time, and be of varying forecast horizons [77]. Thus, we may compute out-of-sample forecasts $f_{n+1}, ..., f_{n+m}$ based on data from times $t = 1, ..., n$. There are commonly used accuracy measures in the forecasting:

7.5.3.1 Scale-dependent measures

These accuracy measures are dependent with the scale of the data. These are useful when comparing different methods applied to the same set of data, but should not be used, for example, when comparing across data sets that have different scales. The most commonly used scale-dependent measures are based on the absolute error or squared errors:

$$MeanSquaredError(MSE) = mean({e_t}^2) \tag{7.1}$$

$$MeanAbsoluteError(MAE) = mean(|e_t|) \tag{7.2}$$

$$RootMeanSquareError(RMSE) = \sqrt{e_t^2} \tag{7.3}$$

7.5.3.2 Measures based on percentage errors

The percentage error is given by $p_t = 100e_t/y_t$. Percentage errors have the advantage of being scale independent, and so are frequently used to compare forecast performance across different data sets. The most commonly used measures are:

$$MeanPercentageError(MPE) = mean(p_t) \tag{7.4}$$

$$MeanAbsolutePercentageError(MAPE) = mean(|p_t|) \tag{7.5}$$

Measures based on percentage errors have the disadvantage of being infinite or undefined if $y_t = 0$ for any t in the period of interest, and having an extremely skewed distribution when any y_t is close to zero.

7.5.3.3 Scaled errors

To make independent with the scale of the data Hyndman et. al [77] proposed scale independent error measure called Mean Absolute Scaled Error (MASE). It is used to determine the success of a model selection procedure.

$$MASE = mean(|q_t|) \tag{7.6}$$

where $q_t = e_t/((1/(n-1)\sum_{i=2}^{n}|y_i - y_{i-1}|)$ When MASE ≤ 1, in the proposed method, gives smaller errors than the one-step errors from other scale dependent measures.

7.5.3.4 Information Criteria(IC)

Information criteria are chosen to choose the best predictive model selection. It is useful in comparison to IC value for another model fitted to same data set.
Akaike's Information Criteria (AIC):

$$AIC = -2log(Likelihood) + 2p \tag{7.7}$$

The AIC [15] provides a method for selecting between the additive and multiplicative error models. Point forecasts from the two models are identical, so that standard forecast accuracy measures such as the MSE or MAPE are unable to select between the error types. The AIC is able to select between the error types because it is based on likelihood rather than one-step forecasts. Minimizing the AIC gives the best model for prediction.
Schwarttz's Bayesian IC(BIC):

$$BIC = AIC + p(log(n) - 2) \tag{7.8}$$

The BIC [123] is used to overcome the inconsistency and over fitted problem in AIC, BIC is used. It is also used in a similar manner like AIC.

$$AICc = AIC + 2(p+1)(p+2)/(n-p) \tag{7.9}$$

where p is the number of estimated parameters in the model. The AICc [75] is an asymptotically efficient information criterion that does an approximate correction for this negative bias. It is also used in a similar manner like AIC.

We have considered all the errors measures in this paper to evaluate the prediction accuracy. ACF1(Autocorrelation of errors at lag 1) is also considered for the error measurements.

Table 7.18: Notation for Monthly Performance Measurement from CSPs' Premises

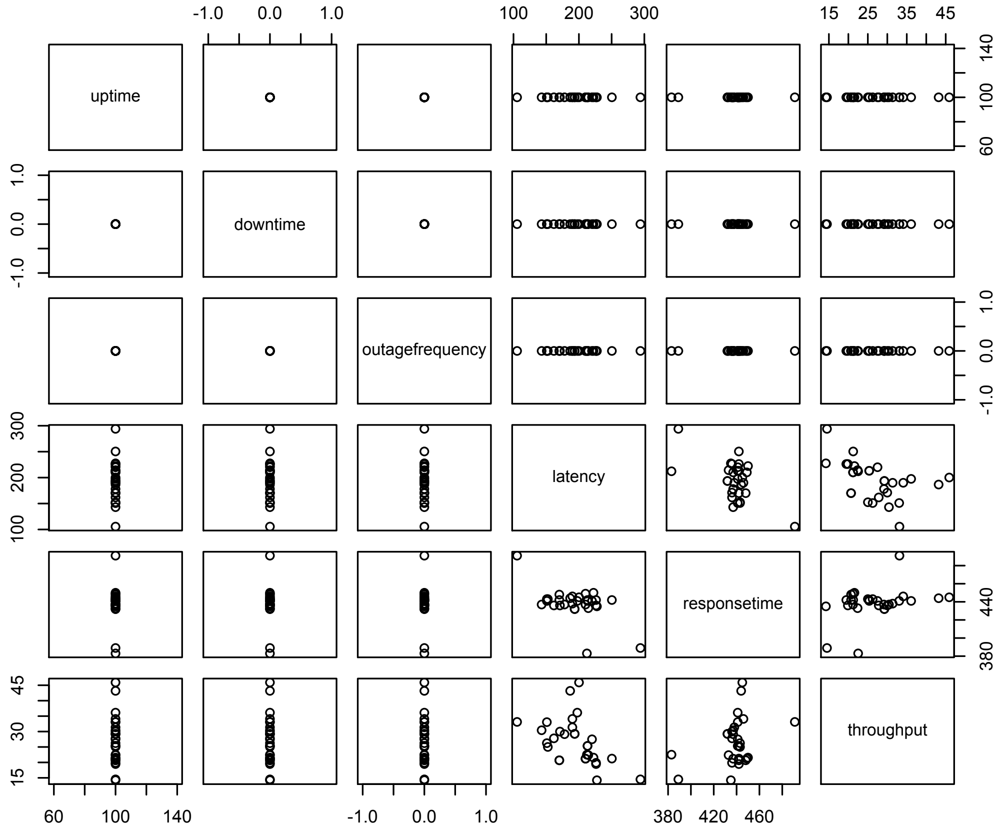
Uptime	Downtime	Outage Frequency	Latency	Response Time	Throughtput
(uptime)	(downtime)	(outagefrequency)	(latency)	(responsetime)	(throughput)
%	sec	Number of Occurance	msec	msec	Mbps

7.6 Performance Measurement

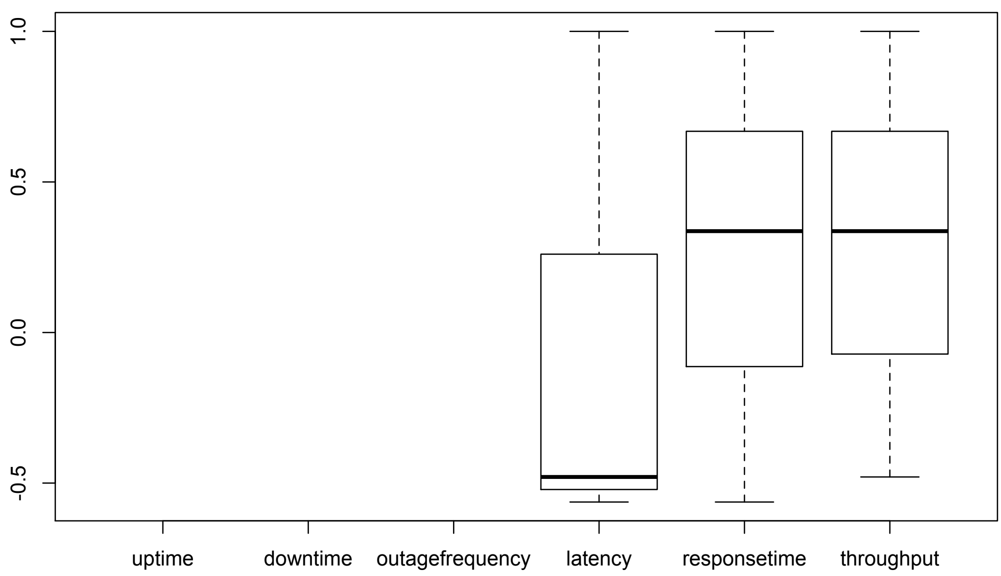
To observe the performance of cloud providers, six major service parameters/metrics are considered in the measurement of the performance of the cloud providers: *Uptime*, *Downtime*, *Outage Frequency*, *Latency*, *Response Time* and *Throughput*. Performance of each cloud providers are obtained using cloud monitoring tool[1] according to the selected service metrics. In our observation, performance of 20 cloud providers collected for 30 days: *Amazon S3*, *GMO Cloud*, *City Cloud*, *Google Cloud Storage*, *Gogrid Cloud*, *Rackspace Cloud*, *Centurylink Cloud*, *UpCloud*, *Softlayer Cloud*, *IBM Cloud*, *HP Cloud*, *Vault Network Cloud*, *Microsoft Azure Cloud*, *Digital Cloud*, *Elastic Host Cloud*, *Exoscale Cloud*, *Sigma Cloud*, *Cloud Central*, *Aruba Cloud* and *Baremetal Cloud*. The performance measurement is based on cloud storage services. It is considered that all cloud service users are located in Luxembourg. Service/availability regions of cloud providers are divided in different regions according to data center locations of the cloud providers. Collected service performance data from cloud providers are merged values of all service/availability regions of the cloud providers.

Figure (a) and (b) of 7.5, 7.6,7.7, 7.8, 7.10, 7.11, 7.12,7.13, 7.14, 7.15, 7.16, 7.17, 7.18, 7.19, 7.20, 7.21, 7.22, 7.23, 7.24 show the service performance measurement and deviation pattern of different 20 cloud providers respectively. The main objective of

[1] cloudharmony.com

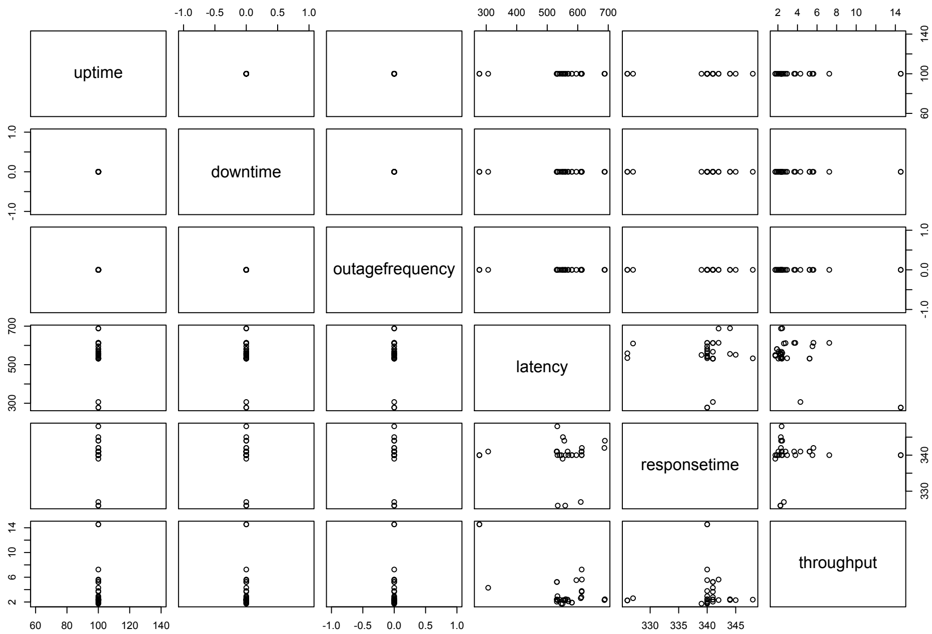


(a) Monthly Performance Pattern

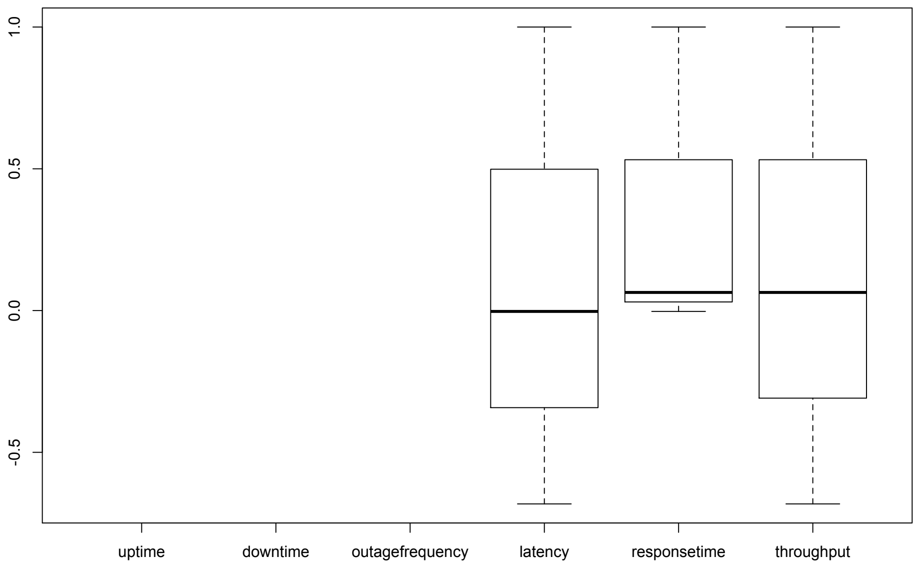


(b) Monthly Deviation Pattern

Figure 7.5: Monthly Service Performance/Deviation Pattern of Amazon-S3 Cloud

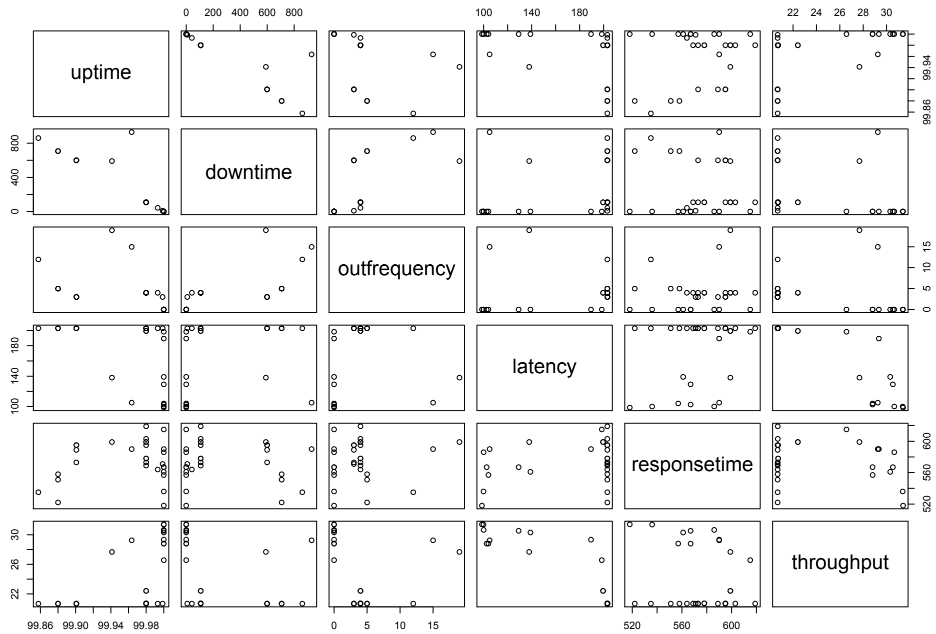


(a) Monthly Performance Pattern

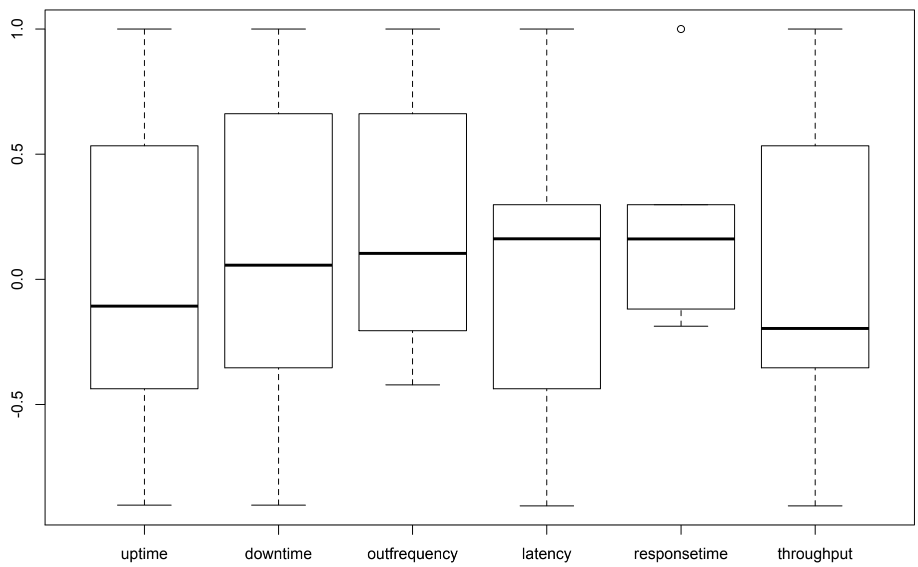


(b) Monthly Deviation Pattern

Figure 7.6: Monthly Service Performance/Deviation Pattern of GMO Cloud

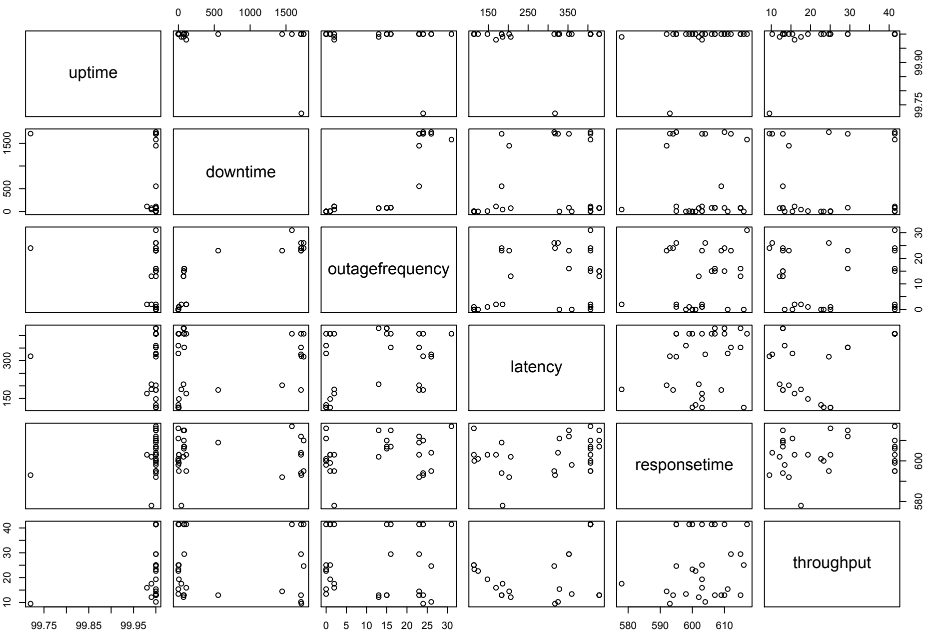


(a) Monthly Performance Pattern

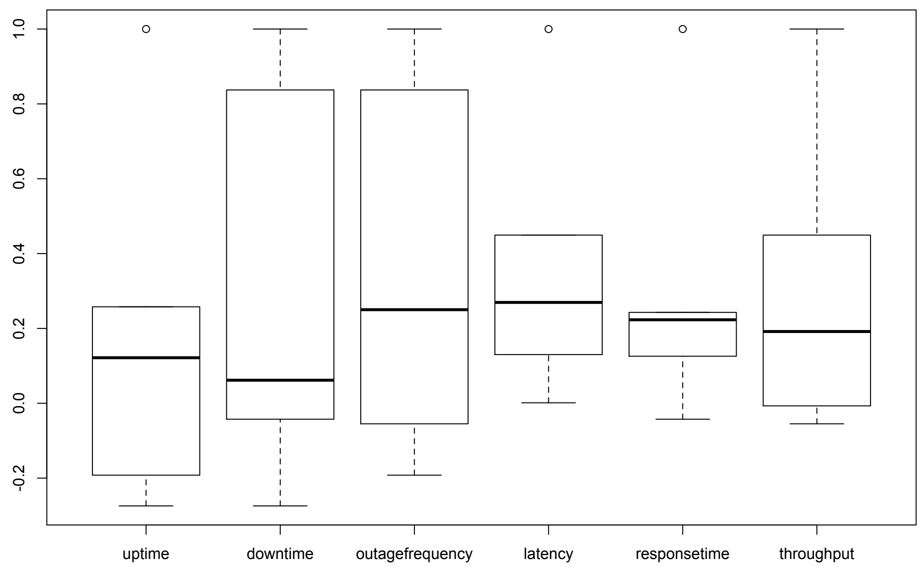


(b) Monthly Deviation Pattern

Figure 7.7: Monthly Service Performance/Deviation Pattern of City Cloud

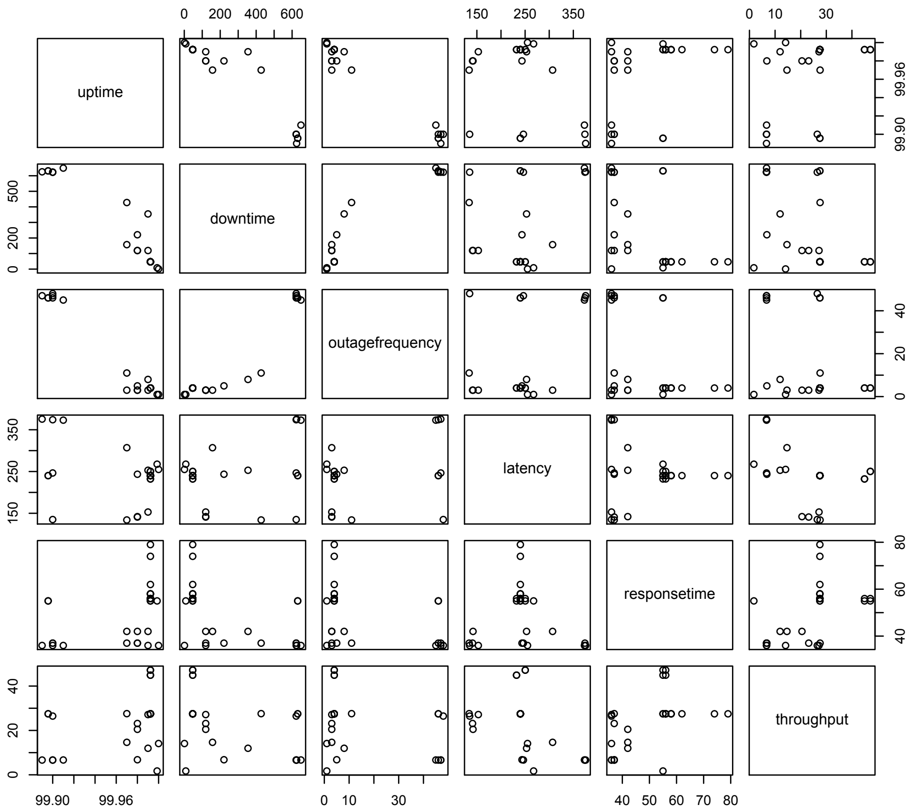


(a) Monthly Performance Pattern

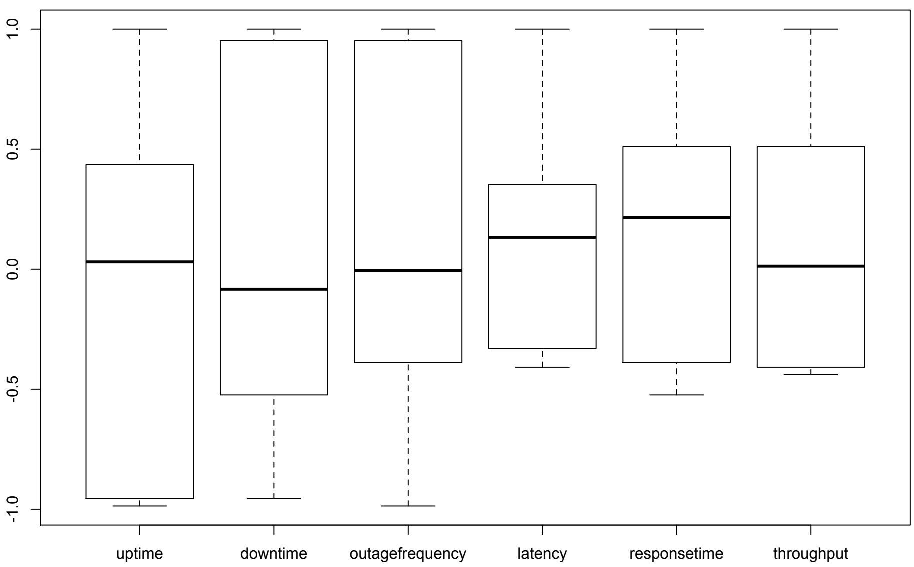


(b) Monthly Deviation Pattern

Figure 7.8: Monthly Service Performance/Deviation Pattern of Digital Cloud

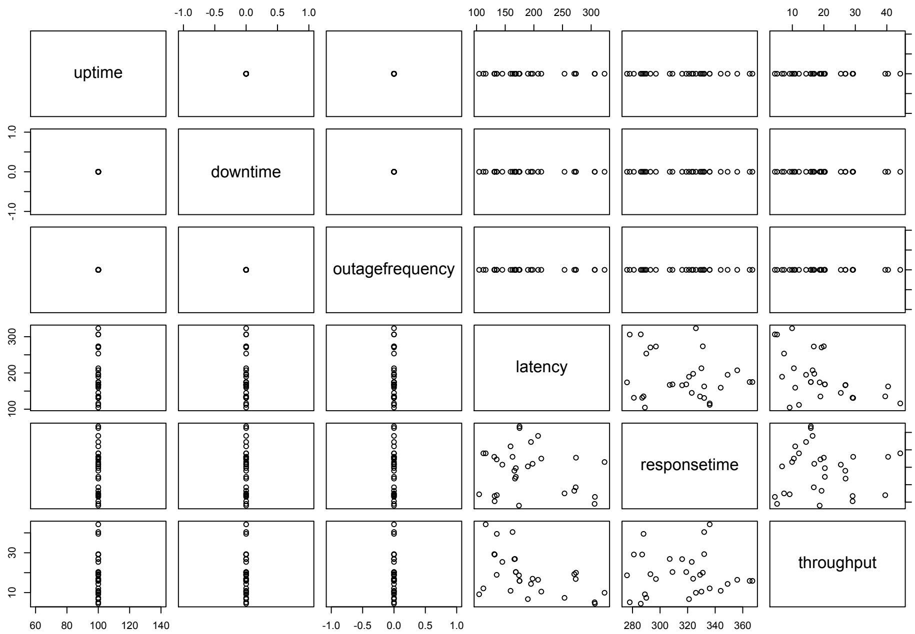


(a) Monthly Performance Pattern

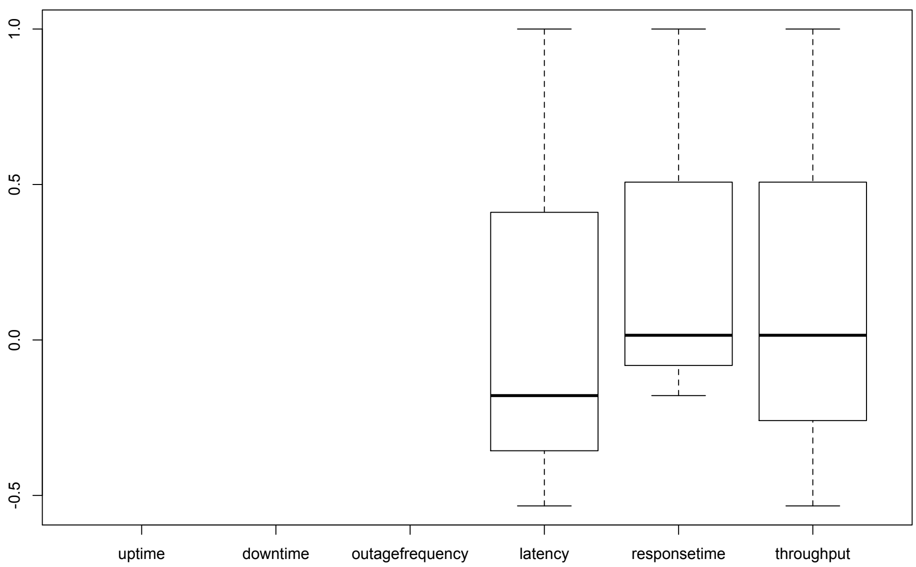


(b) Monthly Deviation Pattern

Figure 7.9: Monthly Service Performance/Deviation Pattern of Elastic Host Cloud

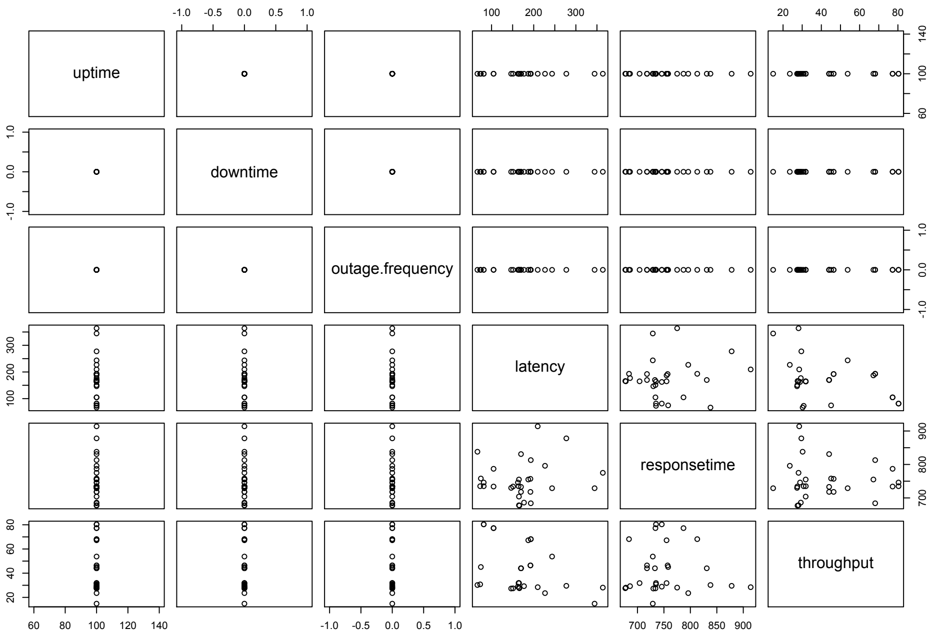


(a) Monthly Performance Pattern

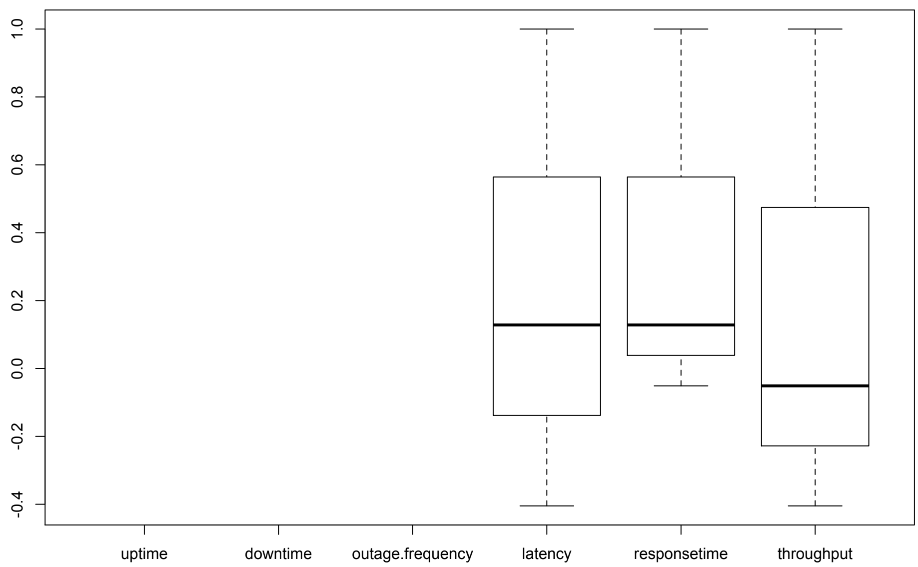


(b) Monthly Deviation Pattern

Figure 7.10: Monthly Service Performance/Deviation Pattern of Microsoftazure

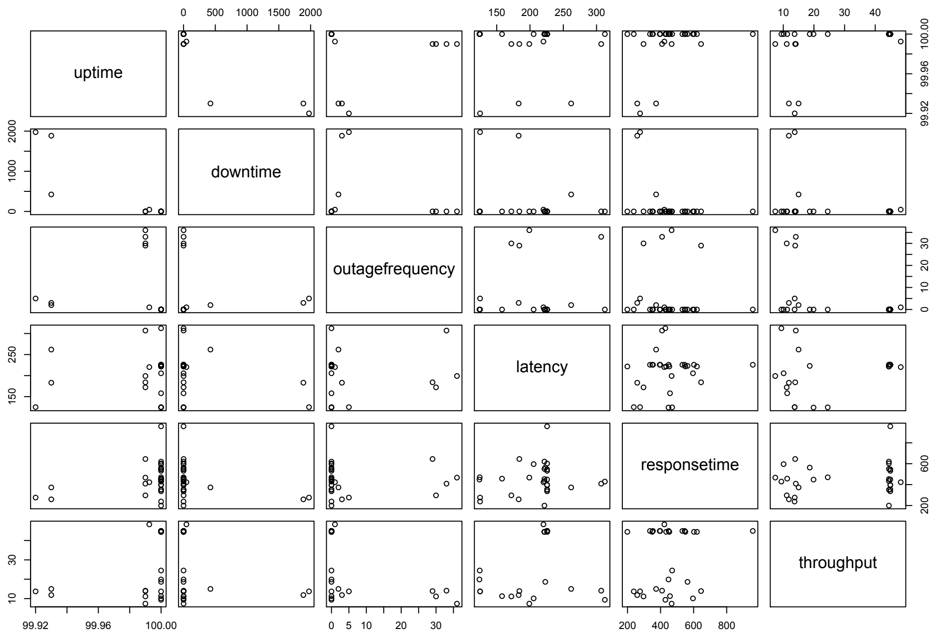


(a) Monthly Performance Pattern

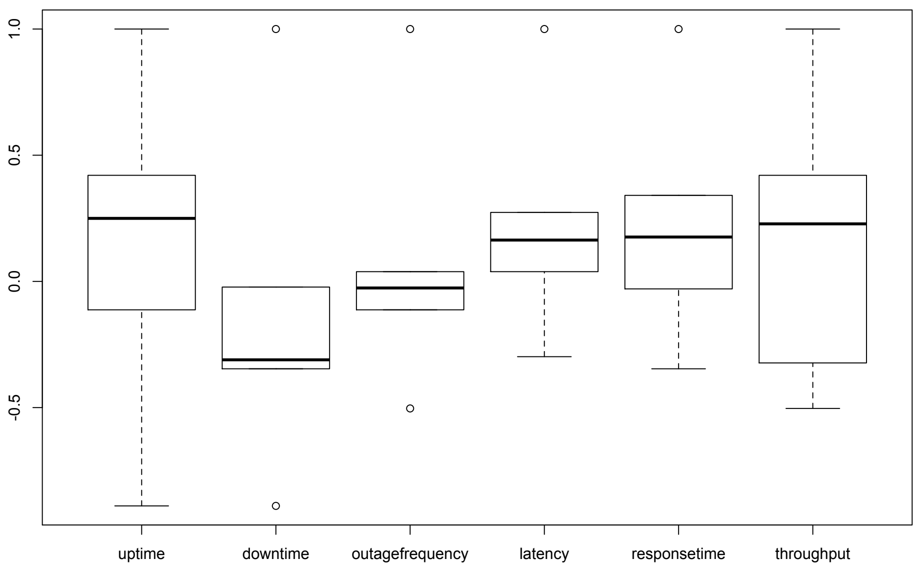


(b) Monthly Deviation Pattern

Figure 7.11: Monthly Service Performance/Deviation Pattern of Google

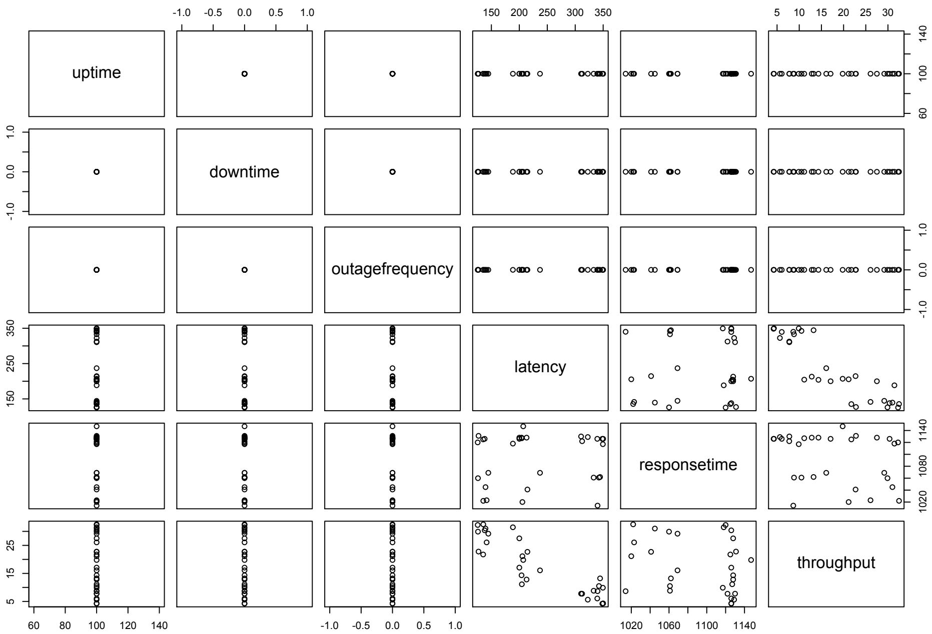


(a) Monthly Performance Pattern

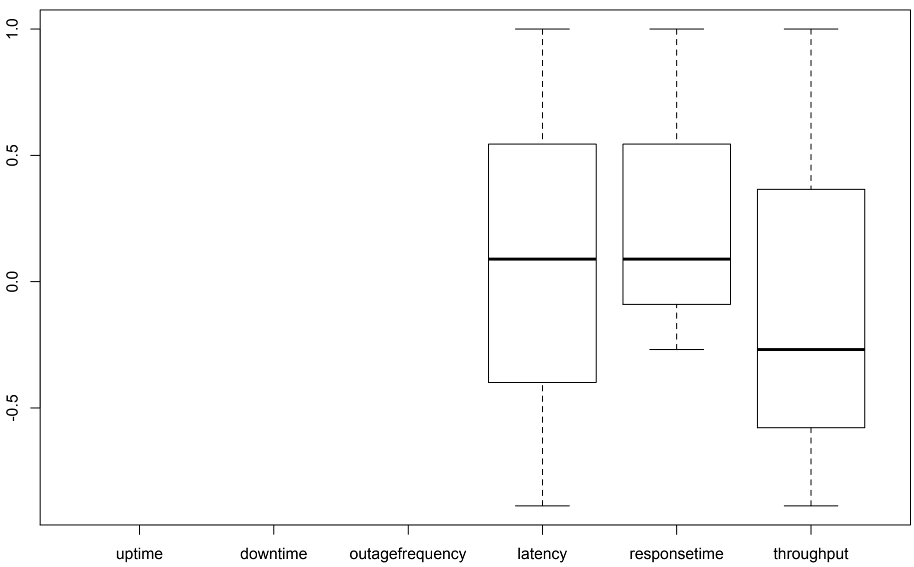


(b) Monthly Deviation Pattern

Figure 7.12: Monthly Service Performance/Deviation Pattern of Cloudsigma

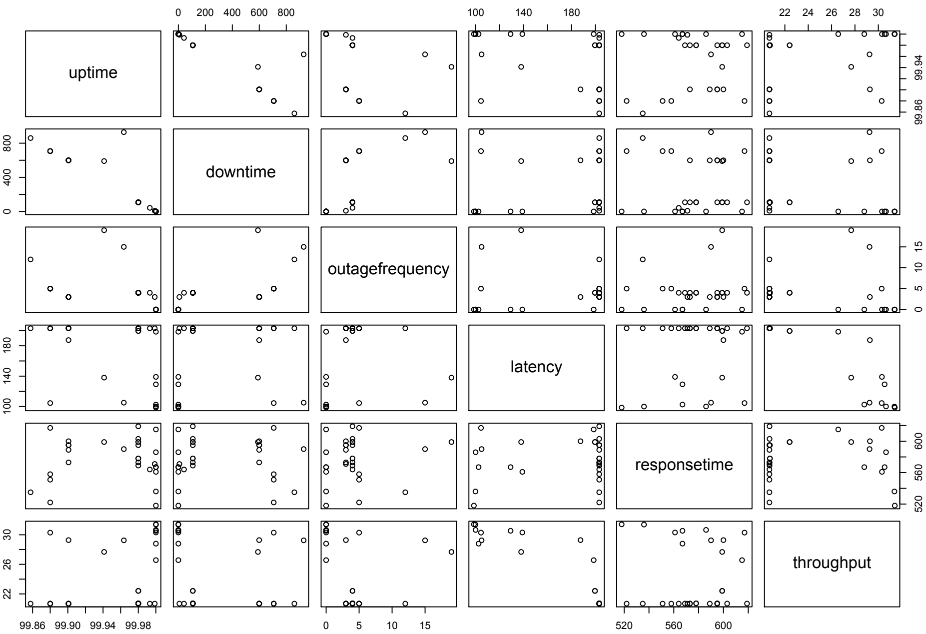


(a) Monthly Performance Pattern

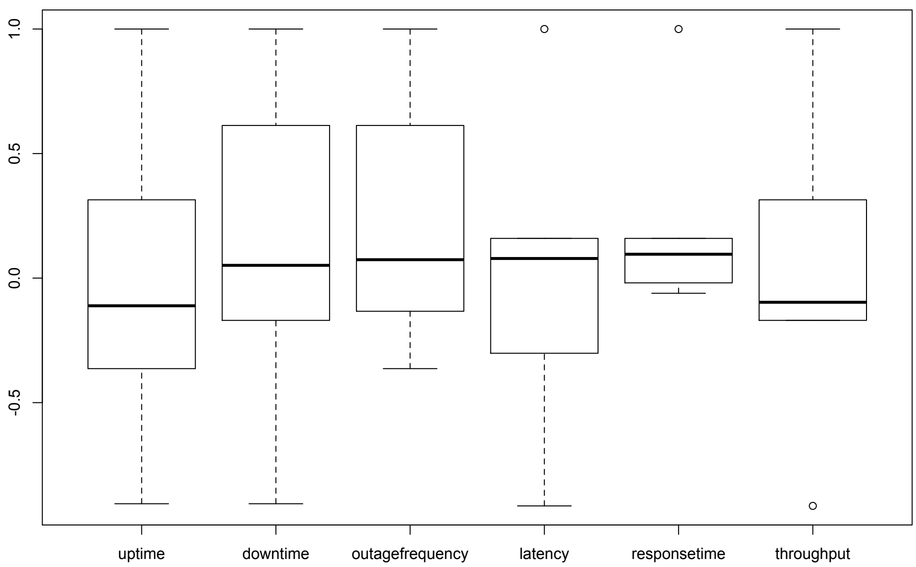


(b) Monthly Deviation Pattern

Figure 7.13: Monthly Service Performance/Deviation Pattern of Gogrid



(a) Monthly Performance Pattern

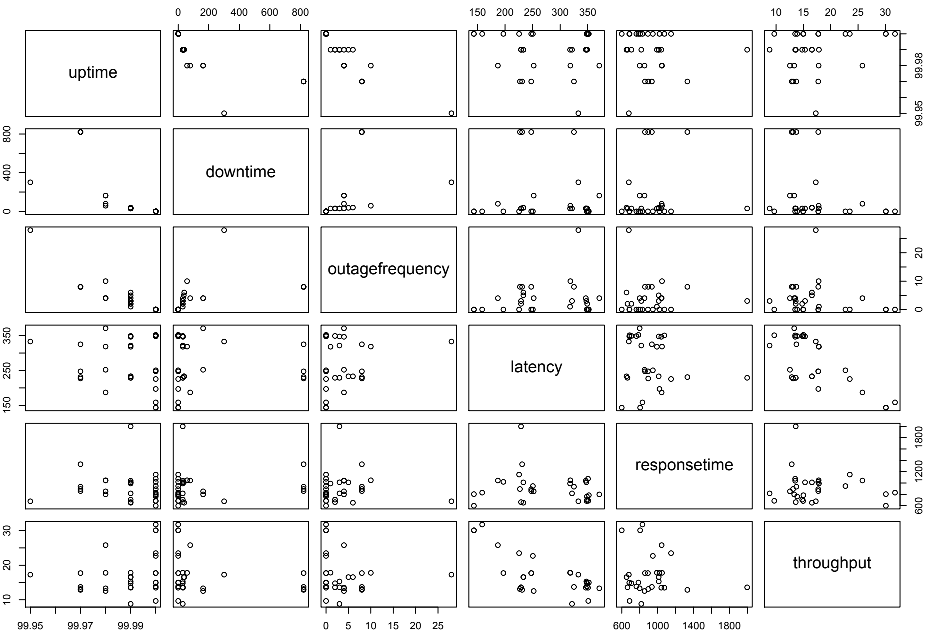


(b) Monthly Deviation Pattern

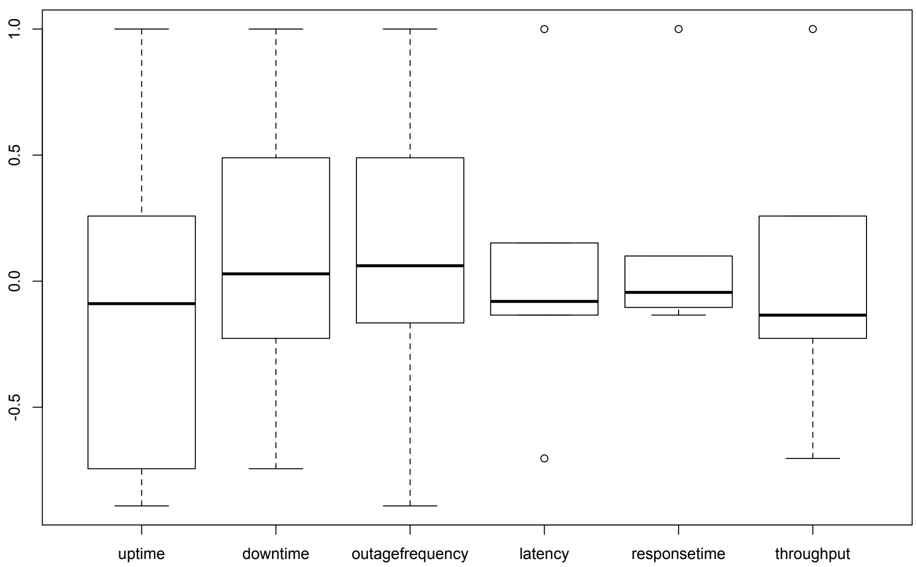
Figure 7.14: Monthly Service Performance/Deviation Pattern of Rackspace

the performance measurement is providing the deviation pattern of the cloud providers, which gives the stability of the performance delivered. For instance, high *uptime*, high *throughput*, low *downtime*, low *outage frequency*, low *latency*, low *responsetime* is always prefered from performance perspective, however, such cloud providers are not prefered if there are high fluctuations in the service performance. The analysis of performances of cloud provider *Amazon S3*, *GMO-US*, *Microsoft Azure*, *Google Cloud*, *Gogrid*, *IBM Cloud* and *VaultNetwork Cloud* found less fluctuated in *Uptime*, *Downtime*, *Outage Frequency* and rest three parameters *Latency*, *Responsetime* and *Throughput* are found more fluctuated and hard to predict performance patterns easily. For example, performance parameters: *uptime*, *downtime*, *outagefrequency* are near in *100%, 0 second and 0 times* in cloud provider *Amazon S3*, *GMO-US*, *Microsoft Azure*, *Google Cloud*, *Gogrid*, *IBM Cloud* and *VaultNetwork Cloud* respectively but these three service parameters were also fluctuating in other selected cloud providers for the performance measurement: *City Cloud*, *Rackspace Cloud*, *Centurylink Cloud*, *UpCloud*, *Softlayer Cloud*, *HP Cloud*, *Microsoft Azure Cloud*, *Digital Cloud*, *Elastic Host Cloud*, *Exoscale Cloud*, *Sigma Cloud*, *Cloud Central*, *Aruba Cloud* and *Baremetal Cloud* together with other three service parameters: *Latency*, *Responsetime* and *Throughput.*

Service performance stability reflects the reliable cloud providers to choose the services according to the requirements. *Latency* of cloud provider *AMZ*, *response time* of *GMO Cloud*, *latency* and *throughput* of cloud provider *City Cloud*, *uptime* and *downtime* of cloud provider *Digital Cloud*, *uptime* and *downtime* of cloud provider *HP Cloud*, *throughput* of cloud providerMicrosoft Azure, *Google Cloud*, *Cloud Sigma*, *Gogrid Cloud*, *downtime* and *outagefrequency* of *Rackspace Cloud*, *uptime* of *Centurylink Cloud*, *downtime* and *responsetime* of *Upcloud*, *downtime* and *outagefrequency* of *Softlayer Cloud*, *latency*, *responsetime* and *throughput* of *IBM Cloud*, *latency* of *HP Cloud*, *uptime* and *throughput* of *Exoscale Cloud*, *downtime* and *outagefrequency* of *Cloudcentral Cloud*, *outage frequency* of *Aruba Cloud*, *uptime* and *downtime* of

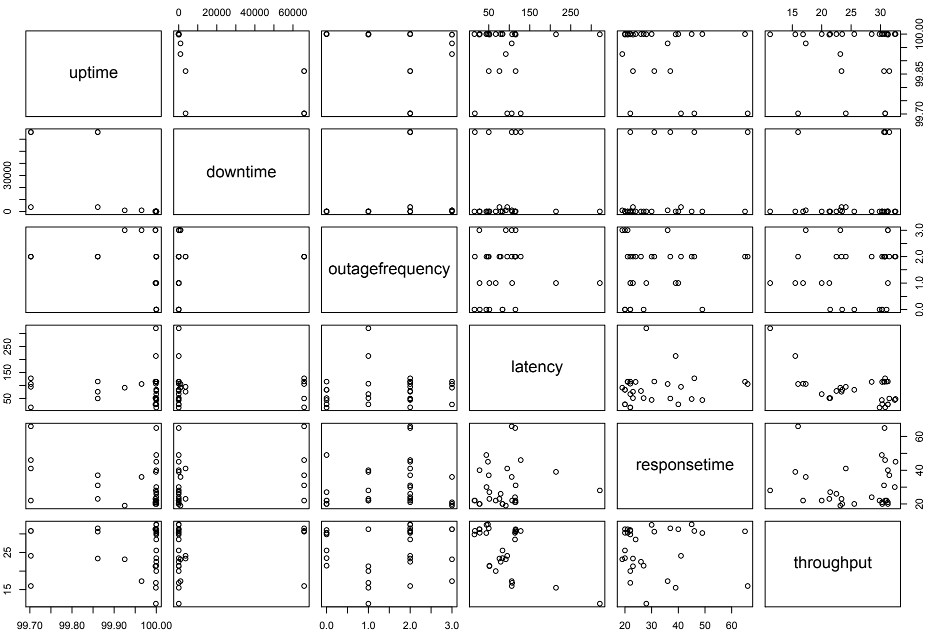


(a) Monthly Performance Pattern

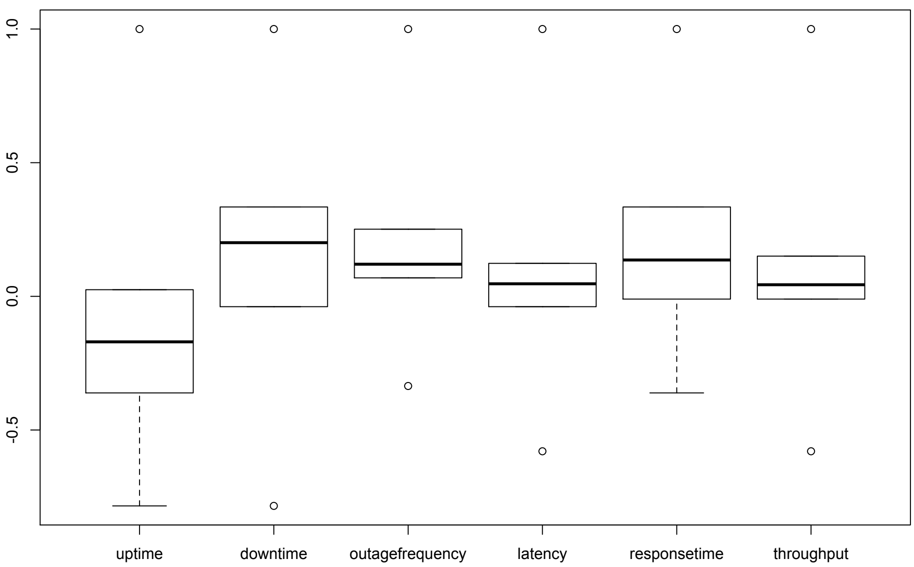


(b) Monthly Deviation Pattern

Figure 7.15: Monthly Service Performance/Deviation Pattern of Centurylink

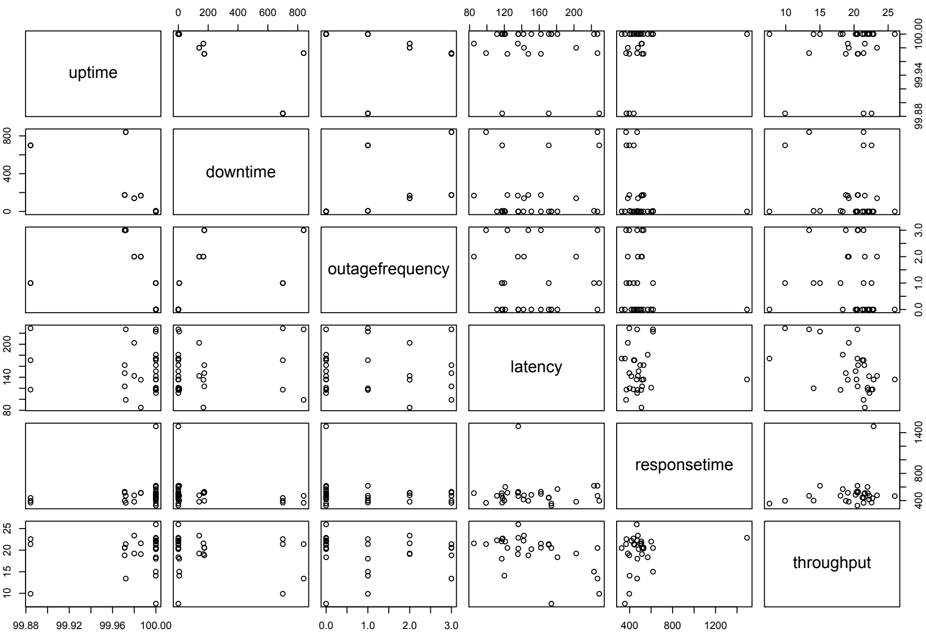


(a) Monthly Performance Pattern

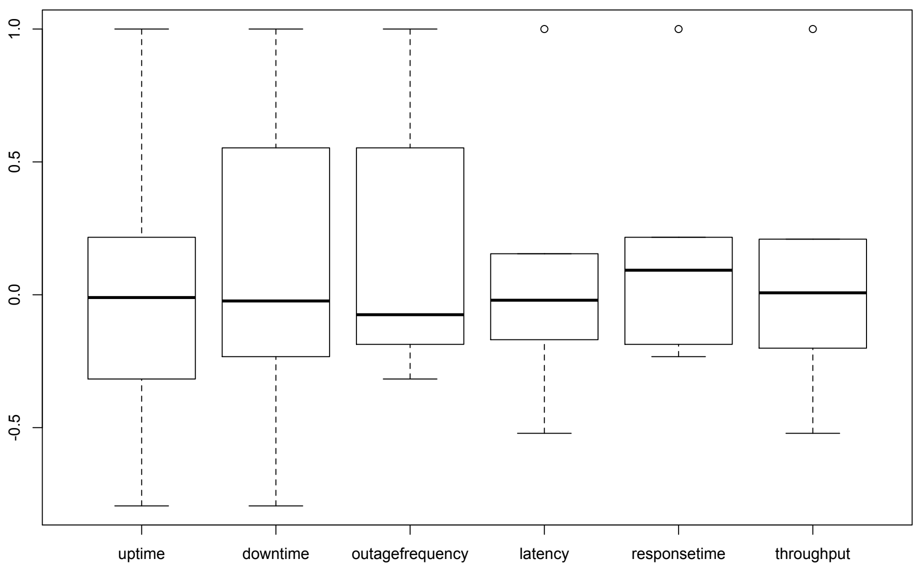


(b) Monthly Deviation Pattern

Figure 7.16: Monthly Service Performance/Deviation Pattern of Upcloud

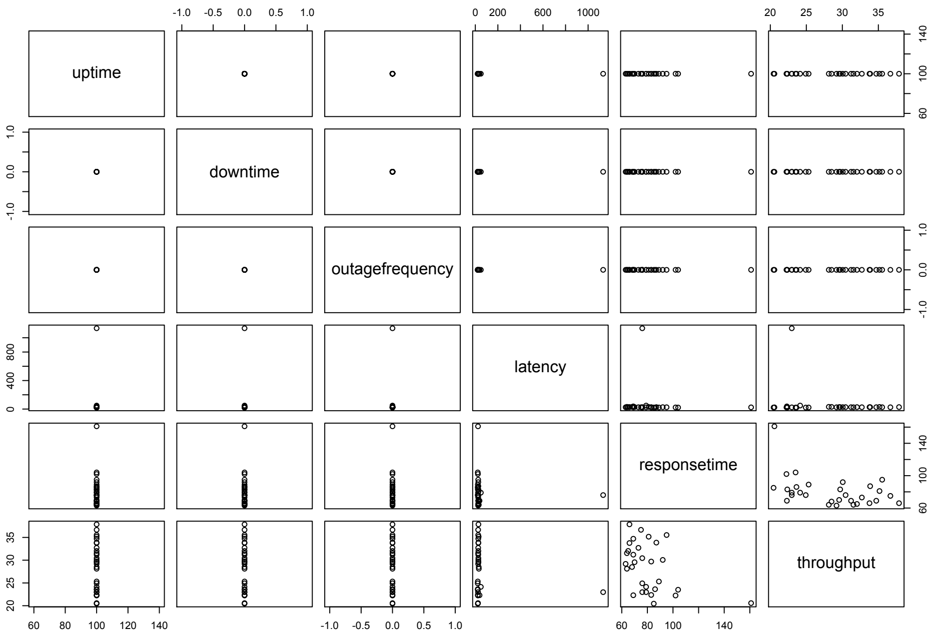


(a) Monthly Performance Pattern

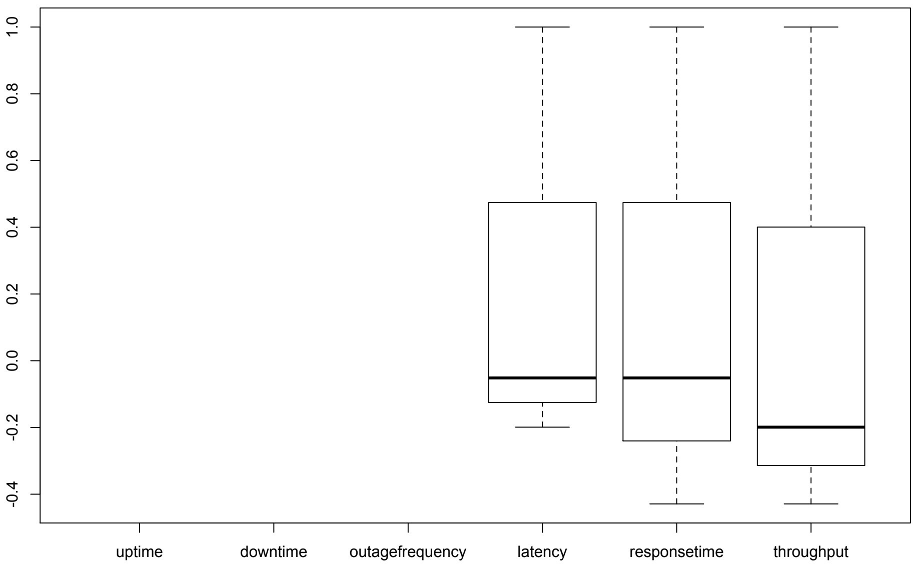


(b) Monthly Deviation Pattern

Figure 7.17: Monthly Service Performance/Deviation Pattern of Softlayer

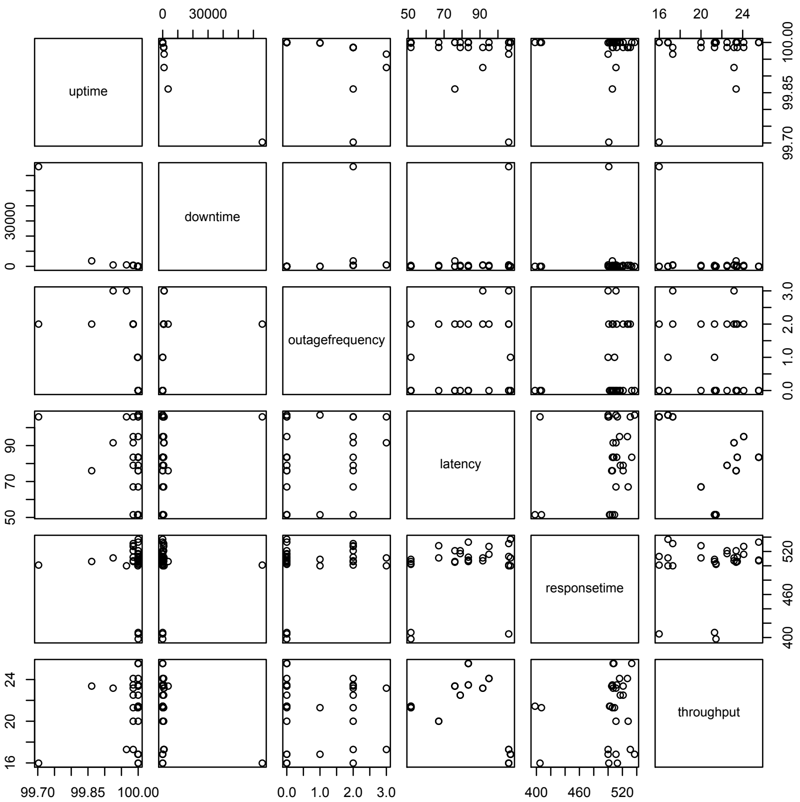


(a) Monthly Performance Pattern

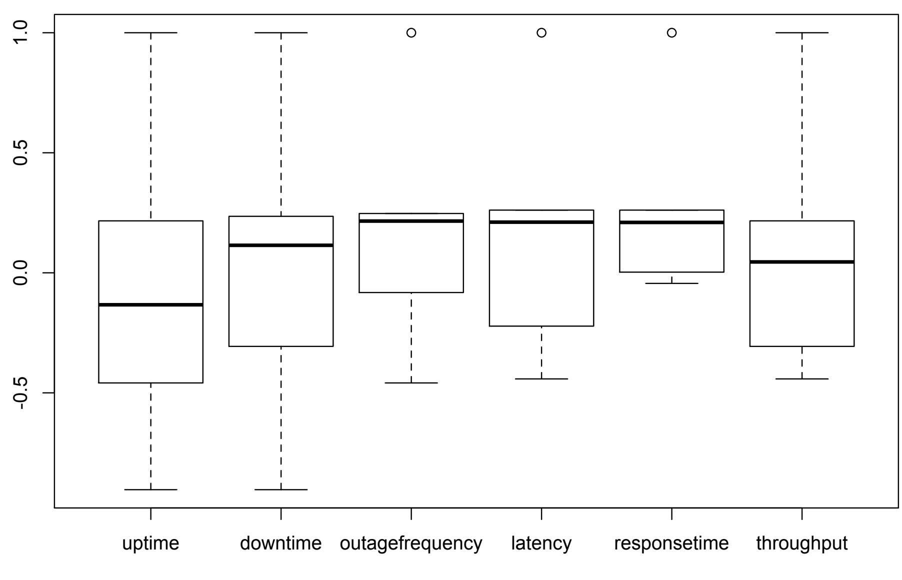


(b) Monthly Deviation Pattern

Figure 7.18: Monthly Service Performance/Deviation Pattern of IBM

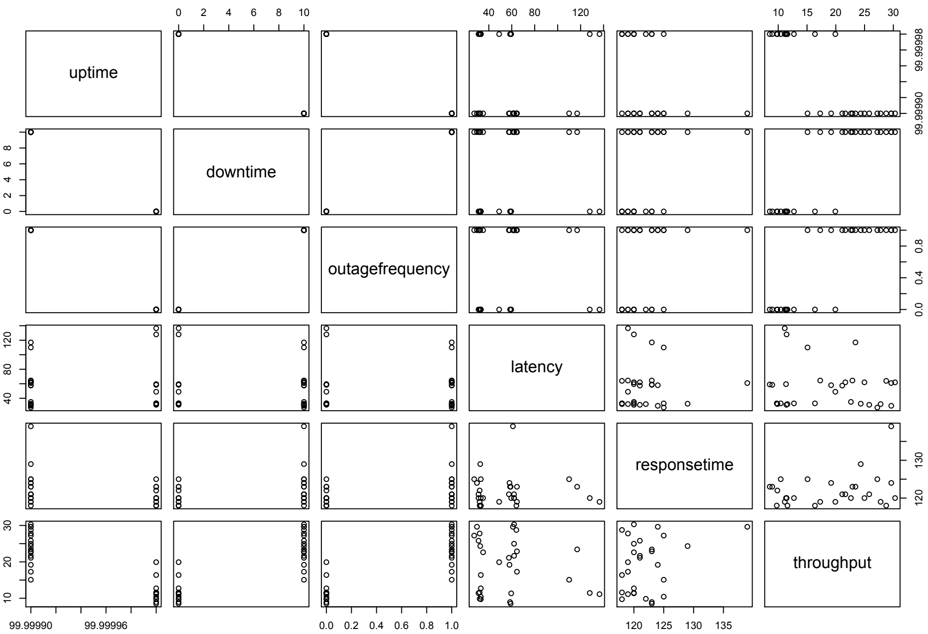


(a) Monthly Performance Pattern

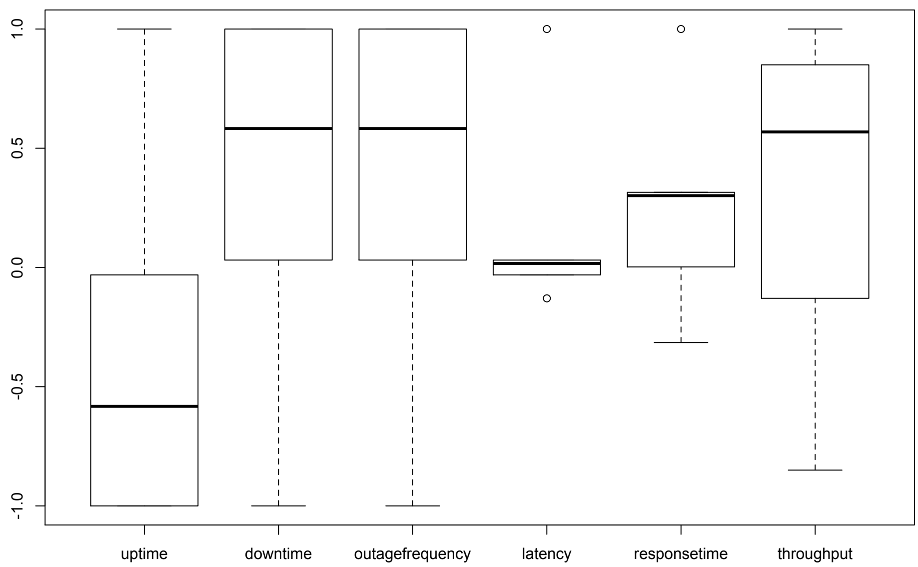


(b) Monthly Deviation Pattern

Figure 7.19: Monthly Service Performance/Deviation Pattern of HP

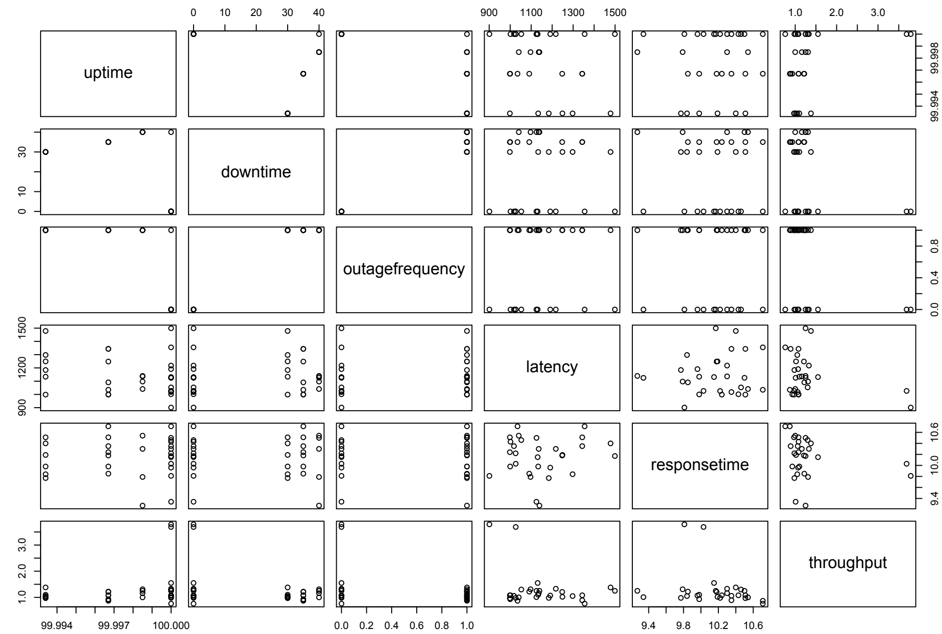


(a) Monthly Performance Pattern

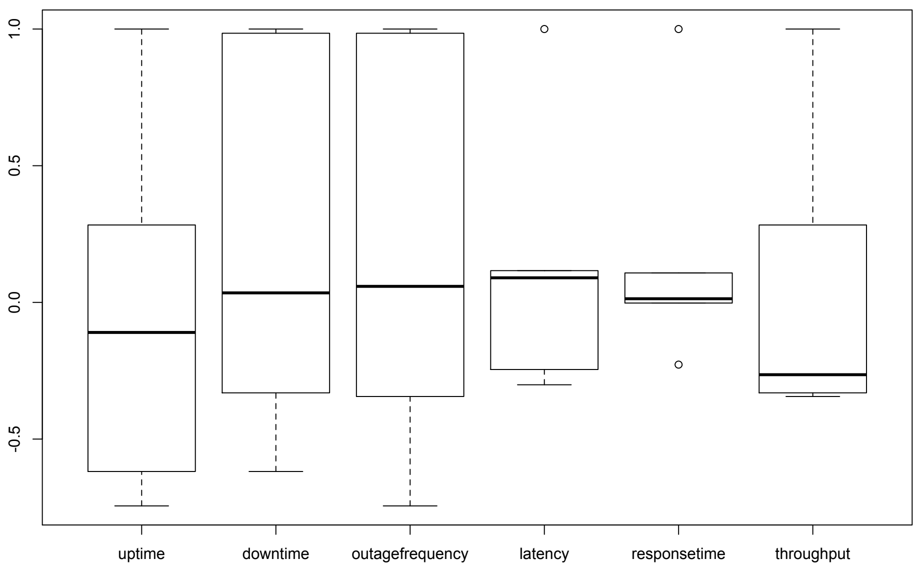


(b) Monthly Deviation Pattern

Figure 7.20: Monthly Service Performance/Deviation Pattern of Exoscale

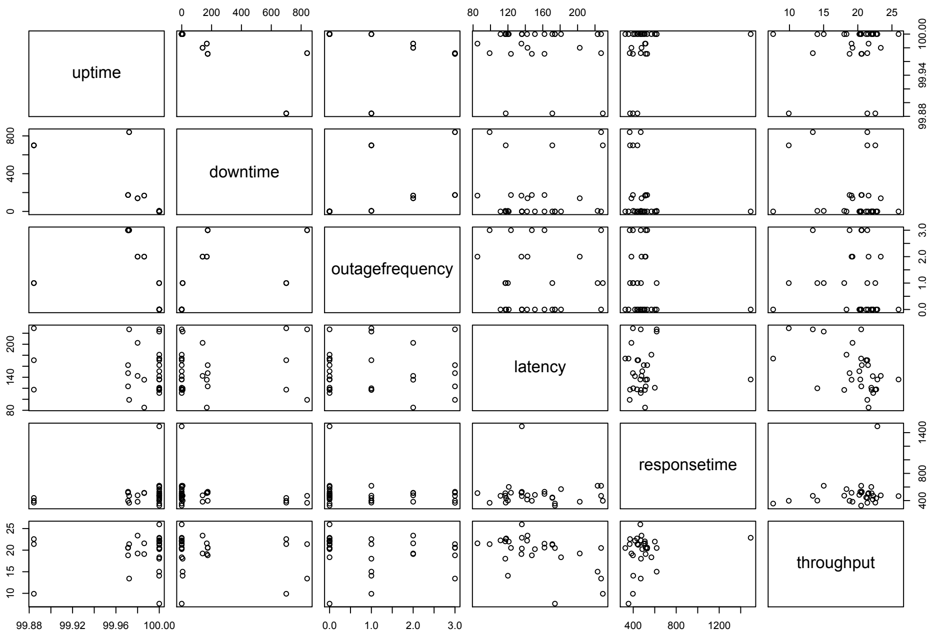


(a) Monthly Performance Pattern

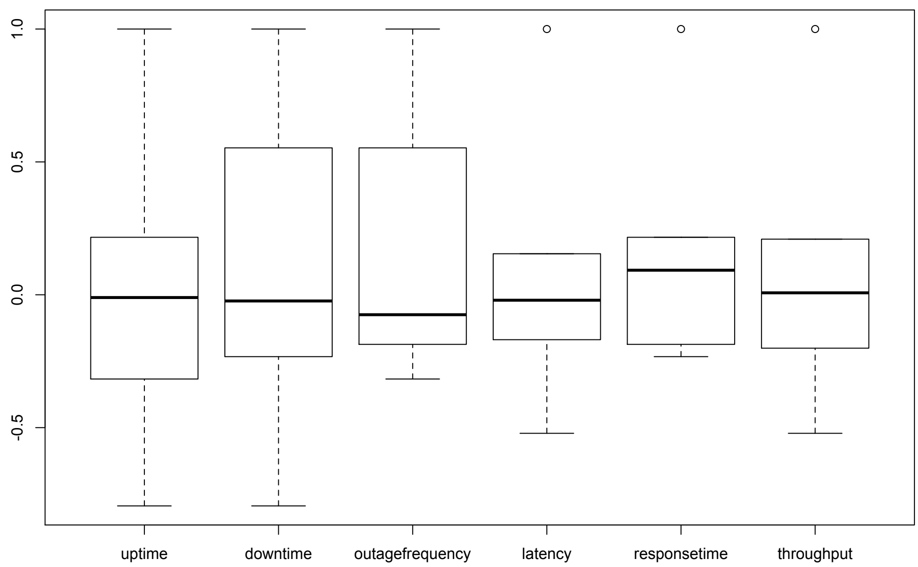


(b) Monthly Deviation Pattern

Figure 7.21: Monthly Service Performance/Deviation Pattern of Cloudcentral

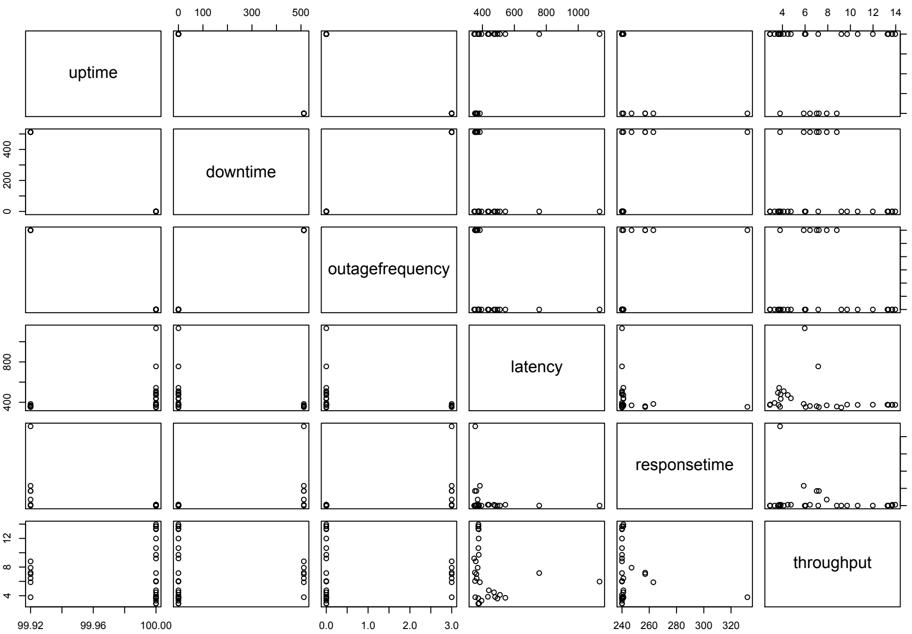


(a) Monthly Performance Pattern

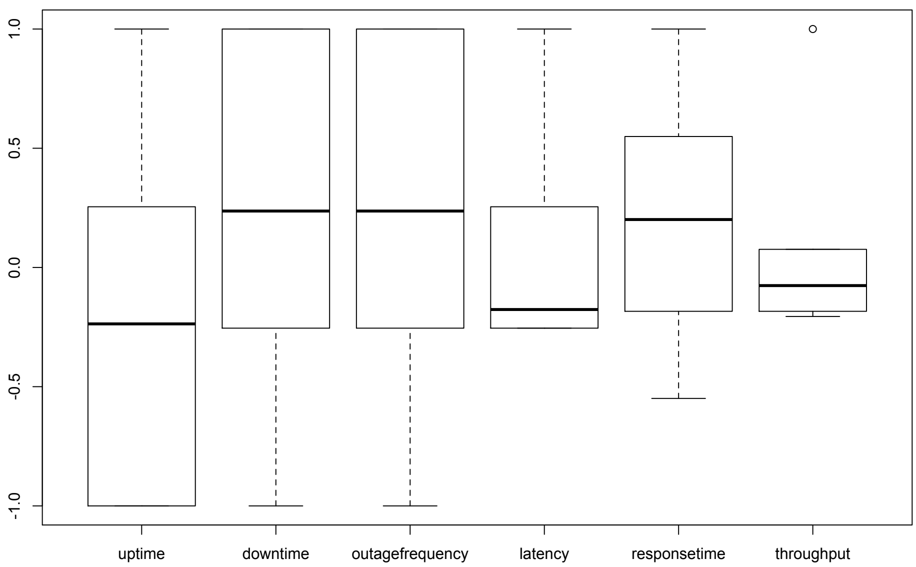


(b) Monthly Deviation Pattern

Figure 7.22: Monthly Service Performance/Deviation Pattern of Aruba

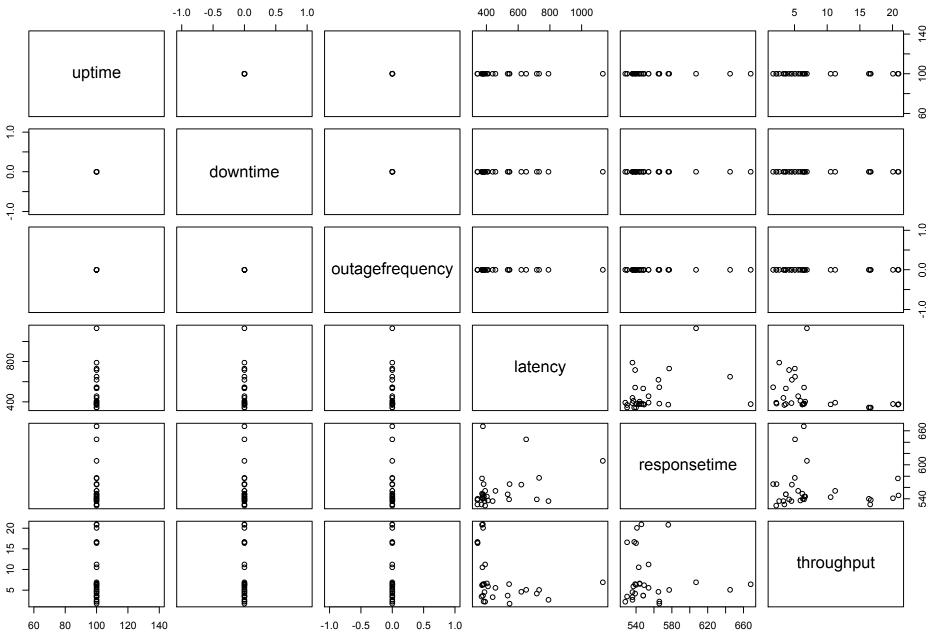


(a) Monthly Performance Pattern

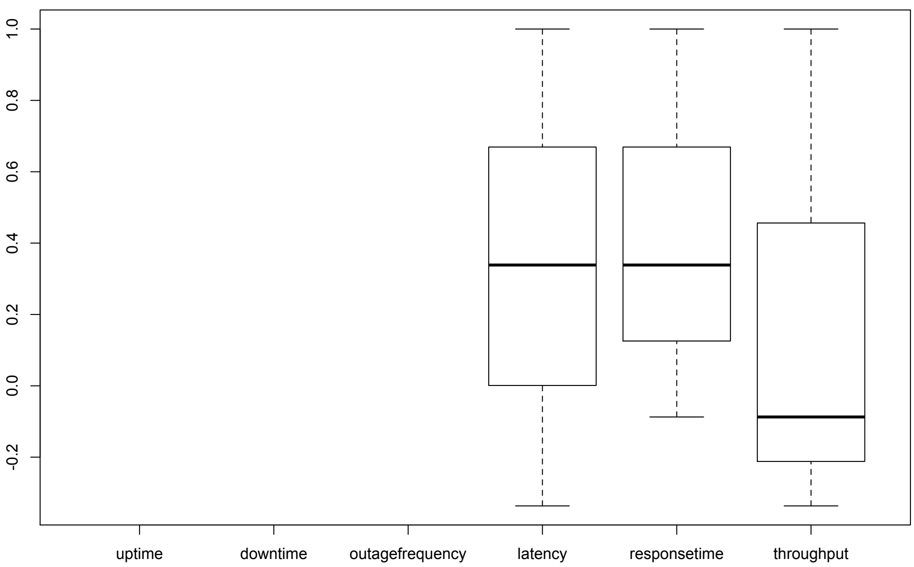


(b) Monthly Deviation Pattern

Figure 7.23: Monthly Service Performance/Deviation Pattern of Baremetal



(a) Monthly Performance Pattern



(b) Monthly Deviation Pattern

Figure 7.24: Monthly Service Performance/Deviation Pattern of VaultNetwork

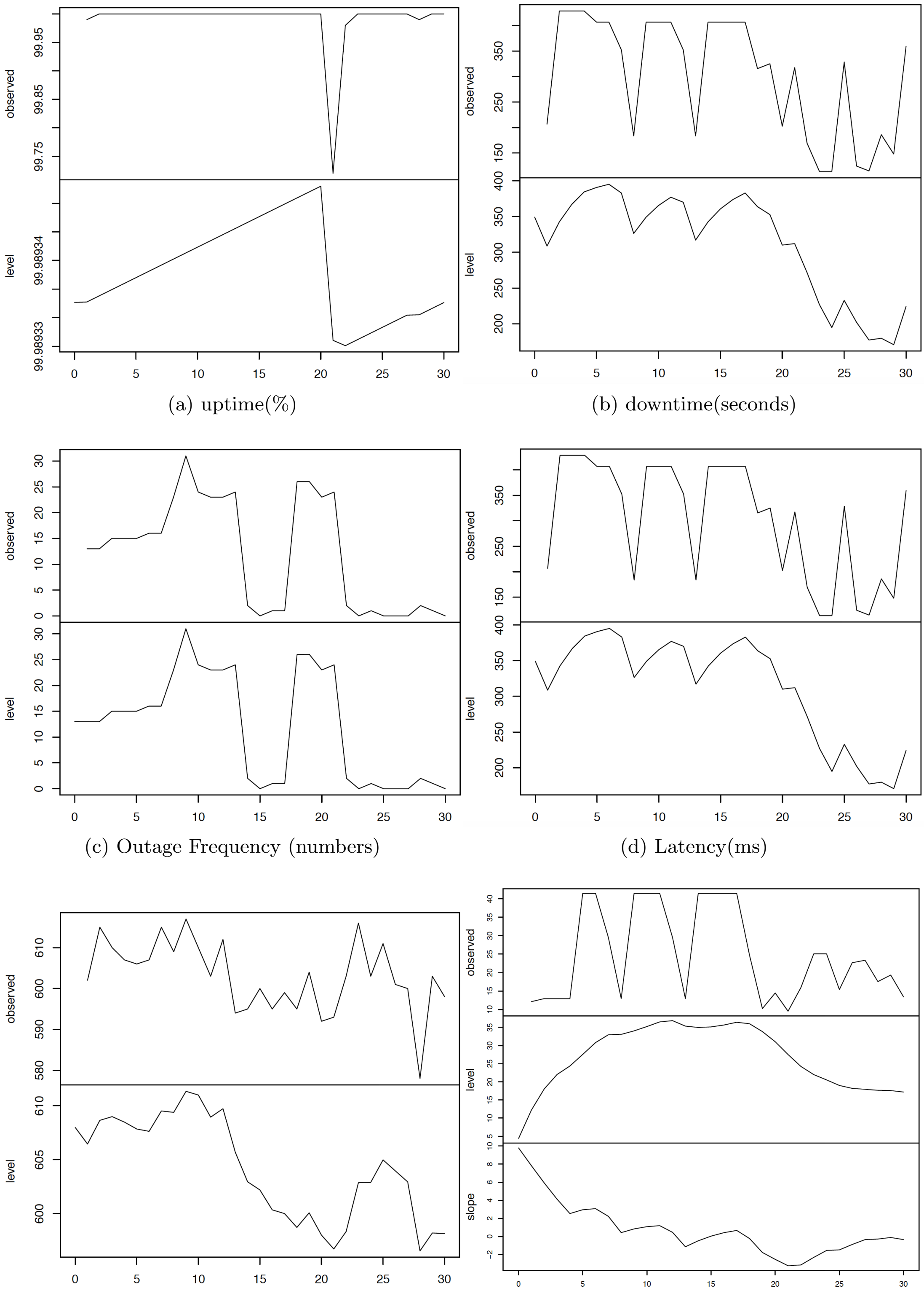
Baremetal Cloud, *throughput* of *VaultNetwork Cloud* are highly fluctuated performance parameters than other parameters in our monthly performance observation from cloud providers.

7.6.1 Performance Pattern Analysis

However, we analysed the performance pattern of all the selected 20 cloud providers, we have included performance patterns of few CSPs in this thesis to show the concept of performance pattern of CSPs. Figure 7.25 and 7.26 show the service performance pattern of the *Digital Cloud* and *Exoscale Cloud*.

7.7 Service Performance Prediction

Future performance behavior of the CSPs are predicted based on the current performances of CSPs using two automatic forecasting algorithm: ARIMA an ETS as mentioned in section 7.5. To analyze the accuracy of our predicted performance of CSPs, we applied two approaches: firstly, we calculated the errors of prediction and secondly matching with 1/3 of observed performance measurement with predicted performances using 2/3 of observed performance of cloud providers. Similarly, performance prediction patterns of few cloud providers are included in this thesis as mentioned in Section 7.6.1 on selected metrics, however, performance prediction accuracy of all cloud providers are presented in the Section 7.8. Service performance patterns in parameters: *Uptime*, *Downtime* and *Outage Frequency* in most of the cloud providers are very close in most of the time series(See for instance in Figure 7.25 and 7.26 for service performance pattern of Digital Cloud and Exocloud respectively) and easily predictable from their performance pattern. The service patterns of all the selected cloud providers give the clear picture of cloud service performance of the cloud providers over a month. The performance of cloud providers collected over the month from multiple cloud providers



(a) uptime(%) (b) downtime(seconds) (c) Outage Frequency (numbers) (d) Latency(ms) (e) Responsetime(ms) (f) Throughput(Mbps)

Figure 7.25: Monthly Service Performance Pattern of Digital Cloud

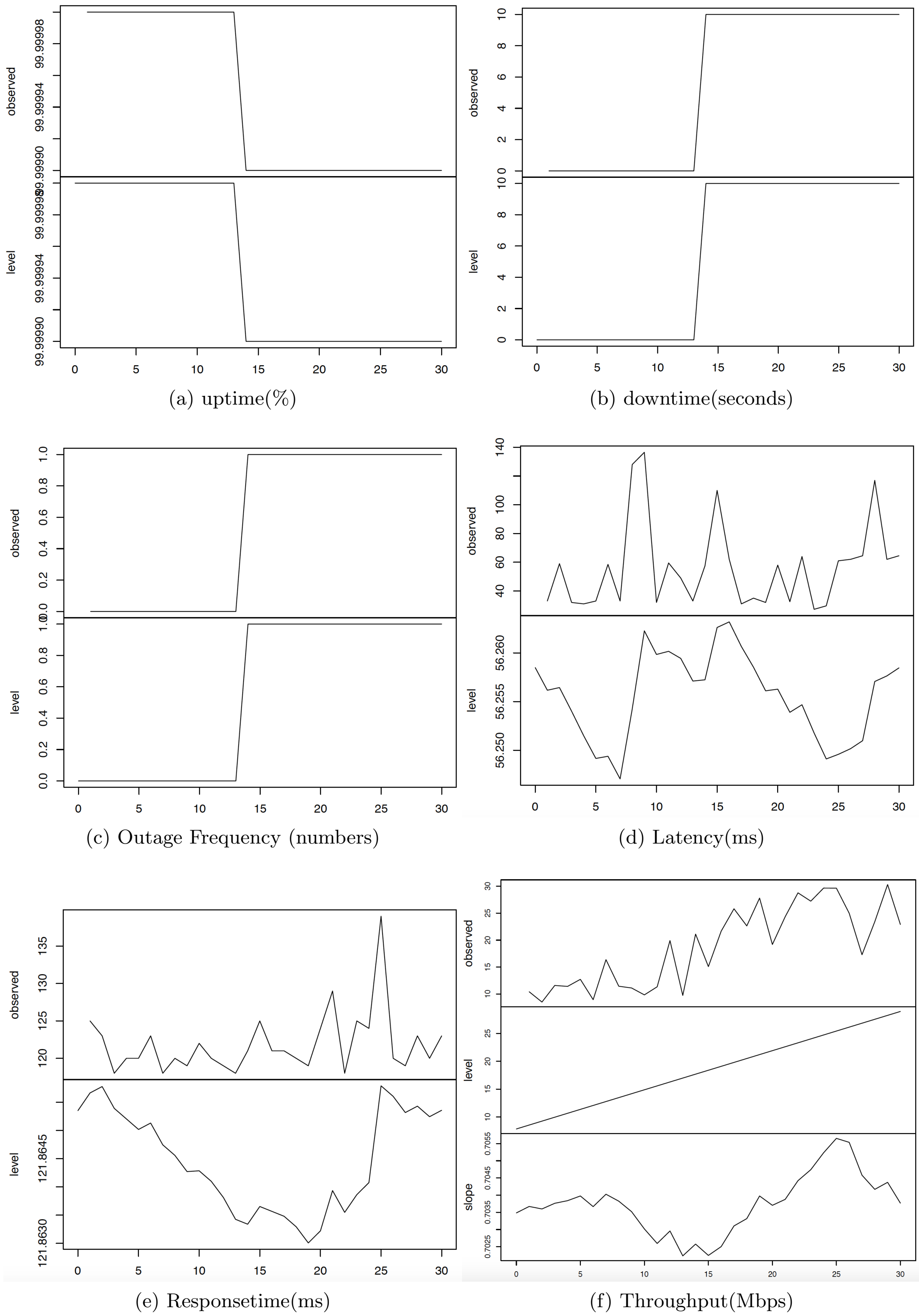
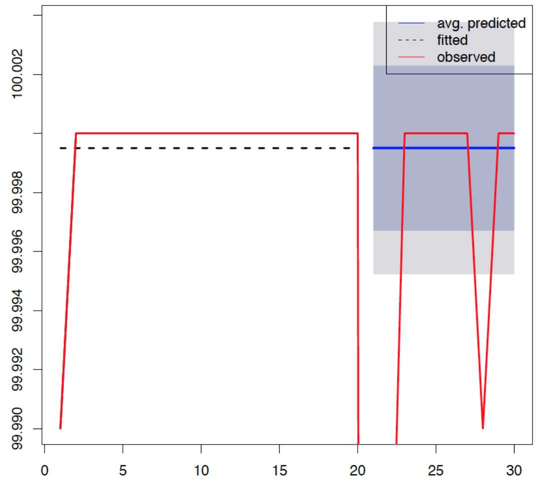


Figure 7.26: Monthly Service Performance Pattern of Exoscale Cloud

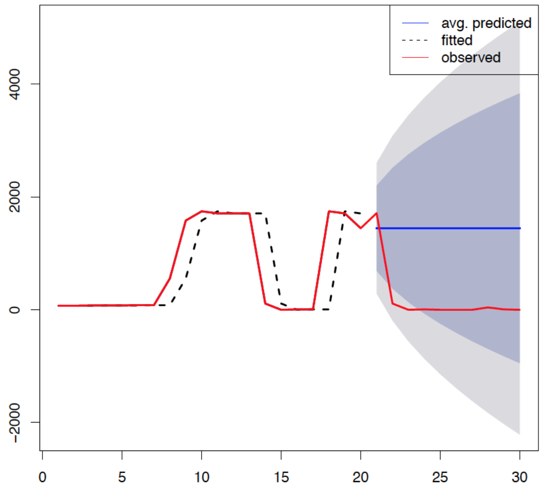
neither followed specific pattern nor remained in stable seasonal patterns for specific time periods. Information of service delivery pattern of cloud providers of entire month (possibly delivery pattern of longer time period e.g. 3 months, 6 months, 1 year or more) gives the tentative impression of cloud service providers to choose appropriate cloud services for the cloud users. From monitoring cost, technical complexities and accessibility to the cloud providers through out the period, it is very challenging to collect the service pattern of cloud provider over the longer time period. Highly efficient prediction of data solves this problem to receive the service performance information for longer terms. To achieve the maximum accuracy in cloud service performance prediction as much as possible, we applied automatic forecasting method to determine the appropriate time series prediction, particularly: ETS and ARIMA method for the cloud providers performance prediction.

Performance pattern prediction of cloud provider *Digital Cloud* and *Exoscale Cloud* predicted using ETS and ARIMA methods are shown in Figure 7.27, 7.28, 7.8.1 and 7.29 respectively. Both prediction methods showed convincing predictions in each performance parameters. Service performance data of 20 days are trained for the performance prediction using ETS and ARIMA prediction method. Prediction of all the selected performance parameters of 20 cloud providers by both prediction methods produced the convincing results as in *Digital Cloud* and *Exoscale Cloud*. To analyse the accuracy of our prediction, different error measurements are calculated (See for instance Table 7.19 and 7.20 for *Digital Cloud* and *Exoscale Cloud* respectively).

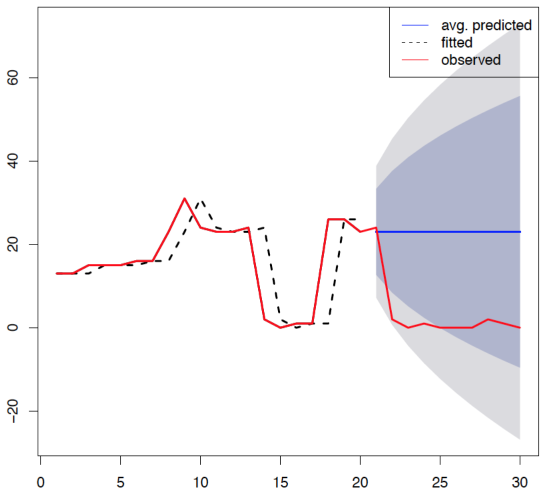
To identify the accuracy of prediction method, errors parameters are considered. In the performance prediction, all parameters do not return the exact accuracy of the prediction method because of different scale of the measured data. So, scale dependent errors, percentage errors and scale independent errors are considered to check the accuracy of the prediction. Accuracy information correction parameters (AIC, BIC, AICc) are used to compare the prediction methods. Smaller the numerical value of



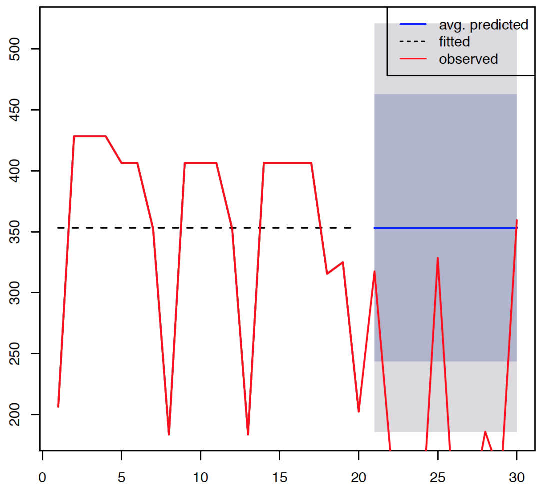
(a) uptime(%)



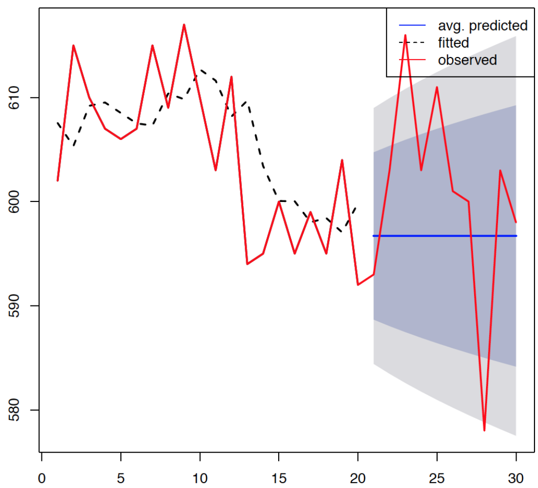
(b) downtime(seconds)



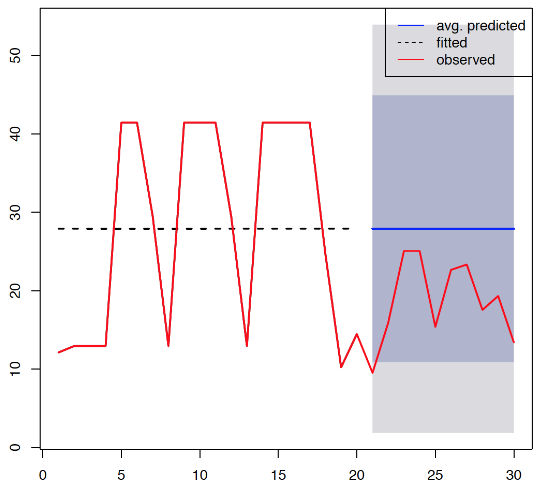
(c) Outage Frequency (times)



(d) Latency(ms)

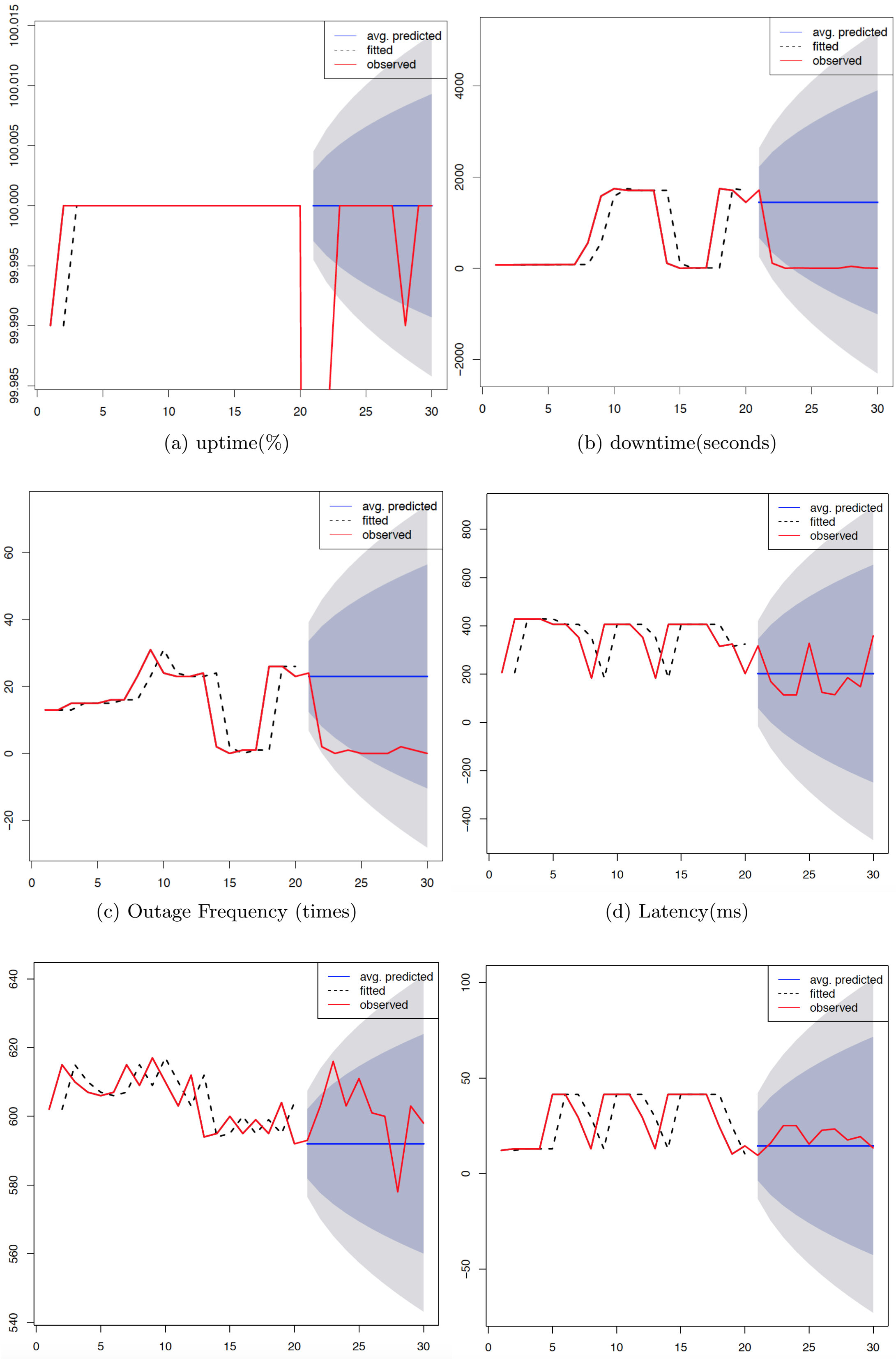


(e) Responsetime(ms)



(f) Throughput(Mbps)

Figure 7.27: Service Performance Prediction of Digital Cloud using ETS



(a) uptime(%)

(b) downtime(seconds)

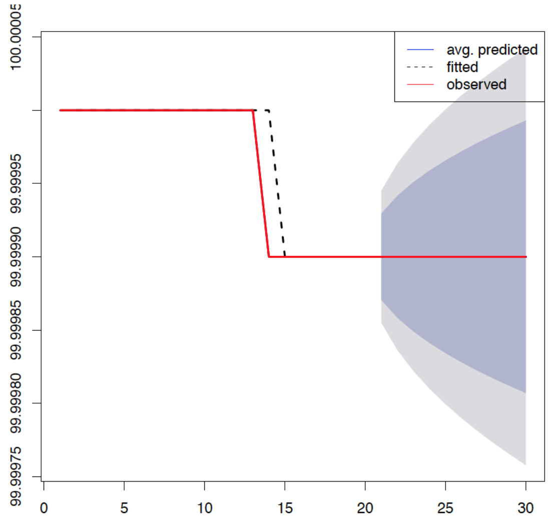
(c) Outage Frequency (times)

(d) Latency(ms)

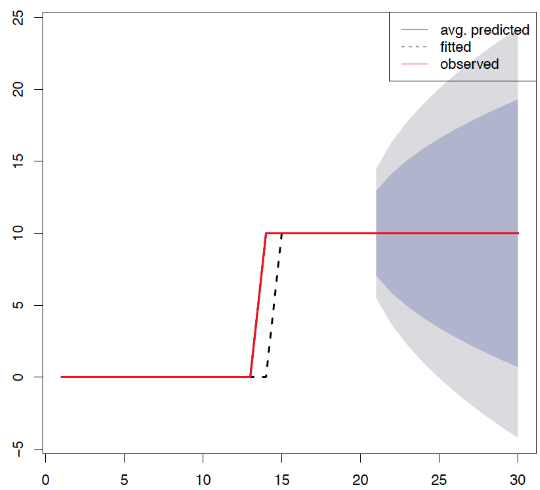
(e) Responsetime(ms)

(f) Throughput(Mbps)

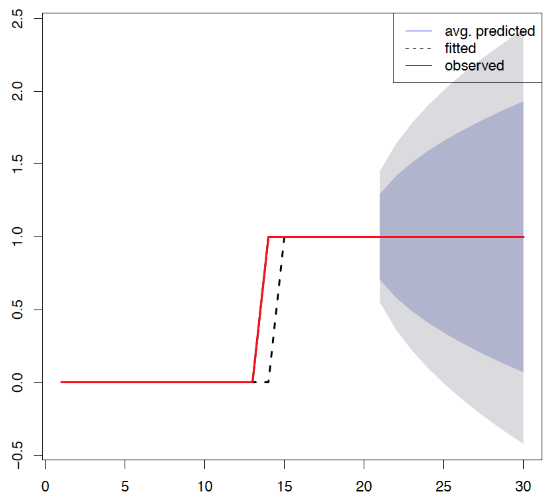
Figure 7.28: Service Performance Prediction of Digital Cloud using ARIMA



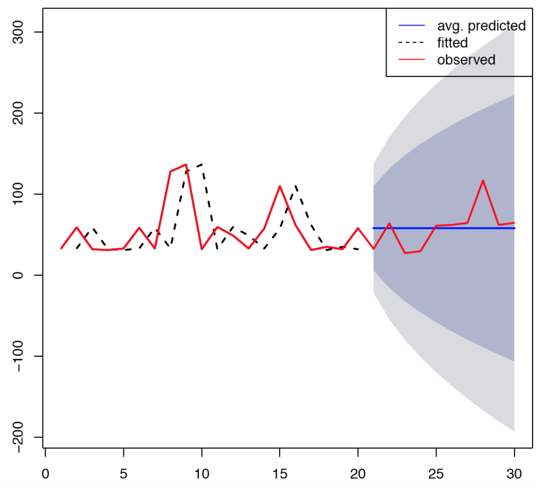
(a) uptime(%)



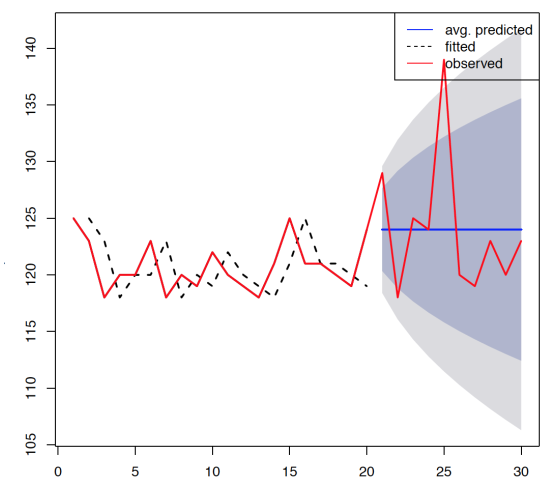
(b) downtime(seconds)



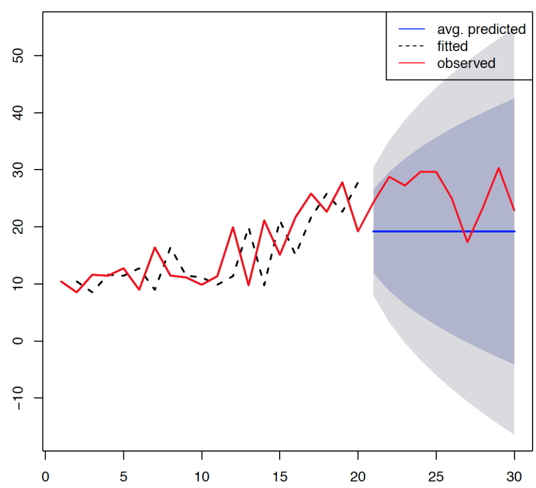
(c) Outage Frequency (times)



(d) Latency(ms)



(e) Responsetime(ms)



(f) Throughput(Mbps)

Figure 7.29: Service Performance Prediction of Exoscale Cloud using ARIMA

information parameters signifies the better prediction method.

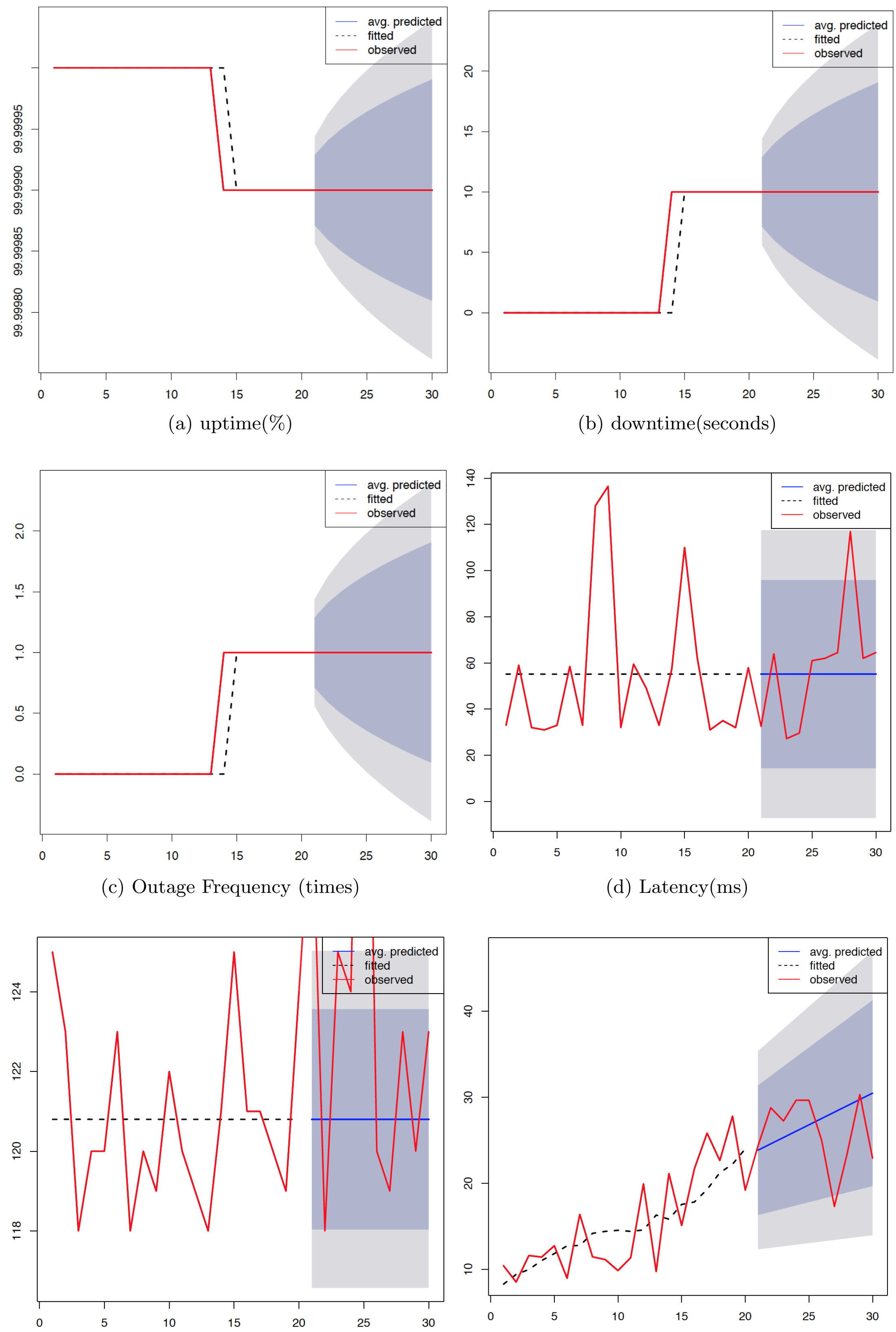
Similarly, error measures of all performance parameters of all the 20 cloud providers are calculated. Prediction results of *uptime*, *downtime* and *outage frequency* are more stable in most of the cloud providers than the rest of the parameters: *latency*, *responsetime* and *throughput*. We chose *Digital Cloud* and *Exoscale Cloud*, to cover all the parameters prediction analysis, because they both have unstable service performance result in all the selected parameters. MASE value of in all predictions was less than or equal to 1 in both ETS and ARIMA prediction technique (except in parameter *Throughput* in ETS predictions with slightly greater than 1))(See Table 7.19). It shows that our selected prediction models are correct. Information correction parameters measured in ETS and ARIMA method shows that ARIMA method is more suited than ETS method (See for instance in Table 7.19 where all values of information correction(IC) have greater in ARIMA method than ETS), however, IC values in each prediction methods are very close with each other.

Table 7.19: Errors Measurement in Performance Prediction of Digital Cloud

Method	Parameters	ME	RMSE	MAE	MPE	MAPE	MASE	ACF1	AIC	AICc	BIC
ETS	Uptime	-1.5E-7	1.2E-3	9E-4	-1.9E-7	9E-4	1.08	-2.6E-2	-181.2	-180.5	-179.2
	Downtime	68.71	590.2	273.3	-inf	Inf	0.95	0.094	319.1	319.8	321.12
	outagefrequency	0.4996	8.03	4.00	-inf	Inf	0.95	0.01	147.2	147.9	149.27
	Latency	-0.02	85.57	70.44	-9.05	26.09	0.98	0.04	241.8	242.59	243.88
	Response Time	-1.35	6.37	5.06	-0.23	0.84	0.76	-0.16	137.92	138.6	139.9
	Throughput	2.5E-2	13.27	12.49	-34.06	64.52	1.32	0.40	167.3	168.0	169.3
ARIMA	Uptime	5E-4	2.2E-3	5E-4	5E-4	5.2E-4	1	-0.002	-175.0	-174.8	-174.08
	Downtime	72.31	605.54	287.68	-inf	Inf	1	0.09	299.3	299.6	300.3
	outagefrequency	0.52	8.24	4.21	-inf	Inf	1	0.01	136.0	136.3	137.03
	latency	-0.21	111.2	71.4	-7.62	24.9	1	-0.25	234.9	235.2	235.9
	response time	-0.5	7.88	6.63	-0.0966	1.097	1	-0.5	134.3	134.6	135.31
	throughput	0.123	14.09	9.4	-15.96	41.42	1	-0.09	156.4	156.7	157.41

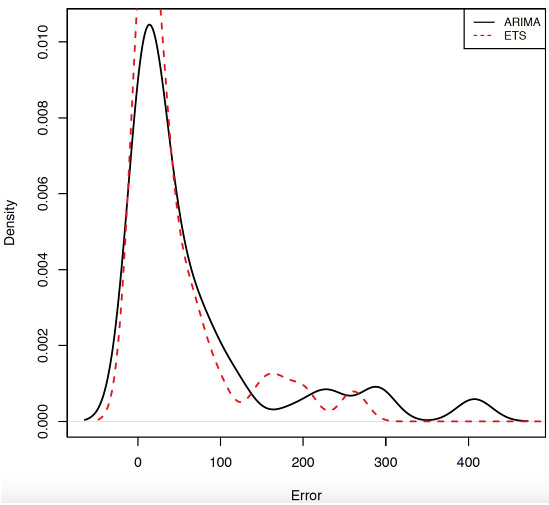
Table 7.20: Errors Measurement in Performance Prediction of Exoscale Cloud

Method	Parameters	ME	RMSE	MAE	MPE	MAPE	MASE	ACF1	AIC	AICc	BIC
ETS	Uptime	-3.3e-6	1.8e-5	3.3e-6	-3.3e-6	3.3e-6	0.96	-0.03	-548.6	-548.1	-545.8
	Downtime	0.33	1.8	0.3	-Inf	Inf	0.96	-0.03	142.1	142.5	144.9
	outagefrequency	3.39E-2	0.18	0.03	Inf	Inf	0.96	-0.03	4.0	4.4	6.8
	Latency	-0.01	29.6	21.6	-23.6	44.1	0.78	0.21	309.3616	309.8	312.1
	Response Time	2.2E-2	4.113	2.8	-0.103	2.2	0.72	0.03	190.8	191.33	193.68
	Throughput	-2.8	11.2	9.04	-36.3	53.8	1.13	0.3	248	250.6	255
ARIMA	Uptime	-3.4E-6	1.8E-5	3.4E-6	-3.4E-6	3.4E-6	1	-0.037	-547.5	-547.4	-546.1
	Downtime	0.34	1.8	0.34	5.8	5.8	1	-0.037	120.2	120.3	121.5
	outagefrequency	0.03	0.18	0.03	5.8	5.8	1	-0.03	-13.3	-13.2	-11.2
	latency	1.08	37.5	27.5	-17.9	54.4	1	-0.3	294.6	294.7	296
	response time	-0.06	5.78	3.93	-0.16	3.18	1	-0.47	186.1	186.3	187.5
	throughput	0.42	5.5	4.6	-2.7	26.9	1	-0.54	183.9	184.1	185.3

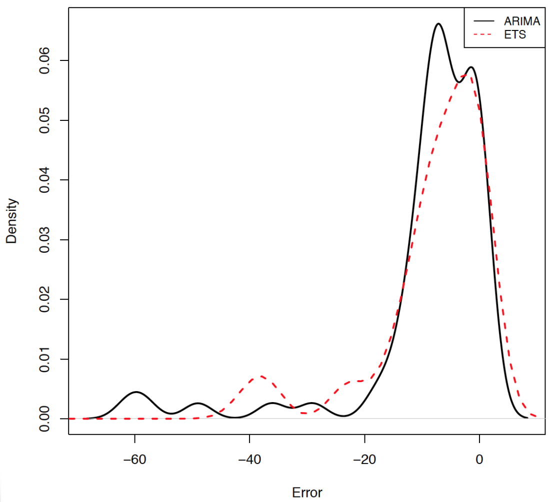


(a) uptime(%)
(b) downtime(seconds)
(c) Outage Frequency (times)
(d) Latency(ms)
(e) Responsetime(ms)
(f) Throughput(Mbps)

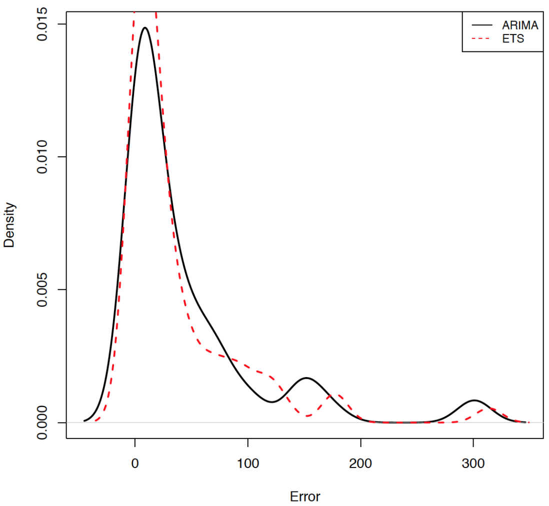
Figure 7.30: Service Performance Prediction of Exoscale Cloud using ETS



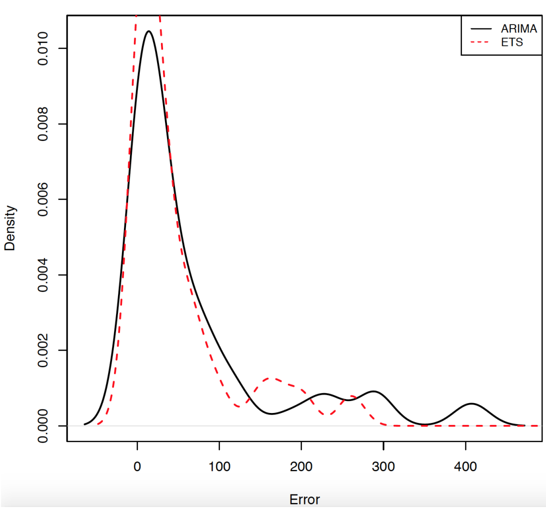
(a) ME



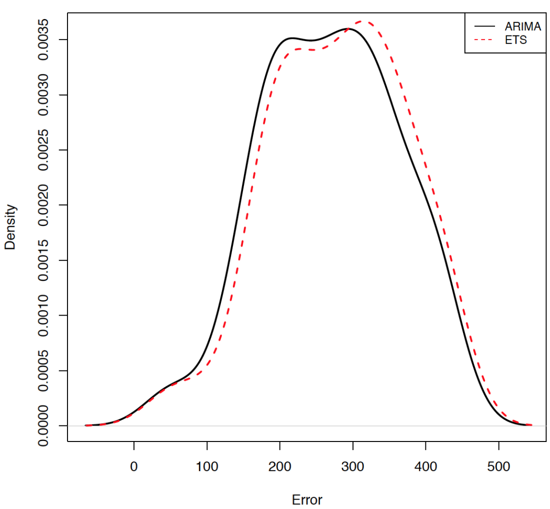
(b) MAE



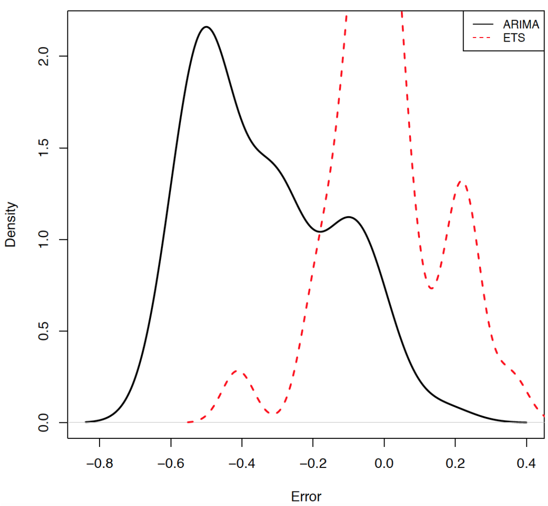
(c) RMSE



(d) MPE

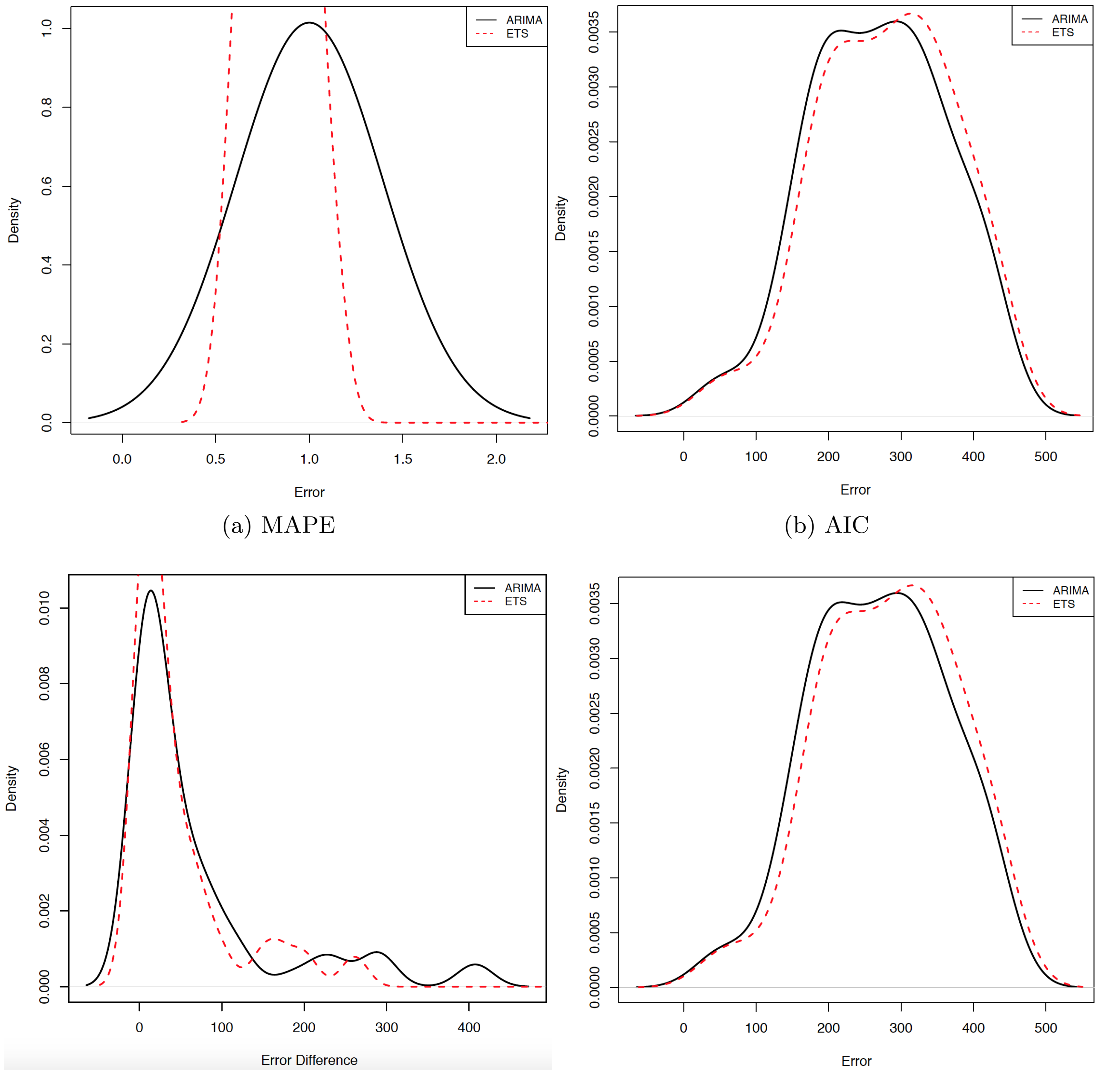


(e) ACF1



(f) MASE

Figure 7.31: Errors comparisions in ARIMA and ETS prediction method of ME, MAE, RMSE, MPE, ACF1and MASE



(a) MAPE (b) AIC (c) BIC (d) AICc

Figure 7.32: Errors comparisions in in ARIMA and ETS prediction method of MAPE, AIC, BIC, AICc

7.8 Errors Measurement and Prediction Accuracy

To evaluate our prediction accuracy, we calculated all error parameters included in Table 7.19 for all 20 selected cloud providers in selected performance parameters. Error patterns of *ME*, *MAE*, *RMSE*, *MPE*, *ACF1*, *AIC*, *BIC* and *AICc* with minimum differences in parameter values in ARIMA and ETS prediction method whereas error patterns are significantly different in error measurement *MASE* and *MAPE*(See Figure 7.31 and 7.32). Most of the error values are near to zero in most of the prediction in *ME*, *MAE*, *RMSE*, *MPE* (See Figure 7.31(a),(b),(c) and d)). Overall information corrections parameters (AIC, BIC, AICc) are lower in ARIMA prediction method than ETS prediction method (See Figure 7.32(b),(c) and (d)). Similarly, *MASE* and *MAPE* have higher values in ETS method than ARIMA method (See Figure 7.31(f) and Figure 7.32(a)). Prediction patterns and related errors calculated to evaluate the prediction method shows that both prediction methods (ARIMA and ETS) are suitable to predict performances of cloud providers according our data patterns collected from multiple cloud providers. However, in comparisons with ARIMA and ETS, ARIMA prediction method gives more smooth prediction than ETS method.

7.8.1 Matching predicted performances with actual measurement

To match with the predicted patterns of the CSPs' service performances, we trained performance pattern of 20 days collected from different cloud providers. Red line (See in Figure , 7.27, 7.28, 7.8.1 and 7.29) gives the actual patterns of the service preformance, dark blue line gives the average predicted performance (point of forecast), dotted black line gives the fitted patterns of actual performance measured for 20 days. The forecast intervals are at 80% to 95%. Lower forecast range at 80%(Low80) to high forecast range at 80%(High80) is shown in light blue background and 95% forecast interval (Low95 (lower forecast range at 95%) to High95 (high forecast range at 95%))

is shown in light black background give the minimum to maximum range of prediction of cloud provider performance. To evaluate the accuracy of the prediction of the CSPs' service performance, we trained the system by 20 days performance data collected from different cloud providers. In most of the predicted performance patterns followed with actual performance patterns in *Digital Cloud* and *Exoscale Cloud* as shown in predicted patterns.

In the analysis of performance prediction pattern of *Digital Cloud*, predicted pattern of *latency* by ARIMA method is more close to observed pattern than the predicted pattern in ETS method (See in Figure 7.27, 7.28, 7.29, and 7.8.1). Observed measurement of *uptime*, *Latency*, and *Responsetime* of *Digital Cloud* is out of prediction range for very limited period in ETS method (See in Figure 7.27) whereas observed performance pattern is within the range of Low80 in ARIMA method (See in Figure 7.28). See, for instance, in Figure 7.29, and 7.8.1) observed measurement pattern of *throughput* followed the almost same pattern as average predicted pattern by ARIMA method but observed measured value range is in between average predicted value to Low80 value in ETS method. Similarly, predicted patterns of service performances of all selected cloud providers are analyzed. *MAPE* value in all prediction ranges from 0.55-15% in most of the predictions. *MASE* values are equal to 1 in ARIMA prediction and less than or near to 1 in ETS method.

7.8.2 Conclusions

This section provides the forecasts of future service performance of cloud service providers. The input for the method is the previously observed performance. The method selected to produce the predictions are ETS and ARIMA. For evaluation, the real monitoring data was divided into training and test sets. Both prediction method returned the convincing results of performance prediction, however, ARIMA method gave better performance prediction results than ETS method, as shown by the analysis of the errors of the prediction methods. The method presented in this paper summarizes the current and future service performance of cloud providers for the selected performance metrics. It helps cloud service users and brokers to choose cloud services according to their requirements. Predicted service performance results show that prediction is applicable for short duration prediction as well as long-term duration. The future work includes evaluation of service performance over longer time periods and applying other prediction methods such as neural networks.

7.9 Summary

In this chapter, we included the evaluation according environment setup in previous chapter. Firstly, performance of multiple CSPs is measured. These measured values are then compared with the SLA offered by CSPs. The next section includes the evaluation of CSPs using IFL technique and Heat Map technique. These two techniques are further compared in the next section. Next section gives the performance measurement of 20 cloud providers including service pattern analysis. Lastly, performance of the CSPs are predicted based on collected data for the future forecasting of performance of CSPs. Further, the errors in different automatic prediction methods are calculated and compared to evaluate the accuracy of the prediction.

Part V

Regulatory Compliance Analysis of Cloud Providers

Chapter 8

Cloud Service Providers' Regulatory Compliance Analysis

8.1 Analysis of Term of Services and SLA committed by Cloud Service Providers

As cloud providers are increasing, cloud users have opportunities to select specific cloud services from multiple cloud providers. So, cloud broker exists between cloud provider and cloud users to facilitate both for the service delivery. Practically standard contract is feasible for big companies but making standard contract is for each Small Medium Enterprises (SME) for every cloud services is time consuming and costly for cloud providers. Cloud users also do not take more attention to make standard contract for a small cloud service subscription. Many of cloud providers offer online agreement even it is not negotiable and user agrees the terms and conditions of the cloud providers as an "I agree" box or similar at the moment of service initiation. Technically, the SLA agreement between cloud provider and cloud user is the legal document on which basis cloud user can claim for service credit or other incase of service infringement by cloud providers. In this paper an overview of SLA offered by some international cloud service providers. Our observation of SLA agreement offered by most of the cloud providers shows that it is still incomplete and need to be provided detail information related to avoid the conflict between cloud users and cloud providers or any third party involved in service delivery.

Our analysis has two perspectives:

- Analyzing how cloud providers have covered important issues in their contract agreement document including regulatory aspects. It analyzes from the perspectives of sufficient information regarding the safe and fair cloud contract. It includes analysis of from both legal and technical issues to be included in their cloud contracts by cloud providers. Table 8.1 gives the criterion selected to analyze the content terms of service committed by cloud providers.

- Performance analysis of cloud providers according service committed in SLA agreement. It collects the SLA commitments by cloud providers and analyzes with real performance delivered by them according to detail information provided by cloud providers. As many of the cloud providers provide limited information for quantitative measurement in their SLA agreement, the service level objectives: performance service level, security service level and cost of service level objective (See in Figure 2.6) are chosen for the service performance analysis.

8.1.1 Terms of service and SLA provided by International Cloud Providers

Most of the cloud service offers SLA commitments to the cloud users. It is very important to know the complete information of cloud service provider before subscribing cloud services from cloud service providers. SLA contains both measurable and non-measurable parameters. In our observation most of the cloud service providers provide very few information regarding the performance delivery of cloud services to the cloud users. In our observation, most of the cloud providers offer contract terms as "Terms

Table 8.1: Criteria and sub-criteria for evaluating cloud services

Criteria	Sub-criteria	Short Name
Liabilities	Liabilities	*Li*
Performance Service Level	Availability Response Time Capacity	*Av* *Res* *Cap*
Security Service Level	Service Reliability Authentication and Authorization Security incident mgmt Reporting Logging Monitoring	*Rel* *Au* *inc* *Rep* *Log* *Mon*
Data Management Service Level	Data Classification Data Backup, Mirroring and Restore Data Lifecycle and Portability	*Dcls* *BMR* *DLP*
Personal Data Protection Service Level	Code of Conduct Purpose of Specification Openness, transparency and notice Accountability Geographical Location of user data	*Ccon* *Pspec* *OTN* *Acc* *DL*
Provider Lock-in and Exit	Lock-in Exit	*In* *Ex*
Terms and conditions	Terms and conditions	*TC*
Changing Service Features	Changing Service Features	*CS*
Intellectual Property Rights(IPR)	IPR	*IPR*

and condition" and "SLA". Some has in the same document and some as a separate document. In this section, we provide the overview of SLA commitment by the commercially available cloud service providers [119]:

Microsoft Azure: Microsoft Azure[1] offers a specific SLA commitments in multiple services. Its SLA commitments range from maximum 99.9% to 99.99%. It provides the sector/region wise SLA commitments to the cloud users. It has detail information regarding the data transfer, however, information in data privacy and security issues in terms and conditions document is not clearly detailed[2].

[1] https://azure.microsoft.com/en-us/support/legal/sla/summary/
[2] https://azure.microsoft.com/en-us/support/legal/services-terms-nov-2014/

GMOCloud: GMO Cloud[3] offers at least 99.999% monthly uptime for all cloud services. SLA document offered by GMO is not service specific commitments. It provides the details of security and backup, IPR however it is silent in data privacy and governing law. Terms of service put liability to the cloud users to protect their privacy[4]. It provides the detail information of data center locations.

HP Cloud: SLA offer of HP cloud[5] ranges from at least 99.95% to 100% in a specific cloud service. There is limited information of data privacy and security in its terms of service. It's detail information of SLA and terms of service are not easily available, as it is not planning to expand public cloud services further.

Amazon: Amazon provides various cloud services, however, Amazon S3[6] and Amazon EC2[7] are the most popular cloud services of Amazon. It offers at least 99.9% uptime for both S3 and EC2 services. It provides an well organized contract agreement for specific services[8,9]. Offered contract agreement contains detail information in security and data privacy, governing law and IPR.

RackSpace: Rackspace cloud[10] service provider provides a service specific SLA commitment. Monthly uptime from at least 99.9% to maximum 100% is offered in their SLA document. It guarantees the user data privacy according to applicable data protection/privacy law[11]. It also provides a detail information of global security policy.

Google Cloud: Google cloud[12] offers service specific SLA. It ranges alteast 99.9% to 100% monthly uptime based on service offer. It covers most of the important terms in "Terms of Service". Data processing, security terms, compliance with different regula-

---

[3] $https : //www.gmocloud.com/common/download/catalog_iqcloud.pdf$
[4] http://us.gmocloud.com/legal/
[5] http://www.hpcloud.com/sla/
[6] http://aws.amazon.com/s3/sla/
[7] http://aws.amazon.com/ec2/sla/
[8] http://portal.aws.amazon.com/gp/aws/developer/terms-and-conditions.html
[9] http://aws.amazon.com/agreement/
[10] https://www.rackspace.com/information/legal/cloud/sla
[11] https://www.rackspace.com/information/legal/cloud/tos
[12] https://cloud.google.com/

tory frameworks, governing law and jurisdiction are covered in the agreement[13]. SLA monitoring issues are still not clear in the committed document. According to the committed document, it is possible to choose data center according to users preferences in different locations.

City Cloud: City cloud[14] offers a SLA commitment at least 100% monthly uptime in all the services irrespective with specific cloud services. It does not provide detail terms of service related to security and data privacy, governing law and jurisdiction. It provides the geo-locations of data centers and monitoring facility of cloud services.

Cloud Sigma: Similarly, Cloud Sigma[15] also offers at least 100% monthly uptime irrespective with a specific service. Terms of service detail liability, privacy policy, IPR, governing law and jurisdiction[16]. It also provides an information related to data center locations. However, terms and conditions are not clear enough as recommended by standard cloud contract guidelines.

Elastic Host: Elastic Host[17] provides a service specific SLA offer ranges from at least 99.95% to 100%. It has lack of specific details in privacy and security issues in the provided SLA agreement and put more liabilities to the users. Proposed agreement is specific in governing law and jurisdiction.

Century Link Cloud: Century Link Cloud[18] is very specific in SLA document. It commits 100% uptime for public/private networks and at least 99.9% for rest of the services. It provides privacy policy[19], data retention issues, Governing law and jurisdiction, however, it is not specific in data liability and other issues, which are necessary to make a safe and fair cloud contract. It provides data center locations in its website.

[13] https://cloud.google.com/terms/
[14] https://www.citynetworkhosting.com/sla/
[15] https://www.cloudsigma.com/features/
[16] https://www.cloudsigma.com/legal-switzerland/
[17] https://www.elastichosts.com/terms-of-service/
[18] https://www.ctl.io/legal/sla/
[19] https://www.ctl.io/legal/privacy/

Digital Ocean: However, Digital Ocean[20] does not provide specific SLA commitments according to the service offers, it provides at least 99.99 % monthly uptime in network, power and virtual server availability. The offered document provides information related to the liabilities, governing law, data privacy but a detail related to physical security is still missing in the document.

GoGrid Cloud: GoGrid Cloud[21,22] provides a very specific SLA commitment for each cloud service. It also provides regional wise specific performance matrix in its SLA document. It is more specific in privacy and security issues, IP and third party offerings and choice of law and jurisdiction; however, it does not take more liabilities in user's data.

UpCloud: UpCloud[23] commit minimum 100% monthly uptime to all services irrespective to specific cloud service. Terms of service is not clear on data security and privacy, governing law & jurisdiction and data locations[24].

IBM Cloud: IBM does not provide a specific service wise SLA metrics. Terms of service of IBM is well organized and provides the details of security descriptions, data protection, conditions of transboarder data flow and information regarding the governing law and jurisdiction[25]. It also provides information of data center locations.

Exoscale Cloud: Exoscale cloud provides 95.95% availability in all services[26]. Terms of service are well described and clear. Document is specific on data security (however, it takes less liabilities), data protection and privacy, governing law and jurisdiction, data storage and IPR.

Baremetal Cloud: It provides 99.999% availability unspecific with a cloud service.

[20]https://www.digitalocean.com/legal/terms/
[21]https://www.datapipe.com/gogrid/legal/sla/
[22]https://www.datapipe.com/gogrid/legal/terms-of-service/
[23]https://www.upcloud.com/blog/how-seriously-does-your-cloud-hosting-provider-take-redundancy/
[24]https://www.upcloud.com/documentation/terms/
[25]https://www-03.ibm.com/software/sla/
[26]https://www.exoscale.ch/terms/

The SLA and terms of service[27] provided is not sufficient on data privacy, provider's liabilities, however, it provides an information related to physical level security and data center locations.

Arubacloud: Aruba cloud provides at least 99.95% availability to all cloud services except 100% in power and air conditioning[28]. It provides detail information on processing of personal data with specific applicable law, jurisdictions and competent but it provides the less information regarding the security issues from technical point of view. It also provides an information related to data center locations and service monitoring details.

Softlayer Cloud: It does not provide a SLA commitment specific with particular services. In SLA agreement document, it uses a sentence "SoftLayer will use reasonable efforts to provide a service level of 100% for the public/private network..." but it guarantees a service credit more than 2 hours[29]. It is not clearly mentioned how it is provided, however, it agrees to maintain reasonable and appropriate measures related to physical security to protect user content[30]. The document is specific on data protection and privacy, governing law and jurisdictions. It also provides geographical locations of data centers.

Vaultnetwork Cloud: The Vault network cloud endeavors to have service(s) available for access by any party in the world 99.5% of the time[31]. Provided document does not detail security, data privacy and protection issues. It is specific on governing law and jurisdictions.

CloudCentral: It commits 99.95% uptime commitment to infrastructure services[32]. The terms and conditions[33] are clear in liabilities, governing law and IPR but there is

[27] https://www.baremetalcloud.com/legal-terms
[28] https://www.arubacloud.com/company/general-conditions.aspx
[29] http://static.softlayer.com/sites/default/files/sla.pdf
[30] http://static.softlayer.com/sites/default/files/assets/page/Terms-of-Service.pdf
[31] https://www.vaultnetworks.com/about/company-policies/terms-of-service/
[32] https://www.cloudcentral.com.au/sla/
[33] https://www.cloudcentral.com.au/terms-and-conditions/

not sufficient information on data privacy and physical security.

8.2 Legal and/or Major Missing Points in the Current Cloud Contracts Offered by Cloud Providers

The details of cloud contracts mentioned by multiple cloud providers are provided in section 8.1.1. We list out here some missing points, which are not properly addressed by cloud providers in their agreement, and some are against the regulatory framework as mentioned in section 4.3, as important issues to be included in cloud contracts.

1. Lack of Liabilities and Indemnity

   Most of the providers claim their entire liability according to the charge paid by user or maximum amount. This is limiting or excluding legal rights of the user could be considered under some law (for instance under EU law it is considered as unfair contract [47])

2. Consent for the collection and processing of personal data for secondary non-compatible purposes

   Information is collected from cloud users for the internal purposes, such as billing or management of its cloud services, gathered by CSPs will belong to them (CSPs) [117] but these information should not be used for the unfair advantage. In our analysis most of the providers do not mention theses issues in the terms of service but some provider still use these information for other purpose without particular consent from data subject [12].

3. Lack of Transparency As we already discussed, there is lack of a standardized format and terminology of cloud contract in cloud computing. Cloud provider prefers to include terms according to their feasibility in the committed terms of service and SLA. Unclear and sometimes unfair terms of service in the cloud con-

tract misguide the rights of cloud users in contract breaching. Lack of clearly monitoring technique in SLA, hidden payment obligation, automatic renewal occurs due to unclear terms of service in the cloud contract.

4. SLA agreement

   a. Lack of Service Monitoring

   User pays as per usage in cloud computing. So, service credit and other claim will be authorized according to the SLA agreement. Many of the contract terms do not mention about the methods of service monitoring. SLA monitoring is challenging issue in recent days because it is observed that all the cloud service provider may not provide services to the user according to their SLA commitments [136].

   b. Disaster Recovery

   In the most of the contract document, how CSPs manage disaster recovery for the services is not clear. Well-managed disaster recovery plan is very significant criteria for users to select appropriate CSP.

   c. Location of Data

   In our observation, many of the CSPs provide information related to data center location in their website. Cloud users can choose appropriate location according to their requirements but these information are not still part of the terms of service and SLA.

   d. Data portability, Data irretrievability

   Very few CSPs provide the information related to data portability and irretrievability. Cloud users should be easily able to retrieve their data if they prefer to switch to another CSP due to any reason.

Sometimes, it is hard to follow these points to most of the cloud users, who are not aware with existing legal framework or users do not have sufficient legal knowledge to follow the legal framework. In the next section, we propose how performance evaluation technique (Heat Map technique) can be implemented to check the regulatory compliance status of the CSPs. Heat Map table gives complete information of regulatory compliance status of the CSPs in a visualized form.

8.2.1 Pictorial Analysis of Cloud Provider's Contracts in HeatMap Table

SLA assured service brokering framework is proposed in [138]. This framework recommends the cloud services to the user with verified service performance delivery against the SLA commitments of CSPs. Wagle et al. [134] and [136] proposed evaluation techniques to evaluate the service performance of the CSPs. These papers are mainly focused on service performance analysis of the CSPs. In cloud computing, specifically in a public cloud scenario, regulatory compliance management is also critical issue as the cloud users outsource data processing and storage to CSPs that can be under legislation/regulation [127]. E Casalicchio et. al [41] have introduced a conceptual framework for legal compliance checking in cloud brokering but it does not give clear picture of regulatory compliance status of the CSPs. Information of service performance status including regulatory compliance status facilitates cloud users in decision making to choose appropriate CSPs according to their requirements. The main motivation of this paper is analyzing the regulatory compliance status of the CSPs. We implement a Heat Map technique [29],[30], [136] proposed for service performance evaluation to evaluate the regulatory compliance status of the cloud providers.

In the Heat Map technique, potential CSPs are sorted into marginal performance quantile classes to rank the CSPs with multiple performance criteria in increasing order or decreasing order [136]. Performance quantile class is associated in the color form *dark red* (worst) to *dark green* (best) for the performance heat map visualization (See the color legend for 7-tiles in Table 8.3). We have considered major parameters described in section 4.2. All the information is taken from their websites. The developed heat map table gives a visualized table in what extent CSPs are accepting regulatory compliance in their contract document.

We assign 0 to 3 ordinary levels according to detail specification provided in the SLA document, terms of service and so on. If there is not any information provided, we assign 'NA' in that particular parameter [119]:

- 3 - "Available, complete and included all the points",
- 2 - "Available, sufficient and missing some points",
- 1- "Avaiable, insufficient and missing some points",
- 0- "Availale, insufficient but not clear points"
- 'NA' - "Not Available"

We assign corresponding ordinal level according to fair and transparent contract document they have committed to the users (See Table 8.1). The proposed visualized table gives an idea to cloud users, cloud service brokers and regulatory bodies; how CSPs are aware of regulatory compliance in contractual terms in cloud computing. First row in the Table 8.3 gives the criteria of the evaluations. Second row represents the weight of the criteria. However, different weights can be assigned for the evaluation according to the evaluator requirements, we have assigned equal weight in each sub-criteria considering all criteria are equally important. **tau** value represents the dominancy level of sorting (for instance 0.52 is dominancy level in this case). However, non of the CSPs the complete information to make safe and fair contract, cloud providers *Amazon*, *Google Cloud Storage* and *Microsoft Azure* give more information in their contract document than other cloud providers in selected providers in this regulatory compliance analysis (See Table 8.3). The ordinary levels and heat map table presented in this section is only for explanatory purposes (See Table 8.3) and should not be considered in any case as conclusive because expressing legal issues in quantitative value is not straightforward. It is worthwhile to mention here that this paper is only concerned with transparency level in terms of their contract document in their website according to the current legal framework and does not check the service performance level of CSPs.

8.2.2 Concluding Remarks

Cloud contract is the most important legal binding document, which ensures fair and safe to all parties before delivering or receiving services in cloud computing. Obviously, it is not possible to cover all the terms and conditions in the contract document but it should be clear enough and fair for all parties involved in the agreement. Current cloud contract committed by CSPs seems it is not sufficient as a fair and safe and transparent cloud contract. The literatures, recommendation of different independent bodies and analysis of terms of service and SLA agreement committed by CSPs show that cloud users are still not convinced with the current cloud contracts. The heat map table presented in this paper gives the position of CSPs according to their regulatory compliance status in their contract document. Visualized table of this information committed by the cloud service providers helps cloud users to choose appropriate CSP according to their requirements and also helps cloud service broker to recommend CSPs according to users' requirements. The potential future work includes the implementation of proposed heat map technique in SLA assured service brokering framework [138], which covers both service performance status and regulatory compliance status in service recommending to the users.

8.3 DPIA

Data protection impact assessment (DPIA) is carried out to assess potential harm to individuals as well as the risks related to carrying out processes [4]. The aim of DPIA is to identify the main risks of a project with respect to the rights of data subjects concerning their personal data [18], [27]. In the revised European data protection regulation (GPDR), data protection impact assessment is going to be mandatory for organizations in certain situations. Organizations have to carry out the DPIA once the new GPDR is in effect[34]. In this section, we provide the data protection impact assessment of decision recommendation tool that is intended to process the data from multiple cloud providers to recommend cloud services to the cloud service users. For the impact assessment, we referred the questionnaire proposed in A4Cloud project [4]. This questionnaire is based on a legal and socio-economic analysis of privacy issues for cloud deployments including analysis of the EU Data Protection Directive (DPD)[35], the proposed EU GPDR, the UK Information Commissioner's Office's (ICO) PIA Handbook[36], and the PIA Guide of the Office of the Australian Information Commissioner (OAIC)[37]. The questionnaire does not assume that the user is familiar with certain basic data processing notions such as "personal data" but rather helps the user in identifying whether personal data is being processed. It also considers the protection of data subjects as the core of its assessment [18].

[34] COM 11 final 2012/0011 (COD) European Commission: Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Brussels, 25.1.2012 p. 1. (2012)

[35] Directive 95/46/EC of the European Parliament and of the 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 OJ L281/31 (DPD) (1995)

[36] Information Commissioner's Office: Privacy Impact Assessment Handbook, $http://ico.org.uk/pia_handbook_html_v2/files/PIAhandbookV2.pdf$ (2011)

[37] Australian Government, Office of the Australian Information Commissioner: Privacy Impact Assessment Guide (OAIC) (2010)

8.3.1 Privacy Risk Indicators

Mainly seven privacy indicators are chosen for the data protection impact analysis [A4cloud]:

1. Sensitivity (SEN): Risks related to a sensitive market (i.e. elderly, children, etc.) and/or sensitive data (i.e. health or medical conditions, finance, sexual behavior)
2. Compliance(C): Risks related to compliance with external standards, policies, laws, etc.
3. Trans-boarder Data Flow (TB): Risks related to transfer of information across national borders
4. Transparency (T): Risks related to transparency in the areas of notice/user messaging and choice/consent
5. Data Control (DC): Risks related to control of the data lifecycle (i.e., collection, usage, quality, and/or retention)
6. Security (SEC): Risks related to security of data and data flows
7. Data Sharing (DS): Risks related to sharing data with third parties

To analyze the data protection impact, initially, we undertook with screening questionnaires and performed further questionnaire in details. Table 8.4 and Table 8.5 show the detail answers of screening questionnaire and further detail answers of questionnaire respectively.

8.3.2 Major Risks and Precautions to be Performed

The nature of the decision recommendation tool we have proposed, however, personal data are not directly processed from individual consumer, it monitors the service performance data of multiple cloud service providers as well as regulatory compliance check of them according to the current legal framework. These data are gathered from multiple locations. In the DPIA screening questions, necessity of DPIA is identified in such circumstances of the recommendation tool. Further impact assessment, with the questionnaires recommended by A4cloud project [4], is performed and the following major risks are identified in:

- Compliance [C],
- Sensitivity [SEN],
- Data Control [DC] and
- Data Sharing [DS].

The main sources of information of cloud service provider for regulatory compliance status analysis are Cloud service providers' available manifests including documents related to Terms of service, Service Level Agreements (SLAs), security practices, privacy policies, the cloud documentations on getting started and other user guides and FAQs, and commercially available cloud monitoring tools, particularly Cloud Harmony [5]& Monitus citeMonitis to analyze the service performance of the cloud service providers. Both monitoring tools are aware of the current legal framework in collecting information from cloud service providers and individual user[38] [39]. While collecting regulatory compliance status and service performance status of cloud service providers, we followed the standard data collection mechanism according to current legal framework to prevent the probable Compliance [C] risk in cloud computing. Another risk indicator Sensitivity [SEN] is comparatively lesser effective than Compliance [C] risk because the decision recommendation tool is not directly involved with the individual information. The personal information collected by third party is aware of Sensitivity [SEN] risk and follow the necessary precaution to collect individual's personal data. In the tool,

[38]https://cloudharmony.com/vendor
[39]http://www.monitis.com/privacy-cookies-policy

lifecycle of data is for certain time period (for instance, over a month or year) and data is shared only within the known parties. So, the tool has already considered the prevention method to minimize the risk of Data Control (DC) and Data Sharing (DS). Another possible risk in our tool might be the Trans-boarder Data flow (TB), which needs to be carefully managed while transferring information across national boarder or especially outside the EEA region. Service performance of cloud service provider is transparently monitored and will be shared to known third parties. So, Transparency (T) risk is less effective in the recommendation tool. However, the recommendation tool does not have strict data security policy (signatures, hashes, encryptions, it has sufficient security provision for the data and secure enough within the system. So, it is less risky in Security (SEC) risk indicator.

8.4 Summary

In this chapter, terms and conditions and SLA committed by cloud providers are analyzed in the first section. In the next section, missing points in terms of service and SLA are discussed. This information is realized in the heat map table to provide the transparent pictorial view of regulatory compliance status of the cloud providers. In the last section, DPIA assessment is carried out to assess potential harm to individuals as well as the risks related to carrying out processes in decision recommendation tool proposed in the thesis.

Table 8.2: SLA offered by International Cloud Providers

SN	Cloud Provider	SLA offer	Last Update/ Revised	
1	Microsoft Azure	99.99% Storage , 99.9% for Azure Active Directive, 99.95% for API management, App Service, Cloud Services and VM, DB, 99.9% App Gateway, Backup, Cache, CDN	2015-09-01	
2	GMOCloud -US	99.95%	2012-12-04	
3	HP Cloud	100% HP cloud DNS, 99.95 compute, Block/object Storage, CDN		
4a	Amazone S3	Amazon S3 99.9%	2015-09-16	
4b	Amazone EC2	Amazon EC2 99.9%	2013-06-01	
5	Rackspace	100% Network Availability, DC HVAC (Heating, Ventilation and AC) and Power, Cloud Server Host including hypervisor, 99.9% Cloud Block Storage,	2015-07-24	
6	Google Cloud	Monthly Uptime 100% DNS, 99.95% in computing, Cloud SQL, cloud Services, 99.9% in Cloud Storage, Prediction API, BigQuery cloud Services,	2015-12-17	
7	City Cloud	100% uptime by city networks		
8	Cloud Sigma	100% uptime reference point		
9	Elastic Host	99.95% in Elastic Computing Services 1x the cost of resources unavailable,		
10	Centurylink	100% uptime for Public Network, Private Network, 99.99% in Control Portal and API, Virtual Servers, 99.9% in Bare Metal Servers, Managed OS, Object Storage,	2015-10-01	
11	Digital Ocean	99.99% uptime SLA around network, power and virtual server availability		
12	GoGrid	100% in Server Uptime Persistent Storage, Network Performance: Internal/External Cloud Storage Server Reboot Support Response Time Domain Name Physical Services Security 24 x 365 Engineering Support	22/11/ 2013	
13	UpCloud	100% uptime in all the services	04/04/2012	
14	IBM	no specific SLA metrics	09/2014	
15	ExoscaleCloud	99.95% uptime in all the services	01/04/2016	
16	Baremetal Cloud	99.95% uptime in all the services	01/04/2016	
17	Aruba Cloud	99.95% minimum uptime in all services		
18	Softlayer Cloud	100% availability in all networks	03/2016	
19	Vaultnetwork Cloud	99.5% minimum uptime in all services		
20	CloudCentral Cloud	95.95% minimum uptime in all services		

Table 8.3: Pictorial View of Cloud Contracts offered by International Cloud Service Providers

criteria	Acc	BMR	Mon	Log	Rep	OTN	inc	Au	Rel	DL	Li	IPR	Ex	In	Res	TC	Pspec	Ccon	DLP	Dcls	Cap	Av	CS
weights	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33
tau(*)	0.52	0.52	0.52	0.52	0.52	0.50	0.49	0.49	0.49	0.34	0.26	0.09	0.04	0.04	0.02	0.00	0.00	0.00	0.00	0.00	0.00	-0.06	-0.34
Amazon Cloud	3	3	3	3	3	3	3	3	3	3	3	3	2	2	1	3	3	3	NA	NA	NA	3	0
Google Cloud Storage	3	3	3	3	3	3	3	3	3	3	2	3	0	0	1	3	3	3	NA	NA	NA	3	2
Microsoft Azure	3	3	3	3	3	3	2	2	2	2	2	2	1	1	1	3	3	3	NA	NA	NA	3	1
Aruba Cloud	3	3	3	3	3	3	3	3	3	3	0	2	0	0	1	3	3	3	NA	NA	NA	3	0
IBM Cloud	2	2	2	2	2	2	3	3	3	3	2	2	0	0	1	3	3	3	NA	NA	NA	2	0
City Cloud	3	3	3	3	3	3	1	1	1	3	2	2	0	0	1	3	3	3	NA	NA	NA	3	2
Rackspace Cloud	0	0	0	0	0	0	3	3	3	0	3	3	1	1	1	3	3	3	NA	NA	NA	3	1
CenturyLinkCloud	1	1	1	1	1	1	1	1	1	3	3	1	0	0	1	3	3	3	NA	NA	NA	3	2
Gogrid Cloud	0	0	0	0	0	0	2	2	2	3	0	3	1	1	2	3	3	3	NA	NA	NA	3	3
ExoCloud	0	0	0	0	0	0	3	3	3	3	0	3	0	0	1	3	3	3	NA	NA	NA	3	3
BareMetal Cloud	0	0	0	0	0	0	3	3	3	0	1	2	0	0	1	3	3	3	NA	NA	NA	3	2
SoftLayer Cloud	0	0	0	0	0	0	2	2	2	3	1	1	1	1	1	3	3	3	NA	NA	NA	3	NA
UpCloud	0	0	0	0	0	0	1	1	1	3	2	2	1	1	1	3	3	3	NA	NA	NA	3	2
Elastic Host	0	0	0	0	0	0	2	2	2	0	1	3	0	0	1	3	3	3	NA	NA	NA	3	2
DigitalOcean Cloud	0	0	0	0	0	0	2	2	2	2	1	2	0	0	1	3	3	3	NA	NA	NA	3	2
Cloudcentral Cloud	0	0	0	0	0	0	1	1	1	0	1	3	1	1	1	3	3	3	NA	NA	NA	3	NA
Cloud Sigma	0	0	0	0	0	0	1	1	1	3	1	2	0	0	1	3	3	3	NA	NA	NA	3	2
HP Cloud	0	0	0	0	0	0	1	1	1	0	1	2	1	1	1	3	3	3	NA	NA	NA	3	2
VaultNetwork Cloud	0	0	0	0	0	0	1	1	1	0	2	1	0	0	1	3	3	3	NA	NA	NA	3	2
GMOCloud-US	0	0	0	0	0	0	0	0	0	0	0	3	1	1	1	3	3	3	NA	NA	NA	3	2

Color legend:

quantile	0.14%	0.29%	0.43%	0.57%	0.71%	0.86%	1.00%

(*) tau: Ordinal (Kendall) correlation between marginal criterion and global ranking relation.

Table 8.4: Answers of DPIA Screening Questions

No	Explanation		Risk Indicator
1	The information can be used associated to particular name of the cloud service provider		
2	The information processed does not directly reveal certain characterestics of individuals		
3	The information fall under the following particularly sensitive nature: a. Location of Data		
4	Scale of processing operation	Large	
5	The nature of activity is monitoring of the publically accessible data		
6	Third parties are involved in storage, processing, use, or transfer of an information		

Table 8.5: Answers of DPIA Questions

No		Explanation	Score	Wt	Risk Indicator
1	Type of Project	Established in EU Territory			N/A
		Web Browsing+ Service (Delivery)			SEN
		Processing for historical, scientific statistical or research purpose			SEN
2	Collection and use of information	Information of individual is not processed. So, individual consent is not obtained			DC
		Information is not completely relied on consent			DC
		Decisions are made on the basis of historical and current data collected			T C
		Processing is necessary for Performance of contract between two parties Processing is necessary in order for compliance with a legal obligation			N/A
		Different types of information rather than individual information is processed			N/A
		All the information and its subsets handled are necessary to fulfill the purpose of the project			C
		It is possible for the individual to restrict the purposes of processing information			DC C
		Result of the outcome does not have direct effect on individual			SEN
		Nature of operation should not comply with the rules regarding data processing in more than one set of regulations			C
		Information comes from 3rd parties			N/A
		Information processing does not have any discrimination			SEN
		Information is double checked in order to ensure the validity and authenticity			N/A
		Project has data security policy (signatures, hashes, encryptions are not used).			SEC
		Security policy is not updated frequently			
		Information is retained for a certain time			DC
3	Transfer of Information	Information is transferred to the third party as a recommendation but personal data will not disclosed			DS DC DC
		Third parties uses information in a manner consistent with the project purposes			DS DC C
		Information may sell/rent or by or simply disclosing information to third parties			DS
4	Cloud Specific Questions	It is owned by or operated for a specific group of users with common interest in a shared manner (community cloud)			C
		It is also applicable for the end users			N/A

Part VI

Concluding Remarks

Chapter 9

Conclusion and Future Works

In this chapter, we conclude the thesis by summarizing its contributions and their implications for the advancement of multi-cloud service brokering research. We present in Section 9.1 a summary of the thesis contributions, and in Section 9.2 we discuss the constraints of the achieved contributions, and the possible extensions to mitigate them. Finally, Section 9.3 presents the potential future research directions that go beyond this research work.

9.1 Summary

The main objective of this research work is to find an answer to the following fundamental question:

How can a SLA assured service-brokering framework be realized to recommend the cloud services to the users according to their preferences from multi-cloud environment, which is also aware with legal/regulatory compliance check of cloud service provider according to the current legal framework?

In the following, we summarize the contributions achieved throughout this thesis, which answer the above question by addressing the four research questions presented in

Section 1.2. The objective of Research Question 1 is to address the current legal issues to be followed by cloud service provider and cloud service broker according to current legal framework. To address this research question, important issues to be considered in *Terms of Service* and *SLA* commitments offered by international cloud providers are analyzed in chapter 4 and their regulatory compliance status is evaluated and missing points are identified in current terms of service and SLA in chapter 8. The proposed Heat Map algorithm is also implemented to evaluate the regulatory status of the cloud providers. However expressing legal terms in ordinary value is not straight forward, it gave transparent and consistent results to evaluate the regulatory compliance status of the cloud providers. With the General Data Protection Regulation (GDPR) there will be a legal obligation for organizations/projects to conduct a Data Protection Impact Assessment (DPIA) to identity the data privacy risks due to establishment of such organizations/projects. According to the new EU General Data Protection Regulation (GDPR), DPIA is performed to analyze the possible data privacy risks due to our proposed decision recommendation tool. Major potential data privacy risks due to decision recommendation tool and necessary precautions to be performed to minimize those risks are also identified.

To address the Research Question 2, SLA assured cloud brokering framework is proposed in chapter 5, which shows:

1) how can an independent 3rd party cloud auditor/verifier can be realized?

2) how can service performance of CSPs be monitored and compared against the SLA committed by cloud service providers?

3) how can service performance be evaluated based on data/information received from cloud service providers?

4) how can cloud services be recommended according to the requirements of the cloud users? and

5) how can SLA attributed be used to monitor and include both measurable and non-

measurable parameters to evaluate the performance of cloud service providers?

To sort/rank the cloud providers according to the service performance (committed and delivered) of CSPs, two evaluation techniques; IFL technique and Heat Map technique, are proposed, which addresses the Research Question 3. These two techniques are also compared in chapter 7 evaluating both proposed techniques using real service performance data of the CSPs. In the overall performance evaluation of cloud service provider, Heat Map technique gave consistent and transparent result than IFL technique. In IFL technique, importance of criteria and weightage of evaluators can be easily assigned than Heat Map technique. However, in the observation, it is seen in IFL technique that it is extremely guided by the opinion of the most critical performance evaluators. If any user/evaluator provides a very bad feedback to the cloud service provider, it extremely changes the position of the CSP. Due to many reasons mentioned in chapter 7, Heat Map technique is recommended to recommend the cloud services to the cloud users as an independent cloud service broker. Heat Map technique provides a convincing, consensually ranked and transparent multiple criteria performance ranking of commercially available providers, contrary to the IFL evaluation technique. The performance Heat Map is a tool that is more expressive and precise than the IFL technique in case of recommendation of cloud services to the cloud users according to their specific requirements by cloud service brokers. Within this thesis, this tool is also called as decision recommendation tool. Moreover, the performance Heat Map technique also provides more convincing results when numbers of alternatives increases to more than few alternatives.

To recommend cloud services to the cloud users according to their requirements, we analyzed the service delivery pattern of the cloud service providers and predicted future performance behavior of the cloud providers, which helps cloud users in decision making to select the appropriate cloud service provider. This contribution addresses the Research Question 4. Service performance behavior of CSPs is analyzed using monitored data gathered over a month. These data are further used to predict the future behavior of CSPs in chapter 7 using automatic prediction methods. Error calculation in service performance prediction shows that these prediction methods can be implemented to collect the future behavior of CSPs for short time period as well as longer time period.

As discussed in this section, SLA committed, SLA delivered, cloud service user feedback, and regulatory compliance status of the cloud service providers are considered to recommend the cloud service to the cloud users as an independent 3rd party SLA assured service broker in multi-cloud environment. Cloud auditor/verifier module verifies the service performance of cloud provider against the SLA commitment of the cloud service providers.

Overall, this work distinguishes itself from existing research achievements with the following unique contributions:

1. A Generic overview of terms of service and SLA commitments of commercially available cloud providers and acceptable SLA attributes to monitor the performance of CSPs to include both measurable and non-measurable parameters.

2. Verification of service performance delivery of the cloud service providers against the service commitments in the SLA document.

3. Service performance evaluation and position ranking of CSPs according to service peformance delivery.

4. Service performance delivery behavior analysis of CSPs to select the multiple alternative sets of performances according to cloud users' requirements. It also includes the future service performance behavior of the cloud providers, which helps cloud users in decision making to select the cloud services appropriate for them.

5. Regulatory compliance analysis of cloud providers based on information provided in manifests including documents related to terms of service, Service Level Agreements (SLAs), security practices, privacy policies, the cloud documentations on getting started and other user guides and FAQs by cloud service providers. Heat Map technique is also implemented in regulatory compliance analysis of cloud service provider as this technique gave convincing, flexible and expandable result for high decision alternatives with higher numbers of decision criteria.

6. Identify the major risks of a decision recommendation tool with respect to the rights of data subjects concerning their personal data and precautions to be performed to minimize the risks of data privacy rights of individuals .

9.2 Experimental Constraints

In this section, we discuss the constraints of the research contributions achieved throughout this thesis, as stated in Chapter 7.

1. In this thesis work, we measured the performance of the cloud providers using two commercially available performance monitoring tools. This two tools are completely independent with each other and may produce the different results in the same measurement due to different monitoring environment.

2. This research work was mainly based on Luxembourg. So, we considered all the users accessing cloud services are located in Luxembourg. So, values of service performance parameters and results produced due to measured value including performance-ranking positions of CSPs might be completely different than the parameter values and evaluated values presented in this thesis.

3. The service verification delivered by cloud providers are performed according to the service level agreement committed by cloud service providers. We could

verify with the information what CSPs has mentioned in the SLA template and rest of the non-mentioned parameters in SLA template are not possible to verify. This lack of details of Key Performance Indicatorss (KPIs) in SLA template may cause regulatory challenges in cloud computing market and may create conflict between cloud service provider and cloud service users due to lack of sufficient transparency and accountability in information sharing by CSPs.

4. To analyze the regulatory compliance status of the cloud providers, we analyzed the providers' available manifests including documents related to Terms of service, Service Level Agreements (SLAs), security practices, privacy policies, the cloud documentations on getting started and other user guides and FAQs.

9.3 Research Challenges and Future Works

This section presents the research challenges and the future works to be performed in SLA assured service brokering:

- In the proposed SLA assured cloud service brokering framework, there is a provision of collecting feedback from cloud service users while evaluating the performance of cloud service providers to include both measurable and non-measurable parameters. These users' feedback are selected randomly for the evaluation propose as it was time consuming and hard to involve all the feedback of cloud users. The potential future work includes the adaptation of real feedback of cloud users in performance evaluation according to their service experience.

- The thesis work is mainly focused on service performance status and regulatory compliance status analysis of the cloud providers. Cost analysis is also another important factor to provide the optimum set of solutions to recommend cloud services. Moreover, another potential future work includes the service optimization considering the price of cloud products and service committed by cloud service providers [132]. Cloud broker collects service performance measurement of cloud providers along with cost of each cloud services and offers set of solutions to the cloud users applying Non-Dominated Sorting in Genetic Algorithms (NSGA) [52], [124].

- In this thesis work, limited cloud service providers are included to evaluate the results of the proposed evaluation techniques and service performance data of 20 cloud providers are included for the service pattern analysis, regulatory compliance status and future performance behavior analysis with 6 major SLA attributes. In the future work, the proposed framework can be expanded/extended involving the data of maximum cloud service providers and SLA attributes.

- Due to limited resources, service performance of 30 days were included to analyze the service performance patterns of CSPs and future service performance behavior of CSPs are predicted for short time period. Data analysis and information of longer time interval will be more reliable to cloud users. The potential future work includes the monitoring of data over the long time period.

Appendix A

Published Works

1. Shyam S. Wagle, Mateusz Guzek, Pascal Bouvry, and Raymond Bisdorff. Comparisons of Heat Map and IFL Technique to Evaluate the Performance of Commercially Available Cloud Providers. In IEEE 9th International Conference on Cloud Computing(CloudCom), pages —–, San Francisco, USA, June 2016(to appear).

2. Shyam S. Wagle, Mateusz Guzek and Pascal Bouvry. Service Performance Pattern Analysis and Prediction of Commercially Available Cloud Providers. In IEEE 8th International Conference on Cloud Computing, pages —, Luxembourg City, Luxembourg, December 2016(to appear).

3. Shyam S. Wagle, Mateusz Guzek, Pascal Bouvry, and Raymond Bisdorff. An evaluation model for selecting cloud services from commercially available cloud providers. In IEEE 7th International Conference on Cloud Computing(CloudCom), pages 107 114, Vancouver, Canada, November 2015.

4. Wagle, S. S., Guzek, M., and Bouvry, P. Cloud service providers ranking based on service delivery and consumer experience. In 2015 IEEE 4th International Conference on Cloud Networking (CloudNet) (CLOUDNET'15), pages 202-205,

Niagara Falls, Canada.

5. Shyam S. Wagle, "Cloud Service Optimization Method for Multi-Cloud Brokering", IEEE International Conference on Cloud Computing for Emerging Markets(CCEM), Banglore, India, November 2015

6. Shyam S. Wagle, "Optimized SLA Assured Service Brokering (SLaB) and Service Verification in Multi-Cloud Environment ", Workshop on Mathematical and Engineering Methods in Computer Science, Telc, Czech Republic, October 2015.

7. Shyam S. Wagle, "SLA Assured Brokering (SAB) and CSP Certification in Cloud Computing", IEEE/ACM 7th International Conference on Utility and Cloud Computing (UCC), London, United Kingdom, 2014.

8. Shyam S. Wagle, " Cloud Computing Contracts Regulatory Issues and Cloud Providers Offer: An Analysis", IFIP conference on Privacy and Identity Management for the Future Internet in the Age of Globalization, Karlstad, Sweden, 2016.

9. Shyam S. Wagle, "Regulatory Challenges in Cloud Computing in VM Migration outside EEA", IFIP conference on Privacy and Identity Management for the Future Internet in the Age of Globalization, Patras, Greece, 2014.

10. Shyam S. Wagle "Security Framework for VM Migration in Cloud Computing" IFIP conference on Privacy and Identity Management for the Future Internet in the Age of Globalization, Patras, Greece, 2014.

Appendix B

Scripts for Performance Evaluator Using Heat Map

B.1 Performance Evaluator implementation

This appendix provide the exact implementation of the Performance evaluator used for our experiments. It is developed in python and for the sake of clarity we decided to hide all the source code but the main procedure.

```
##################
from decimal import Decimal
from collections import OrderedDict
actions = OrderedDict([
('a02', {'name': 'GMOCloud-US','comment': 'status_down','shortName':'GMO'}),
('a04', {'name': 'Amazon_S3','comment': 'status_up','shortName':'Amz'}),
('a10', {'name': 'Elastic_Host','comment': 'status_up','shortName':'Ela'}),
])
objectives = OrderedDict([
('A', {'name': 'Availability','weight':6.0,'criteria':['1a11','1a12','1a13']}),
('R', {'name': 'Reliability','weight':6.0,'criteria':['1a21','1a22','1a23']}),
('P', {'name': 'Performance','weight':3.0,'criteria':['1a31','1a32','1a33']}),
('C', {'name': 'Costs','weight':4.0,'criteria':['1a41','1a42']}),
('S', {'name': 'Security','weight':3.0,'criteria':['1a51','1a52','1a53']}),
])
criteria = OrderedDict([
('1a11', {'name': 'Uptime', 'comment': 'SLA_delivered_by_external_auditor_1',
'objective': 'A', 'shortName': 'upT',
'weight':Decimal("2.00"),'scale': (Decimal("0.00"),Decimal("6.00")),'preferenceDirection':'max',
'thresholds' : {'pref': (Decimal('1.0'), Decimal('0.0')), 'ind': (Decimal('0.0'), Decimal('0.0')), 'veto': (Decima
('1a12', {'name': 'Downtime', 'comment': 'SLA_delivered_by_external_auditor_1', 'objective':'A','shortName': 'dwT'
```

```
'weight':Decimal("2.00"),'scale': (Decimal("0.00"),Decimal("6.00")),'preferenceDirection':'max',
'thresholds' : {'pref': (Decimal('1.0'), Decimal('0.0')), 'ind': (Decimal('0.0'), Decimal('0.0')), 'veto':
('1a13', {'name': 'Outage', 'comment': 'SLA delivered by external auditor 1',
'objective': 'A', 'shortName': 'ouT','weight':Decimal("2.00"),'scale': (Decimal("0.00"),Decimal("6.00")),'p
'thresholds' : {'pref': (Decimal('1.0'), Decimal('0.0')), 'ind': (Decimal('0.0'), Decimal('0.0')), 'veto':
('1a21', {'name': 'Load balacing', 'comment': 'SLA delivered by external auditor 1', 'objective': 'R','shor
'weight':Decimal("2.00"),'scale': (Decimal("0.00"),Decimal("6.00")),'preferenceDirection':'max',
'thresholds' : {'pref': (Decimal('1.0'), Decimal('0.0')), 'ind': (Decimal('0.0'), Decimal('0.0')), 'veto':
('1a22', {'name': 'MTBF', 'comment': 'SLA delivered by external auditor 1',
'objective': 'R','shortName': 'MTBF','weight':Decimal("2.00"),'scale': (Decimal("0.00"),Decimal("6.00")),'p
'thresholds' : {'pref': (Decimal('1.0'), Decimal('0.0')), 'ind': (Decimal('0.0'), Decimal('0.0')), 'veto':
('1a23', {'name': 'Recoverable', 'comment': 'SLA delivered by external auditor 1', 'objective': 'R','shortN
'thresholds' : {'pref': (Decimal('1.0'), Decimal('0.0')), 'ind': (Decimal('0.0'), Decimal('0.0')), 'veto':
('1a31', {'name': 'Latency', 'comment': 'SLA delivered by external auditor 1',
'objective': 'P','shortName': 'Lat','weight':Decimal("2.00"),'scale':(Decimal("0.00"),Decimal("6.00")),'pre
'thresholds' : {'pref': (Decimal('1.0'), Decimal('0.0')), 'ind': (Decimal('0.0'), Decimal('0.0')), 'veto':
('1a32', {'name': 'Response Time', 'comment': 'SLA delivered by external auditor 1', 'objective': 'P','shor
'thresholds' : {'pref': (Decimal('1.0'), Decimal('0.0')), 'ind': (Decimal('0.0'), Decimal('0.0')), 'veto':
('1a33', {'name': 'Throughput', 'comment': 'SLA delivered by external auditor 1', 'objective': 'P','shortNa
'thresholds' : {'pref': (Decimal('1.0'), Decimal('0.0')), 'ind': (Decimal('0.0'), Decimal('0.0')), 'veto':
('1a41', {'name': 'Storage Cost', 'comment': 'SLA delivered by external auditor 1', 'objective': 'C','short
('1a42', {'name': 'Snapshot Cost', 'comment': 'SLA delivered by external auditor 1', 'objective': 'C','shor
'thresholds' : {'pref': (Decimal('1.0'), Decimal('0.0')), 'ind': (Decimal('0.0'), Decimal('0.0')), 'veto':
('1a51', {'name': 'Authentication', 'comment': 'SLA delivered by external auditor 1', 'objective': 'S','sho
'thresholds' : {'pref': (Decimal('1.0'), Decimal('0.0')), 'ind': (Decimal('0.0'), Decimal('0.0')), 'veto':
('1a52', {'name': 'Encryption', 'comment': 'SLA delivered by external auditor 1', 'objective': 'S','shortNa
'thresholds' : {'pref': (Decimal('1.0'), Decimal('0.0')), 'ind': (Decimal('0.0'), Decimal('0.0')), 'veto':
('1a53', {'name': 'Auditability', 'comment': 'SLA delivered by external auditor 1', 'objective': 'S','short
evaluation = {
'1a11': {
'a02':Decimal("0"),
'a04':Decimal("4"),
'a10':Decimal("2"),
},
'1a12': {
'a02':Decimal("3"),
'a04':Decimal("3"),

'a10':Decimal("2"),
},
'1a13': {
'a02':Decimal("3"),
'a04':Decimal("3"),
'a10':Decimal("1"),
},
'1a21': {
'a02':Decimal("4"),
'a04':Decimal("4"),
'a10':Decimal("4"),
},
'1a22': {
'a02':Decimal("1"),
```

```
'a04':Decimal("3"),
'a10':Decimal("3"),
},
'1a23': {
'a02':Decimal("3"),
'a04':Decimal("3"),
'a10':Decimal("1"),
},
'1a31': {
'a02':Decimal("2"),
'a04':Decimal("4"),
'a10':Decimal("3"),
},
'1a32': {
'a02':Decimal("-999"),
'a04':Decimal("-999"),
'a10':Decimal("-999"),
},
'1a33': {
'a02':Decimal("1"),
'a04':Decimal("4"),
'a10':Decimal("2"),
},
'1a41': {
'a02':Decimal("3"),
'a04':Decimal("4"),
'a10':Decimal("3"),
},
'1a42': {
'a02':Decimal("-999"),
'a04':Decimal("-999"),
'a10':Decimal("4"),
},
'1a51': {
'a02':Decimal("4"),
'a04':Decimal("4"),
'a10':Decimal("4"),
},
'1a52': {
'a02':Decimal("4"),
'a04':Decimal("4"),
'a10':Decimal("4"),
},
'1a53': {
'a02':Decimal("4"),
'a04':Decimal("4"),
'a10':Decimal("4"),
},}
```

Acronyms

AHP analytic hierarchy process 53

ARIMA Autoregressive Integrated Moving Average vi

CC Cloud Computing 3

CU Cloud User/Customer 3

CSU Cloud Service User/Customer 7

CSB Cloud Service Broker 8

CSC Cloud Standards Coordination 49

CSP Cloud Service Provider 3

CPU Computer Processing Unit 53

DPIA Data Protection Impact Assessment ix

EEA European Economic Area 68

ETSI European Telecommunications Standard Institute 49

EU European Union 67

GDPR General Data Protection Directive 63

IDC International Data Corporation 23

IFL Intuinistic Fuzzy Logic viii

IFS Intuinistic Fuzzy Set 89

IPR Intellectual Property Rights vii

ISO International Organizations for Standardization 49

KPI Key Performance Indicators 188

MAUT Multi Attribute Utility Theory 39

MCDM Multicriteria Decision Making vi

NSGA Non-Dominated Sorting in Genetic Algorithms 189

OCCI Open Cloud Computing Interface 55

OGF Open Grid Forum 49

QoS Quality of Service 7

SLA Service Level Agreement 5

SME Small Medium Enterprises 161

TPA Third Party Auditor 49

XDR External Data Representation 80

XML Extensible Markup Language 80

VM Virtual Machine 49

Bibliography

[1] *The Early History of MCDM*, chapter 1, pages 1–16.

[2] [Online] aneka. http://www.manjrasoft.com/aneka-architecture.html.

[3] [Online] azurewatch. https://www.paraleap.com.

[4] [Online] cloud accountability project. http://www.a4cloud.eu.

[5] [Online] cloudharmony. https://cloudharmony.com.

[6] [Online] cloudstatus. http://www.vmware.com/products/vrealize-hyperic.html.

[7] [Online] cloudwatch. https://aws.amazon.com/cloudwatch/.

[8] [Online] logicmonitor. http://www.logicmonitor.com.

[9] [Online] monitis. http://www.monitis.com.

[10] [Online] nms. https://support.nimsoft.com.

[11] Qos-aware web services selection with intuitionistic fuzzy set under consumers vague perception. *Expert Systems with Applications*, 36(3, Part 1):4460 – 4466, 2009.

[12] Negotiating cloud contracts: Looking at clouds from both sides now. *STANFORD TECHNOLOGY LAW REVIEW*, 2012.

[13] SLAware kearney, k.t.: Slaware, 2012. https://dl.dropbox.com/u/ 50697125/SLAware.

[14] Giuseppe Aceto, Alessio Botta, Walter de Donato, and Antonio Pescap. Cloud monitoring: A survey. *Computer Networks*, 57(9):2093 – 2115, 2013.

[15] H. Akaike. A new look at the statistical model identification. *IEEE Transactions on Automatic Control*, 19(6):716–723, Dec 1974.

[16] A. Al Falasi and Mohamed Adel Serhani. A framework for sla-based cloud services verification and composition. In *Innovations in Information Technology (IIT), 2011 International Conference on*, pages 287–292, April 2011.

[17] Elvira Albert, Frank de Boer, Reiner Hähnle, Einar Broch Johnsen, and Cosimo Laneve. Engineering virtualized services. In *Proceedings of the Second Nordic Symposium on Cloud Computing 38; Internet Technologies*, NordiCloud '13, pages 59–63, New York, NY, USA, 2013. ACM.

[18] Rehab Alnemr, Erdal Cayirci, Lorenzo Dalla Corte, Alexandr Garaga, Ronald Leenes, Rodney Mhungu, Siani Pearson, Chris Reed, Anderson Santana de Oliveira, Dimitra Stefanatou, Katerina Tetrimida, and Asma Vranaki. *A Data Protection Impact Assessment Methodology for Cloud*, pages 60–92. Springer International Publishing, Cham, 2016.

[19] Alba Amato, Beniamino Di Martino, and Salvatore Venticinque. Multi-objective genetic algorithm for multi-cloud brokering. In Dieter an Mey, Michael Alexander, Paolo Bientinesi, Mario Cannataro, Carsten Clauss, Alexandru Costan, Gabor Kecskemeti, Christine Morin, Laura Ricci, Julio Sahuquillo, Martin Schulz, Vittorio Scarano, StephenL. Scott, and Josef Weidendorfer, editors, *Euro-Par 2013: Parallel Processing Workshops*, volume 8374 of *Lecture Notes in Computer Science*, pages 55–64. Springer Berlin Heidelberg, 2014.

[20] Alba Amato, Loredana Liccardo, Massimiliano Rak, and Salvatore Venticinque. Sla negotiation and brokering for sky computing. In *CLOSER'12*, pages 611–620, 2012.

[21] A. Amin, A. Colman, and L. Grunske. An approach to forecasting qos attributes of web services based on arima and garch models. In *Web Services (ICWS), 2012 IEEE 19th International Conference on*, pages 74–81, June 2012.

[22] G. F. Anastasi, E. Carlini, M. Coppola, and P. Dazzi. Qbrokage: A genetic approach for qos cloud brokering. In *2014 IEEE 7th International Conference on Cloud Computing*, pages 304–311, June 2014.

[23] K. Atanassov and G. Gargov. Interval valued intuitionistic fuzzy sets. *Fuzzy Sets Syst.*, 31(3):343–349, July 1989.

[24] Krassimir T. Atanassov. Intuitionistic fuzzy sets. *Fuzzy Sets Syst.*, 20(1):87–96, August 1986.

[25] Paolo Balboni. *ISSE 2010 Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe 2010 Conference*, chapter Data Protection and Data Security Issues Related to Cloud Computing in the EU, pages 163–172. Vieweg+Teubner, Wiesbaden, 2011.

[26] D. Bernstein, E. Ludvigson, K. Sankar, S. Diamond, and M. Morrow. Blueprint for the intercloud - protocols and formats for cloud computing interoperability. In *Internet and Web Applications and Services, 2009. ICIW '09. Fourth International Conference on*, pages 328–336, May 2009.

[27] Felix Bieker, Michael Friedewald, Marit Hansen, Hannah Obersteller, and Martin Rost. *A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation*, pages 21–37. Springer International Publishing, Cham, 2016.

[28] Raymond Bisdorff. On measuring and testing the ordinal correlation between bipolar outranking relations. In *From Multiple Criteria Decision Aid to Preference Learning*, pages 91–100, NOV 2012.

[29] Raymond Bisdorff. On polarizing outranking relations with large performance differences. *Journal of Multi-Criteria Decision Analysis*, 20(1-2):3–12, 2013.

[30] Raymond Bisdorff. The euro 2004 best poster award: Choosing the best poster in a scientific conference. In Raymond Bisdorff, Luis C. Dias, Patrick Meyer, Vincent Mousseau, and Marc Pirlot, editors, *Evaluation and Decision Models with Multiple Criteria*, International Handbooks on Information Systems, pages 117–165. Springer Berlin Heidelberg, 2015.

[31] Raymond Bisdorff. Hpc ranking big performance tableaux with multiple incommensurable criteria. In *From 30th Annual Conference of the Belgian Operational Research Society UCL CORE,LouvainlaNeuve, Belgium*, JAN 2016.

[32] A. Biswas, S. Majumdar, B. Nandy, and A. El-Haraki. An auto-scaling framework for controlling enterprise resources on clouds. In *Cluster, Cloud and Grid Computing (CCGrid), 2015 15th IEEE/ACM International Symposium on*, pages 971–980, May 2015.

[33] A. Biswas, S. Majumdar, B. Nandy, and A. El-Haraki. Predictive auto-scaling techniques for clouds subjected to requests with service level agreements. In *2015 IEEE World Congress on Services*, pages 311–318, June 2015.

[34] R. Biswas. Intuitionistic fuzzy relations. bulletin for studies and exchange of fuzziness and its applications. *BUSEFAL*, 70:2229, july 1997.

[35] Rajkumar Buyya, James Broberg, and Andrzej M. Goscinski. *Cloud Computing Principles and Paradigms.* Wiley Publishing, 2011.

[36] Rajkumar Buyya, Suraj Pandey, and Christian Vecchiola. *Market-Oriented Cloud Computing and The Cloudbus Toolkit.*

[37] Rajkumar Buyya, Rajiv Ranjan, and RodrigoN. Calheiros. Intercloud: Utility-oriented federation of cloud computing environments for scaling of application services. In Ching-Hsien Hsu, LaurenceT. Yang, JongHyuk Park, and Sang-Soo Yeo, editors, *Algorithms and Architectures for Parallel Processing*, volume 6081 of *Lecture Notes in Computer Science*, pages 13–31. Springer Berlin Heidelberg, 2010.

[38] Rajkumar Buyya, Chee Shin Yeo, Srikumar Venugopal, James Broberg, and Ivona Brandic. Cloud computing and emerging {IT} platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems*, 25(6):599 – 616, 2009.

[39] R. N. Calheiros, E. Masoumi, R. Ranjan, and R. Buyya. Workload prediction using arima model and its impact on cloud applications x2019; qos. *IEEE Transactions on Cloud Computing*, 3(4):449–458, Oct 2015.

[40] Gerardo Canfora, Massimiliano Di Penta, Raffaele Esposito, and Maria Luisa Villani. An approach for qos-aware service composition based on genetic algorithms. In *Proceedings of the 7th Annual Conference on Genetic and Evolutionary Computation*, GECCO '05, pages 1069–1075, New York, NY, USA, 2005. ACM.

[41] Emiliano Casalicchio and Monica Palmirani. A cloud service broker with legal-rule compliance checking and quality assurance capabilities. In *1st International Conference on Cloud Forward: From Distributed to Complete Computing, October 6-8, 2015, Pisa, Italy.*, pages 136–150, 2015.

[42] Bice Cavallo, Massimiliano Di Penta, and Gerardo Canfora. An empirical comparison of methods to support qos-aware service selection. In *Proceedings of the 2Nd International Workshop on Principles of Engineering Service-Oriented Systems*, PESOS '10, pages 64–70, New York, NY, USA, 2010. ACM.

[43] Hoi Chan and Trieu Chieu. Ranking and mapping of applications to cloud computing services by svd. In *Network Operations and Management Symposium Workshops (NOMS Wksps), 2010 IEEE/IFIP*, pages 362–369, April 2010.

[44] Xi Chen, Zibin Zheng, and Michael R. Lyu. *QoS-Aware Web Service Recommendation via Collaborative Filtering*, pages 563–588. Springer New York, New York, NY, 2014.

[45] P. Choudhury, M. Sharma, K. Vikas, T. Pranshu, and V. Satyanarayana. Service ranking systems for cloud vendors. pages 433–440, January 2012.

[46] European Commission. Cloud SLA Standardisation Guidelines, year = 1993, url = https://ec.europa.eu/digital-single-market/en/news/cloud-service-level-agreement-standardisation-guidelines, accessed = 2016-04-21.

[47] European Commission. Unfair contract terms, year = 1993, url = http://ec.europa.eu/consumers/consumer-rights/rights-contracts/unfair-contract/index-en.htm, accessed = 2016-04-21.

[48] [Online]practical guide to cloud service agreements version 2.0, 2015. CSCC, "http://www.cloud-council.org/".

[49] [Online] (csmic), smi framework, 2014. "http://betawww.cloudcommons.com/servicemeasure mentindex".

[50] ISO/IEC jtc 1/sc 38 distributed application platforms and services (daps). http://www.iso.org/iso/home/.

[51] Supriya Kumar De, Ranjit Biswas, and Akhil Ranjan Roy. An application of intuitionistic fuzzy sets in medical diagnosis. *Fuzzy Sets and Systems*, 117(2):209 – 213, 2001.

[52] Kalyanmoy Deb. Multi-objective genetic algorithms: Problem difficulties and construction of test problems. *Evolutionary Computation*, 7:205–230, 1999.

[53] V.C. Emeakaroha, I. Brandic, M. Maurer, and S. Dustdar. Low level metrics to high level slas - lom2his framework: Bridging the gap between monitored metrics and sla parameters in cloud environments. In *High Performance Computing and Simulation (HPCS), 2010 International Conference on*, pages 48–54, June 2010.

[54] ETSI cloud standards coordination. http://csc.etsi.org, year=.

[55] Jian Mao Robert Bohn John Messina Mark Badger Fang Liu, Jin Tong and Dawn Leaf. Nist cloud computing reference architecture. 2011.

[56] Ana Juan Ferrer, Francisco Hernndez, Johan Tordsson, Erik Elmroth, Ahmed Ali-Eldin, Csilla Zsigri, Ra?l Sirvent, Jordi Guitart, Rosa M. Badia, Karim Djemame, Wolfgang Ziegler, Theo Dimitrakos, Srijith K. Nair, George Kousiouris, Kleopatra Konstanteli, Theodora Varvarigou, Benoit Hudzia, Alexander Kipp, Stefan Wesner, Marcelo Corrales, Nikolaus Forg, Tabassum Sharif, and Craig Sheridan. Optimis: A holistic approach to cloud service provisioning. *Future Generation Computer Systems*, 28(1):66 – 77, 2012.

[57] J. Figueira and B. Roy. Electre methods. In J. Figueira, S. Greco, and M. Ehrgott, editors, *Multiple Criteria Decision Analysis: State of the Art Surveys*, pages 133–161. Springer, 2005.

[58] Ian Foster and Carl Kesselman, editors. *The Grid: Blueprint for a New Computing Infrastructure*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 1999.

[59] Yan Gao, Bin Zhang, Jun Na, Lei Yang, Yu Dai, and Qiang Gong. Optimal selection of web services with end-to-end constraints. In *Computer and Computational Sciences, 2006. IMSCCS '06. First International Multi-Symposiums on*, volume 2, pages 460–467, June 2006.

[60] S.K. Garg, S. Versteeg, and R. Buyya. Smicloud: A framework for comparing and ranking cloud services. In *Utility and Cloud Computing (UCC), 2011 Fourth IEEE International Conference on*, pages 210–218, Dec 2011.

[61] [Online]cloud services brokerage. gartner research, 2013. Gartner, "http://www.gartner.com/it-glossary/cloud-services-brokerage- csb".

[62] N. Ghosh and S.K. Ghosh. An approach to identify and monitor sla parameters for storage-as-a-service cloud delivery model. In *Globecom Workshops (GC Wkshps), 2012 IEEE*, pages 724–729, Dec 2012.

[63] Elena Giachino, Stijn Gouw, Cosimo Laneve, and Behrooz Nobakht. *Theory and Practice of Formal Methods: Essays Dedicated to Frank de Boer on the Occasion of His 60th Birthday*, chapter Statically and Dynamically Verifiable SLA Metrics, pages 211–225. Springer International Publishing, Cham, 2016.

[64] GICTF global inter-cloud technology forum. http://www.dmtf.org/sites/default/files/, year=2011.

[65] M. Godse, U. Bellur, and R. Sonar. Automating qos based service selection. In *Web Services (ICWS), 2010 IEEE International Conference on*, pages 534–541, July 2010.

[66] [Online] google app engine. https://cloud.google.com/appengine/docs,.

[67] Nikolay Grozev and Rajkumar Buyya. Inter-cloud architectures and application brokering: Taxonomy and survey. *Softw. Pract. Exper.*, 44(3):369–390, March 2014.

[68] John B. Guerard. *An Introduction to Time Series Modeling and Forecasting*, pages 47–72. Springer New York, New York, NY, 2013.

[69] M. Guzek, P. Bouvry, and E.-G. Talbi. A survey of evolutionary computation for resource management of processing in cloud computing [review article]. *IEEE Computational Intelligence Magazine*, 10(2):53–67, May 2015.

[70] Mateusz Guzek, Alicja Gniewek, Pascal Bouvry, Jedrzej Musial, and Jacek Blazewicz. Cloud brokering: Current practices and upcoming challenges. *Cloud Computing, IEEE*, 2(2):40–47, Mar 2015.

[71] Mateusz Guzek, Johnatan E. Pecero, Bernab Dorronsoro, and Pascal Bouvry. Multi-objective evolutionary algorithms for energy-aware scheduling on distributed computing systems. *Applied Soft Computing*, 24:432–446, 2014.

[72] Mateusz Guzek, Sébastien Varrette, Valentin Plugaru, Johnatan E. Pecero, and Pascal Bouvry. A holistic model of the performance and the energy efficiency of hypervisors in a hpc environment. *Concurrency and Computation: Practice and Experience*, 26(15):2569–90, 2014.

[73] Tom Gurout, Samir Medjiah, Georges Da Costa, and Thierry Monteil. Quality of service modeling for green scheduling in clouds. *Sustainable Computing: Informatics and Systems*, 4(4):225 – 240, 2014. Special Issue on Energy Aware Resource Management and Scheduling (EARMS).

[74] Qiang Huang, Lin Ye, Xinran Liu, and Xiaojiang Du. Auditing cpu performance in public cloud. In *Services (SERVICES), 2013 IEEE Ninth World Congress on*, pages 286–289, June 2013.

[75] CLIFFORD M. HURVICH and CHIH-LING TSAI. Bias of the corrected aic criterion for underfitted regression and time series models. *Biometrika*, 78(3):499–509, 1991.

[76] Rob Hyndman and Yeasmin Khandakar. Automatic time series forecasting: The forecast package for r. *Journal of Statistical Software*, 27(1):1–22, 2008.

[77] Rob J Hyndman and Anne B Koehler. Another look at measures of forecast accuracy. *International Journal of Forecasting*, pages 679–688, 2006.

[78] [Online] web services architecture overview. "http://www.ibm.com/developerworks/webservices/library ovr/",.

[79] [Online] cloudkick. https://www.rackspace.com/cloud/monitoring.

[80] [Online] idc forecasts worldwide cloud it infrastructure market, 2015. "http://www.idc.com/getdoc.jsp?containerId=prUS25946315/".

[81] ISO/IEC 20000-1:2011 information technology ? service management ? part 1: Service management system requirements, 2011. http://www.iso.org/iso/.

[82] Michael C. Jaeger and Gero Muehl. Qos-based selection of services: The implementation of a genetic algorithm. In *Communication in Distributed Systems (KiVS), 2007 ITG-GI Conference*, pages 1–12, Feb 2007.

[83] Foued Jrad, Jie Tao, and Achim Streit. Sla based service brokering in intercloud environments. In *Proceedings of the 2nd International Conference on Cloud Computing and Services Science*, pages 76–81, 2012.

[84] R. L. Keeney and H. Raiffa. Decisions with multiple objectives: Preferences and value tradeoffs. *Behavioural Science*, 39(2):169–170, 1993.

[85] Nancy J. King and V.T. Raja. Protecting the privacy and security of sensitive customer data in the cloud. *Computer Law and Security Review*, 28(3):308–319, 2012.

[86] George Kousiouris, George Vafiadis, and Marcelo Corrales. *A Cloud Provider Description Schema for Meeting Legal Requirements in Cloud Federation Scenarios*, pages 61–72. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.

[87] Ang Li, Xiaowei Yang, Srikanth Kandula, and Ming Zhang. Theory and applications of analytic network process. Pittsburgh, PA, 2005. RWS Publications.

[88] Ang Li, Xiaowei Yang, Srikanth Kandula, and Ming Zhang. Cloudcmp: Comparing public cloud providers. In *Proceedings of the 10th ACM SIGCOMM Conference on Internet Measurement*, IMC '10, pages 1–14, New York, NY, USA, 2010. ACM.

[89] Ang Li, Xiaowei Yang, Srikanth Kandula, and Ming Zhang. Cloudcmp: Comparing public cloud providers. In *Proceedings of the 10th ACM SIGCOMM Conference on Internet Measurement*, IMC '10, pages 1–14, 2010.

[90] M. Li, J. Huai, and H. Guo. An adaptive web services selection method based on the qos prediction mechanism. In *Web Intelligence and Intelligent Agent Technologies, 2009. WI-IAT '09. IEEE/WIC/ACM International Joint Conferences on*, volume 1, pages 395–402, Sept 2009.

[91] E.M. Maximilien and M.P. Singh. A framework and ontology for dynamic web services selection. *Internet Computing, IEEE*, 8(5):84–93, Sept 2004.

[92] [online] microsoft azure. https://azure.microsoft.com/en-us/?b=16.01,.

[93] L. D. Ngan and R. Kanagasabai. Owl-s based semantic cloud service broker. In *Web Services (ICWS), 2012 IEEE 19th International Conference on*, pages 560–567, June 2012.

[94] [Online] nimbus. http://www.nimbusproject.org, year=2015.

[95] Online]cloud computing reference architecture, 2011. NIST, "http://www.nist.gov/customcf/get pdf.cfm?pub id=909505".

[96] P. N. Nobile, R. R. F. Lopes, C. E. Moron, and L. C. Trevelin. Qos proxy architecture for real time rpc with traffic prediction. In *Distributed Simulation and Real-Time Applications, 2007. DS-RT 2007. 11th IEEE International Symposium*, pages 261–267, Oct 2007.

[97] Daniel Nurmi, Rich Wolski, Chris Grzegorczyk, Graziano Obertelli, Sunil Soman, Lamia Youseff, and Dmitrii Zagorodnov. The eucalyptus open-source cloud-computing system. In *Proceedings of the 2009 9th IEEE/ACM International Symposium on Cluster Computing and the Grid*, CCGRID '09, pages 124–131, Washington, DC, USA, 2009. IEEE Computer Society.

[98] [Online] occi working group. "http://occi-wg.org", year=2015.

[99] cloud computing contracts. http://ec.europa.eu/justice/contract/cloud-computing/index-en.htm, year=.

[100] cloud service level agreement standardisation guidelines. https://ec.europa.eu/digital-single-market/en/news/cloud-service-level-agreement-standardisation-guidelines, year=.

[101] quality of service modelling for green scheduling in cloud. http://homepages.laas.fr/tguerout/data/PUBLIS/REVUES/SUSCOM-EARMS-QoS-Modeling-for-Green-Scheduling-in-Clouds.pdf, year=.

[102] NIST cloud computing service metrics descriptions. http://www.nist.gov/itl/cloud/upload/RATAX-CloudServiceMetricsDescription-DRAFT-20141111.pdf, year=.

[103] NIST cloud computing technology roadmap. http://www.nist.gov/itl/ cloud/upload/, year=.

[104] Inc Gartner. Gartner Says Cloud Consumers Need Brokerages to Unlock the Potential of Cloud Services, 2009. http://www.gartner.com/ newsroom/id/1064712 (accessed: 2016-11-17).

[105] cloud computing service level agreements - exploitation of research results, 2016. http://ec.europa.eu/digital-agenda/en/news/cloud-computing- service-level-agreements-exploitation-research-results.

[106] Google docs, 2016. https://www.google.com/docs/about/.

[107] [Online] open nebula. http://opennebula.org,.

[108] [Online]openstack. https://www.openstack.org, year=2015.

[109] Jitendra Padhye, Victor Firoiu, Don Towsley, and Jim Kurose. Modeling tcp throughput: A simple model and its empirical validation. *SIGCOMM Comput. Commun. Rev.*, 28(4):303–314, October 1998.

[110] J. Panneerselvam, L. Liu, N. Antonopoulos, and Y. Bo. Workload analysis for the scope of user demand prediction model evaluations in cloud environments. In *Utility and Cloud Computing (UCC), 2014 IEEE/ACM 7th International Conference on*, pages 883–889, Dec 2014.

[111] D.F. Parkhill. *The Challenge of the Computer Utility.* Number p. 246 in The Challenge of the Computer Utility. Addison-Wesley Publishing Company, 1966.

[112] Dana Petcu. Consuming resources and services from multiple clouds. *Journal of Grid Computing*, 12(2):321–345, 2014.

[113] Dana Petcu, Beniamino Di Martino, Salvatore Venticinque, Massimiliano Rak, Tamás Máhr, Gorka Esnal Lopez, Fabrice Brito, Roberto Cossu, Miha Stopar, Svatopluk Šperka, and Vlado Stankovski. Experiences in building a mosaic of clouds. *Journal of Cloud Computing: Advances, Systems and Applications*, 2(1):1–22, 2013.

[114] Maria Grazia Porcedda. *European Data Protection: In Good Health?*, chapter Law Enforcement in the Clouds: Is the EU Data Protection Legal Framework up to the Task?, pages 203–232. Springer Netherlands, Dordrecht, 2012.

[115] Gridbus Project. Gridbus Service Broker, year = 2014, url = http://www.cloudbus.org/broker/, accessed = 2016-04-21.

[116] Lie Qu, Yan Wang, Mehmet A. Orgun, Ling Liu, and Athman Bouguettaya. Cloud service selection based on contextual subjective assessment and objective assessment. In *Proceedings of the 2014 International Conference on Autonomous Agents and Multi-agent Systems*, AAMAS '14, pages 1483–1484, Richland, SC, 2014. International Foundation for Autonomous Agents and Multiagent Systems.

[117] Chirs Reed.

[118] B. Rochwerger, A. Galis, E. Levy, J.A. Caceres, D. Breitgand, Y. Wolfsthal, I.M. Llorente, M. Wusthoff, R.S. Montero, and E. Elmroth. Reservoir: Management technologies and requirements for next generation service oriented infrastructures. In *Integrated Network Management, 2009. IM '09. IFIP/IEEE International Symposium on*, pages 307–310, June 2009.

[119] Wagle S S. *Cloud Computing Contracts Regulatory Issues and Cloud Providers' Offer: An Analysis*, pages 61–78. Springer International Publishing, Karlstad, 2016.

[120] T.L. Saaty. *The Analytic Hierarchy Process, Planning, Piority Setting, Resource Allocation*. McGraw-Hill, New york, 1980.

[121] A. Samba. Logical data models for cloud computing architectures. *IT Professional*, 14(1):19–26, Jan 2012.

[122] B. Schroeder and G.A. Gibson. A large-scale study of failures in high-performance computing systems. *Dependable and Secure Computing, IEEE Transactions on*, 7(4):337–350, Oct 2010.

[123] Gideon Schwarz. Estimating the dimension of a model. *Ann. Statist.*, 6(2):461–464, 03 1978.

[124] N. Srinivas and Kalyanmoy Deb. Muiltiobjective optimization using nondominated sorting in genetic algorithms. *Evol. Comput.*, 2(3):221–248, September 1994.

[125] Y. Syu, Y. Y. Fanjiang, J. Y. Kuo, and S. P. Ma. Applying genetic programming for time-aware dynamic qos prediction. In *2015 IEEE International Conference on Mobile Services*, pages 217–224, June 2015.

[126] Using cloud standards for interoperability of cloud frameworks, 2010. TechRep:2010, "http://www.nist.gov/customcf/get pdf.cfm?pub id=909505. 2010".

[127] Dirk Thatmann, Mathias Slawik, Sebastian Zickau, and Axel Küpper. *Towards a Federated Cloud Ecosystem: Enabling Managed Cloud Service Consumption*, pages 223–233. Springer Berlin Heidelberg, Berlin, Heidelberg, 2012.

[128] W. Theilmann, C. Kotsokalis, A. Edmonds, K. Kearney, and J. Lambea. A reference architecture for multi-level sla management. *Journal of Internet Engineering*, page 2010.

[129] [online]cloud computing reference architecture, 2015. TM Forum, "http://www.tmforum.org/".

[130] Adel Nadjaran Toosi, Rodrigo N. Calheiros, and Rajkumar Buyya. Interconnected cloud computing environments: Challenges, taxonomy, and survey. *ACM Comput. Surv.*, 47(1):7:1–7:47, May 2014.

[131] H. Wada, P. Champrasert, J. Suzuki, and K. Oba. Multiobjective optimization of sla-aware service composition. In *Services - Part I, 2008. IEEE Congress on*, pages 368–375, July 2008.

[132] S. S. Wagle. Cloud service optimization method for multi-cloud brokering. In *2015 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM)*, pages 132–139, Nov 2015.

[133] Shyam S. Wagle. Sla assured brokering (sab) and csp certification in cloud computing. In *Utility and Cloud Computing (UCC), 2014 IEEE/ACM 7th International Conference on*, pages 1016–1017, Dec 2014.

[134] Shyam S. Wagle, Mateusz Guzek, and Pascal Bouvry. Cloud service providers ranking based on service delivery and consumer experience. In *IEEE 4th International Conference on Cloud Networking (CloudNet)*, pages 202–205, Niagara Falls, Canada, October 2015.

[135] Shyam S. Wagle, Mateusz Guzek, and Pascal Bouvry. Service performance pattern analysis and prediction of commercially available cloud providers. In *IEEE 8th International Conference on Cloud Computing*, pages 111–119, Luxembourg City, Luxembourg, December 2016.

[136] Shyam S. Wagle, Mateusz Guzek, Pascal Bouvry, and Raymond Bisdorff. An evaluation model for selecting cloud services from commercially available cloud providers. In *IEEE 7th International Conference on Cloud Computing*, pages 107–114, Vancouver, Canada, November 2015.

[137] Shyam S. Wagle, Mateusz Guzek, Pascal Bouvry, and Raymond Bisdorff. Comparisons of heat map and ifl technique to evaluate the performance of commercially available cloud providers. In *IEEE 9th International Conference on Cloud Computing (Cloud 2016)*, pages 206–213, San Francisco, USA, 2016.

[138] S.S. Wagle. Sla assured brokering (sab) and csp certification in cloud computing. In *Utility and Cloud Computing (UCC), 2014 IEEE/ACM 7th International Conference on*, pages 1016–1017, Dec 2014.

[139] L. Wang, R. Ranjan, J. Chen, and B. Benatallah. *Cloud Computing: Methodology, Systems, and Applications*. CRC Press, 2011.

[140] Reinhard Wilhelm, Jakob Engblom, Andreas Ermedahl, Niklas Holsti, Stephan Thesing, David Whalley, Guillem Bernat, Christian Ferdinand, Reinhold Heckmann, Tulika Mitra, Frank Mueller, Isabelle Puaut, Peter Puschner, Jan Staschulat, and Per Stenström. The worst-case execution-time problem—overview of methods and survey of tools. *ACM Trans. Embed. Comput. Syst.*, 7(3):36:1–36:53, May 2008.

[141] Bo Yang, Feng Tan, and Yuan-Shun Dai. Performance evaluation ofcloud service considering fault recovery. *The Journal of Supercomputing*, 65(1):426–444, 2013.

[142] Lin Ye, Hongli Zhang, Jiantao Shi, and Xiaojiang Du. Verifying cloud service level agreement. In *Global Communications Conference (GLOBECOM), 2012 IEEE*, pages 777–782, Dec 2012.

[143] Milan Zeleny. Multiple criteria decision making (mcdm): From paradigm lost to paradigm regained? *Journal of Multi-Criteria Decision Analysis*, 18(1-2):77–89, 2011.

[144] Liangzhao Zeng, Christoph Lingenfelder, Hui Lei, and Henry Chang.

[145] Y. Zhang, Z. Zheng, and M. R. Lyu. Exploring latent features for memory-based qos prediction in cloud computing. In *Reliable Distributed Systems (SRDS), 2011 30th IEEE Symposium on*, pages 1–10, Oct 2011.

[146] Y. Zhang, Z. Zheng, and M. R. Lyu. Real-time performance prediction for cloud components. In *Object/Component/Service-Oriented Real-Time Distributed Computing Workshops (ISORCW), 2012 15th IEEE International Symposium on*, pages 106–111, April 2012.

[147] Z. Zheng, X. Wu, Y. Zhang, M. R. Lyu, and J. Wang. Qos ranking prediction for cloud services. *IEEE Transactions on Parallel and Distributed Systems*, 24(6):1213–1222, June 2013.

[148] Zibin Zheng, Yilei Zhang, and M.R. Lyu. Cloudrank: A qos-driven component ranking framework for cloud computing. In *Reliable Distributed Systems, 2010 29th IEEE Symposium on*, pages 184–193, Oct 2010.

[149] Suihui Zhu, Zhihui Du, Yinong Chen, Xudong Chai, and Bohu Li. Qos enhancement for pdes grid based on time series prediction. In *Proceedings of the Sixth International Conference on Grid and Cooperative Computing*, GCC '07, pages 423–429, Washington, DC, USA, 2007. IEEE Computer Society.

[150] [Online] zimory going beyond. http://www.zimory.com,.