

EVALUATING IDENTITY THEFT PROTECTIONS BY TRUST-BASED MODEL FOR CLOUD COMPUTING

A THESIS SUBMITTED TO AUCKLAND UNIVERSITY OF TECHNOLOGY
IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE
OF DOCTOR OF PHILOSOPHY

Supervisors

Dr Brian Cusack

Dr Alan T. Litchfield

July 2018

By

Eghbal Ghazi Zadeh

School of Engineering, Computer and Mathematical Sciences

Declaration

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which to a substantial extent has been submitted for the award of any other degree or diploma of a university or other institution of higher learning, except where explicitly defined in the acknowledgements.

A handwritten signature in black ink, appearing to read 'Eghbal Ghazi Zadeh', with a long horizontal stroke extending to the right.

Eghbal Ghazi Zadeh

Acknowledgements

This research has been completed at the Faculty of Design and Creative Technologies of the Auckland University of Technology. During the last three years, nothing makes me happier than the successful completion of this thesis as it was my main objective. Therefore, it is with the utmost joy and gratitude that I thank the following people. They dedicated their time, advice and endless support towards the completion of this thesis. To begin with, I must give thanks to my family for helping, inspiring, motivating, and supporting me during this strenuous yet extremely rewarding journey towards effectively completing this study. I am thankful for the numerous prayers, support and encouragement I have received throughout the years which have motivated me to finish this thesis despite the challenges that I have met along the way.

First and foremost, I am extremely thankful to my primary supervisor Dr. Brian Cusack for his constant and continuously advice and support throughout the research for last three years. He dedicated the same amount of time, effort, patience and hard work into this study as I have and that will never cease to amaze me. In addition, my second supervisor, Dr. Alan Litchfield, your support and review of the research outcomes with valuable feedback helped me immensely to improve the research deliverable. Thirdly, I would like to thank all my colleagues and friends who helped and motivated me during the research with countless hours and rewarding discussions.

My mother and mother in law, your prayers, support and words of encouragement have been truly appreciated. Last but not least, the assistance of AUT administrators, Scholarship office, IT services, Library, and in particular, AUT postgraduate office are also acknowledged with gratitude.

Abstract

The trust level in Cloud Computing (CC) is a topic that is currently attracting significant interest. Federated clouds with different attributes and secure elements present a complex decision-making context for the cloud services customers. Cloud identity federation can help maintain users' identity and their ability to use their identity in the distributed environment (Cloud). Therefore, due to the vast diversity of capability, capacity, and security in the available Cloud Identity Providers (CIdPs), from the Cloud identity Users' (CIdU) point of view, the lack of evidence is the main decision making problem. A decision to decide which providers a CIdU should use and what is the evidence basis for their decision and selection, is currently difficult and under addressed by CIdPs.

Currently, there is no comprehensive framework that can allow CIdUs to evaluate identity service offerings and rank them based on their ability to meet a trust framework (attributes, characteristics, features, and secure elements) requirements and this is a gap and an opportunity to research in this thesis. To address the gap, the objective is to establish a trust management framework that measures, aggregates and manages trust-related information from different sources which are available and relevant when assessing the trustworthiness of the CIdPs. Consequently, as a response to the gap, this study involves developing to a new cloud identity trust framework to answer the research questions and to make sure that the new artefact is evaluated and refined to a high standard. A mixed (Design Science (DS), Trust and Reputation System, Reputation System, and DeSPoT Trust System) trust and Design Science (TDS) research method is designed and employed to guide the study. The mixed method is used to mature the design artefact and to benefit the processes from problem identification, to evaluation and trust dissemination. The TDS method influences the design of the study and the evaluation methodology employed to evaluate the artefact which is done in the fifth phase of the DS research method.

The literature review showed there are many trust models and frameworks, but, they are either developed for a specific sub-field such as infrastructure, mobile, and network, or, a generic cloud trust framework model. This study is aimed to fill the gap identified in the literature where no comprehensive and useful trust

framework model is currently available to help CIdUs to make a knowledge-based decision that considers both service provider and customer perspectives. Therefore, the primary aim of the proposed trust framework is to consider the full cloud identity environment and to capture all potential trust attributes and elements as evidence, including functional and non-functional elements. In this regard, by utilising evaluation theory, Importance-Performance Analysis, Expert Interviews, and the Analytical Hierarchy Process, the modelling of trust a framework is done including, priorities, attributes, characteristics, the measurement processes, and an aggregate result for granular level trust metrics.

Therefore, the potential outcome of this research is to make an innovative structure based on the existing works and present it in a systematic way that helps the CIdUs to make the best decision for a CIdP or combinations of them for specific requirements. The impact of this research is to facilitate the knowledge base decision making for both identity providers and end users. Such a framework can bring a significant impact on the trust between a provider and the customers, and improve the decision-making process for users' identity management. Moreover, it helps CIdUs directly, without involving IT experts.

As a result, the application artefact has been designed, built, and implemented to test and evaluate the usability and feasibility of the proposed model. The application has passed the usability testing by the industry experts, but it still needs continuous improvement. Standardisation and technology updates are required before generalisation and release as a market version. The recommendations for further research from thesis are:

- Utilize the semantic web to determine the Service Level Agreement (SLA)
- Test the Trusted Platform Module hardware with trusted computing
- Further research to redesign the input sources of consumer opinion
- Utilize different threat models to test the artefact
- Improve the artefact to integrate with Cloud Access Security Brokers options
- Further research to improve the discovery database of cloud identity service providers
- Provide further aggregated information in the application dashboard
- Expand the scope to the Internet of Things (IoT) and Mobile Cloud Computing (MCC)

Publications

- Ghazizadeh, E & Cusack, B. (2018). Evaluation Theory for characteristics of Cloud Identity Trust Framework. *Cloud Computing*, Intech Open access, London, United Kingdom
- Ghazizadeh, E & Cusack, B. (2018). A Synthesis Technique for Cloud Life-Cycle Evaluation. *The Proceedings of the 2018 Cyber Forensics and Security International Conference*, Tonga
- Ghazizadeh, E & Cusack, B. (2018). Cloud Security Issues that Impact Privacy in Digital Identity Management. *The Proceedings of the 2018 Cyber Forensics and Security International Conference*, Tonga
- Ghazizadeh, E & Cusack, B. (2018). Satisfying Secure Load Balancing Expectations in the Cloud. *AMCIS 2018, the Proceedings of the 28th Americas Conference on Information Systems*, New Orleans, USA
- Ghazizadeh, E & Cusack, B. (2017). Trust Assessment for Cloud Identity Providers Using Analytical Hierarchy Process. *CSCI 2017, the Proceedings of the 2017 International Conference on Computational Science and Computational Intelligence*, Las Vegas, USA
- Ghazizadeh, E & Cusack, B. (2016). Formulating Methodology to Build a Trust Framework for Cloud Identity Management. *The Proceedings of the 22nd Americas Conference on Information Systems (AMCIS 2016)*, San Diego, USA
- Ghazizadeh, E & Cusack, B. (2016). Evaluating single sign-on security failure in cloud services. *Business Horizons*, 59(6), 605-614.
- Ghazizadeh, E & Cusack, B. (2016). Analyzing Trust Issues in Cloud Identity Environments. *ACIS 2016, the Proceedings of the 27th Australasian Conference on Information Systems*, Wollongong, Australia
- Ghazizadeh, E & Cusack, B. (2016). Evaluating Identity Theft Protections by Trust-Based Model for Cloud Computing. *The Proceedings of 11th Annual Postgraduate Research Symposium*, Auckland, New Zealand
- Ebrahimi, A., Ghazizadeh, E., & Alizadeh, M. (2015). Paint-doctored JPEG image forensics based on blocking artifacts. *IEMCON2015, the Proceedings of the 2015 IEEE International Conference and Workshop on Computing and Communication*, (pp. 1-5). Vancouver, British Columbia, Canada
- Ghazizadeh, E & Cusack, B. (2015). Evaluating single sign on security failure in cloud services. *The Proceedings of the 2015 SRI Security Congress*, Perth, Western Australia

- Ghazizadeh, E., Zamani, M., Ab Manan, J. L., & Alizadeh, M. (2014). Trusted computing strengthens cloud authentication. *The Scientific World Journal*, 2014. *Hindawi*.
- Ghazizadeh, E., Shams Dolatabadi, Z. S., Khaleghparast, R., Zamani, M., Manaf, A. A., & Abdullah, M. S. (2014). Secure OpenID authentication model by using Trusted Computing. *In Abstract and Applied Analysis (Vol. 2014)*. *Hindawi*.
- Alizadeh, M., Hassan, W. H., Zamani, M., Karamizadeh, S., & Ghazizadeh, E. (2013). Implementation and evaluation of lightweight encryption algorithms suitable for RFID. *Journal of Next Generation Information Technology*, 4(1), 65.
- Ghazizadeh, E., Zamani, M., & Pashang, A. (2012). A survey on security issues of federated identity in the cloud computing. *The Proceedings of the 4th IEEE International Conference on Cloud Computing Technology and Science Proceedings* (pp. 532-565), Taipei, Taiwan
- Ghazizadeh, E., Zamani, M., Khaleghparast, R., & Taherian, A. (2012). A trust based model for federated identity architecture to mitigate identity theft. *ICITST 2012, the Proceedings of the 2012 IEEE Internet Technology and Secured Transactions*, (pp. 376-381), London, UK

Contents

Declaration	ii
Acknowledgements	iii
Abstract	iv
Publications	vi
List of Tables.....	xii
List of Figures	xiv
List of Abbreviations.....	xvii

Chapter One Introduction

1.0	INTRODUCTION	1
1.1	MOTIVATION.....	3
1.2	THE APPROACH	5
1.3	THE FINDINGS	8
1.4	THESIS STRUCTURE	9

Chapter Two Literature Review

2.0	INTRODUCTION	11
2.1	THE LITERATURE SELECTION	12
2.1.1	Delphi Method Definition	14
2.1.2	Define Method Applications	14
2.2	CLOUD COMPUTING.....	15
2.2.1	Definition.....	15
2.2.2	Architectures	16
2.2.3	Evolving Challenges.....	19
2.3	IDENTITY.....	20
2.3.1	Definition.....	20
2.3.2	Management	21
2.3.3	Privacy.....	22
2.3.4	Theft and Attack.....	22
2.3.5	The New Security Perimeter	24
2.4	SYSTEM ARCHITECTURE	25

2.4.1	Definition.....	25
2.4.2	Cloud Federated Identity	26
2.4.3	Models and Standards	27
2.4.4	System Access	32
2.4.5	Limitations of IAM Protocols	36
2.5	TRUST COMPUTING.....	39
2.5.1	Cloud, Trust, Control and Visibility.....	40
2.5.2	Cloud and Assessment.....	42
2.6	LITERATURE SUMMARY	42
2.6.1	Privacy Conclusions	43
2.6.2	Security Conclusions.....	43
2.6.3	Trust Conclusions.....	44
2.7	CONCLUSION	45

Chapter Three Methodology

3.0	INTRODUCTION	47
3.1	PROBLEM STATEMENT.....	47
3.2	ESTABLISHING TRUST	51
3.3	THE RESEARCH QUESTION AND HYPOTHESES.....	54
3.4	TRUST SYSTEM METHODOLOGY	56
3.4.1	Methodology/Research Methods.....	60
3.4.2	Method Application in Brief	61
3.5	SYSTEMATIC LITERATURE.....	68
3.6	IMPLEMENTATION AND USABILITY CHECKING	69
3.7	EXPERT EVALUATION	71
3.8	DATA ANALYSIS	73
3.9	FEASIBILITY ASSESSMENT.....	74
3.10	COMMUNICATION	75
3.11	CONCLUSION	75

Chapter Four Evaluation Theory

4.0	INTRODUCTION	77
4.1	TRUST MANAGEMENT.....	78

4.2	EVALUATION SYSTEM ARCHITECTURE	80
4.3	THESIS TARGET	81
4.4	EVALUATION CRITERIA	82
4.4.1	Trust Framework	82
4.4.2	Trust Elements	84
4.5	EVALUATION YARDSTICK	89
4.6	DATA GATHERING	89
4.6.1	Data Gathering and Trust Framework	90
4.6.2	Data Gathering and Past Experience	93
4.7	SYNTHESIS TECHNIQUE	97
4.7.1	Framework Synthesis	97
4.7.2	Critical Interpretive Synthesis	109
4.7.3	Analysis	121
4.8	EVALUATION PROCESS	123
4.8.1	Preparation Process	123
4.8.2	Examination Process	123
4.8.3	Decision Making Process	124
4.8.4	Discussion and Analysis of The Result	131
4.9	CONCLUSION	135

Chapter Five Implementation and Usability Study

5.0	INTRODUCTION	137
5.1	APPLICATION ARCHITECTURE	138
5.2	APPLICATION WORKFLOW AND MODELLING TRUST	140
5.3	TCIDPF APPLICATION OVERVIEW	141
5.4	FORMULATION FOR TRUST EVALUATION	145
5.5	EXPERT USABILITY EVALUATION	158
5.5.1	Ethics and Privacy	161
5.5.2	Critical Reflection on Experts' Evaluation Results	162
5.6	CONCLUSION	173

Chapter Six Findings

6.0	INTRODUCTION	174
6.1	EVALUATION THE ARTEFACT	175
6.1.1	Developing the Trust Evaluation Hierarchy.....	178
6.2	CLOUD IDENTITY STANDARDS AND GUIDELINES.....	188
6.2.1	Standards' Comparisons.....	190
6.2.2	Discussion and Analysis of the Result	192
6.3	FEASIBILITY VALIDATION	198
6.3.1	Threat Modelling.....	200
6.3.2	Discussion and Analysis of the Result	203
6.4	CONCLUSION	209

Chapter Seven Discussion of Findings

7.0	INTRODUCTION	210
7.1	HYPOTHESES EVALUATION.....	211
7.2	RESEARCH QUESTION EVALUATION.....	214
7.3	IMPLICATION OF THE RESULTS	216
7.4	CONTRIBUTION	217
7.5	DISSEMINATION	222
7.6	CONCLUSION	225

Chapter Eight Conclusion

8.0	INTRODUCTION	227
8.1	RESEARCH SUMMARY.....	227
8.2	RESEARCH CHALLENGES	233
8.3	LIMITATIONS OF THIS STUDY	233
8.4	AREAS FOR FUTURE RESEARCH	235

References 237

Appendix A Ethical Approval	254
Appendix B Consensus Assessments	255
Appendix C Risk Assessment.....	260

List of Tables

TABLE 2.1: COMPARATIVE OF CURRENT IAM SOLUTIONS	37
TABLE 3.1: THE RESEARCH DATA PLAN	66
TABLE 3.2: INTERVIEW QUESTIONS FROM	72
TABLE 3.3: QUESTION OF ARTEFACT EVALUATION	73
TABLE 4.1: CLOUD IDENTITY BALANCING ISSUES	93
TABLE 4.2: CLOUD IDENTITY SSO ISSUES	94
TABLE 4.3: CLOUD IDENTITY LIFECYCLE ISSUES	94
TABLE 4.4: CLOUD IDENTITY PRIVACY ISSUES	94
TABLE 4.5: CLOUD IDENTITY RISK ISSUES.....	95
TABLE 4.6: CLOUD IDENTITY STANDARD ISSUES	96
TABLE 4.7: COMPARISON OF EXISTING CLOUD MONITORING APPROACHES.....	104
TABLE 4.8: COMPARISON OF EXISTING SLA CLOUD TRUST APPROACHES.....	111
TABLE 5.1: ENABLING TECHNOLOGY IN THE TCIdPF	142
TABLE 5.2: TRUST LEVEL ESTIMATION.....	149
TABLE 5.3: EFFECTIVE OF AVISPA TOOL.....	150
TABLE 5.4: TRUST LEVEL OF CURRENT IAM SOLUTIONS	151
TABLE 5.5: USER WEIGHT FOR THE SLA PARAMETERS	152
TABLE 5.6: EXTRACTED PARAMETERS FOR THE PROVIDERS	153
TABLE 5.7: COMPLIANCE WEIGHT	155
TABLE 5.8: INTERVIEW PARTICIPANTS.....	160
TABLE 5.9: ANALYSIS THE INTERVIEWEES QUESTION (GENERAL QUESTIONS)	163
TABLE 5.10: ANALYSIS OF THE INTERVIEWEE'S QUESTION	168
TABLE 6.1: SCALE OF RELATIVE IMPORTANCE (SAATY & KEARNS, 2014).....	177
TABLE 6.2: CONSISTENCY TEST FOR CIdP TRUST CHARACTERISTICS.....	181
TABLE 6.3: CONSISTENCY TEST FOR TRUST FRAMEWORK ATTRIBUTES	181
TABLE 6.4: ESA LOCAL AND GLOBAL WEIGHT	183
TABLE 6.5: ESC LOCAL AND GLOBAL WEIGHT	185
TABLE 6.6: IDENTITY STANDARDS OVERLAPS AND DIFFERENCES.....	192

TABLE 6.7: IDENTITY STANDARDS AND THEIR MOST FREQUENT WORDS	192
TABLE 6.8: ENISA AND ITS RELEVANT WITH ESC AND ESA	194
TABLE 6.9: CSA IAM AND ITS RELEVANT WITH ESC AND ESA.....	194
TABLE 6.10: NIST AND ITS RELEVANT WITH ESC AND ESA.....	195
TABLE 6.11: DFD AND THE STRID THREAT TYPES	200
TABLE 6.12: THREAT LIST, PROPERTIES.....	204
TABLE 7.1: HYPOTHESIS 1 EVALUATION	212
TABLE 7.2: HYPOTHESIS 2 EVALUATION	213
TABLE 7.3: HYPOTHESIS 3 EVALUATION	214

List of Figures

FIGURE 1.1: THESIS METHODOLOGY	7
FIGURE 2.1: CHAPTER TWO PATHWAY.....	11
FIGURE 2.2: DELPHI TECHNIQUE.....	13
FIGURE 2.3: DEPLOYMENT MODELS FOR CLOUD COMPUTING.	16
FIGURE 2.4: NAAS	18
FIGURE 2.5: CLOUD IN AN ENTERPRISE ECOSYSTEM.....	19
FIGURE 2.6: AVATIER IDENTITY MANAGEMENT SOFTWARE.	25
FIGURE 2.7: CLOUD FEDERATED IDENTITY	26
FIGURE 2.8: THE ARCHITECTURE OF THE LIBERTY ALLIANCE	28
FIGURE 2.9: SHIBBOLETH.....	28
FIGURE 2.10: WS-FEDERATION	29
FIGURE 2.11: ARCHITECTURE OF HUB AND SPOKE MODEL	29
FIGURE 2.12: FSSO PROCESS FLOW.....	30
FIGURE 2.13: AAO PROCESS FLOW.....	30
FIGURE 2.14: IPISE PROCESS FLOW	31
FIGURE 2.15: OPENID GENERAL WORKFLOW	32
FIGURE 2.16: OAUTH GENERAL WORKFLOW	33
FIGURE 2.17: WINDOWS CARDSPACE GENERAL WORKFLOW.....	33
FIGURE 2.18: U-PROVE GENERAL WORKFLOW	34
FIGURE 2.19: IDEMIX GENERAL WORKFLOW	34
FIGURE 2.20: HIGGINS GENERAL WORKFLOW	35
FIGURE 2.21: OPENID CONNECT GENERAL WORKFLOW	36
FIGURE 2.22: LEVELS OF REQUIREMENT FULFILLED.....	36
FIGURE 2.23: VISIBILITY OF THE SECURITY IN THE CLOUD.....	42
FIGURE 2.24: PRIVACY, SECURITY, AND TRUST ISSUES	45
FIGURE 3.1: WORKFLOW OF OPENID CONNECT AND TRUST ISSUES.	52
FIGURE 3.2: PROPOSED TRUST FRAMEWORK.	53
FIGURE 3.3. SUMMARY OF ADOPTED METHODOLOGIES.....	57
FIGURE 3.4. DSRM PROCESS MODEL.....	59
FIGURE 3.5: TRUST DESIGN SCIENCE RESEARCH METHODOLOGY (TDSRM)	61
FIGURE 3.6: CLOUD IDENTITY TRUST UNIFIED EVALUATION FRAMEWORK.....	63
FIGURE 3.7: EVALUATION METHOD TYPES (PEFFERS ET AL., 2012, P. 402).....	64
FIGURE 3.8: EVALUATION INPUTS AND APPROACHES	65

FIGURE 3.9: THE WORKFLOW OF THE TDSRM.	67
FIGURE 3.10: ARCHITECTURE OF THE CIDP'S TRUST FRAMEWORK	70
FIGURE 3.11: GUIDELINES REVIEW PROCESS.	74
FIGURE 4.1: CHAPTER FOUR PATHWAY	77
FIGURE 4.2: COMPONENTS OF AN EVALUATION AND THEIR INTERRELATIONS	80
FIGURE 4.3: CLOUD IDENTITY TRUST EVALUATION FRAMEWORK	81
FIGURE 4.4: TYPES OF TRUST FRAMEWORKS.	83
FIGURE 4.5: SERVICE TRUST EVALUATION SYSTEM ARCHITECTURE.	86
FIGURE 4.6: TRUST ELEMENTS	87
FIGURE 4.7: COMPUTATIONAL TRUST SOLUTION.....	90
FIGURE 4.8: TRUST MODEL.....	91
FIGURE 4.9: TRUST UNIFIED EVALUATION FRAMEWORK.....	92
FIGURE 4.10: AGGREGATION APPROACH FRAMEWORK.	102
FIGURE 4.11: CLOUD SERVICE MAPPER	102
FIGURE 4.12: CLOUDRANK'S SYSTEM ARCHITECTURE.	103
FIGURE 4.13: CURRENT TRENDS FOR TRUST ESTABLISHMENT	107
FIGURE 4.14: ESA FOR THIS THESIS.....	108
FIGURE 4.15: CLOUD COMPUTING FRAMEWORK SYNTHESIS.....	114
FIGURE 5.1: CHAPTER FIVE PATHWAY	137
FIGURE 5.2: ARCHITECTURE OF THE CIDP'S TRUST FRAMEWORK	139
FIGURE 5.3: CLOUD IDENTITY TRUST DECISION-MAKING WORKFLOW	141
FIGURE 5.4: TRUST CLOUD IDENTITY PROVIDER FRAMEWORK	143
FIGURE 5.5: CIDU DASHBOARD.....	144
FIGURE 5.6: CIDP DASHBOARD	144
FIGURE 5.7: INTERVIEWEE DASHBOARD	144
FIGURE 5.8: CONSENSUS ASSESSMENTS FORM (CIMI)	145
FIGURE 5.9: RISK ASSESSMENTS FORM	147
FIGURE 5.10: RISK LEVEL ESTIMATION.....	149
FIGURE 5.11: AVISPA'S ARCHITECTURE IN THE PROPOSED FRAMEWORK	149
FIGURE 5.12: IAM FORM	151
FIGURE 5.13: SLA EVALUATION PROCESS	152
FIGURE 5.14: USER INTERFACE FOR WEIGHTING THE SLA PARAMETERS	153
FIGURE 5.15: WEB INTERFACE FOR UPLOADING THE SLA	154
FIGURE 5.16: WEB INTERFACE FOR STANDARDS.....	155
FIGURE 5.17: WEB INTERFACE FOR USER FEEDBACK	156

FIGURE 5.18: WEB INTERFACE OF CIDP TRUST LEVEL	158
FIGURE 5.19: INTERVIEW PAGE AND ITS COMPONENTS	159
FIGURE 5.20: INTERVIEW QUESTIONS DASHBOARD FROM TRUST ELEMENTS	161
FIGURE 5.21: QUESTION DASHBOARD OF ARTEFACT EVALUATION	162
FIGURE 6.1: CHAPTER SIX PATHWAY	174
FIGURE 6.2: THE HIERARCHY OF TRUST FRAMEWORK ATTRIBUTES	178
FIGURE 6.3: THE HIERARCHY OF CIDP DECISION MAKING	179
FIGURE 6.4: THE ESA WEIGHTING INTERFACE	180
FIGURE 6.5: ESC AND AHP SCALE METHODS.....	188
FIGURE 6.6: ESA AND AHP SCALE METHODS	188
FIGURE 6.7: GUIDELINES REVIEW PROCESS	191
FIGURE 6.8: CSA IAM AND ITS MOST FREQUENT WORDS	191
FIGURE 6.9: NVIVO TEXT SEARCH CRITERIA (CSA AND STANDARD).....	196
FIGURE 6.10: NVIVO TEXT SEARCH CRITERIA (ENISA AND STANDARD).....	196
FIGURE 6.11: NVIVO TEXT SEARCH CRITERIA (NIST AND STANDARD).....	196
FIGURE 6.12: OUATH2.0 DATA FLOW DIAGRAM.....	199
FIGURE 6.13: OUATH2.0 THREAT MODELLING REPORT.....	201
FIGURE 6.14: THE CIDP TRUST FRAMEWORK CONCEPT	202
FIGURE 7.1: CHAPTER SEVEN PATHWAY	210
FIGURE 7.2: OVERALL WORKFLOW OF PROPOSED TRUST FRAMEWORK.....	222
FIGURE 8.1: THESIS METHODOLOGY	228

List of Abbreviations

CC	Cloud Computing
CSP	Cloud Service Provider
CSC	Cloud Service Customer
CIdP	Cloud Identity Provider
SaaS	Software as a Service
PaaS	Platform as a Service
IaaS	Infrastructure as a Service
TaaS	Trust as a Service
IDaaS	Identity as a Service
IdM	Identity Management
IAM	Identity and Access Management
FIM	Federated Identity Management
SSO	Single Sign On
SAML	Security Assertion Markup Language
JSON	JavaScript Object Notation
QoS	Quality of Service
QoP	Quality of Protection
DS	Design Science
IS	Information Systems
TDS	Trust Design Science
SLA	Service Level Agreement
AHP	Analytical Hierarchy Priorities
NIST	National Institute of Standards and Technology
NaaS	Network as a Service
VPN	Virtual Private Network
SecaaS	Security as a Service
GDPR	General Data Protection Regulatory
CASB	Cloud Access Security Brokers
IPA	Importance Performance Analysis
IT	Information Technology
IDS	Intrusions Detection System
VPN	Virtual Private Network

XaaS	Anything-as-a-Service
DaaS	Data-as-a-Service
SecaaS	Security-as-a-Service
CSA	Cloud Security Alliances
IPS	Intrusion Prevention System
DoS	Denial of Service
DDoS	Distributed Denial of Service
CFIAM	Cloud Federated Identity and Access Management
ID-SIS	Identity Services Interface Specifications
FSSO	Federated Single Sign-On and Attribute Sharing
AAO	Attribute Aggregation and Operations
IPiSE	Identity Privacy in Shared Environment
SPML	Services Provisioning Markup Languages
PSP	Provisioning Service Point
PST	Provisioning Service Target
RA	Requesting Authority
SCIM	Simple Cloud Identity Management
XACML	eXtensible Access Control Markup Languages
LDAP	Lightweight Directory Access Protocol
JSON	JavaScript Object Notation
XrML	eXtensible rights Markup Language
Idemix	Identity Mixer
CTA	Cloud Trust Authority
MIS	Management Information System
FCD	Formulation, Calculation, and Dissemination
MCDM	Multiple Criteria Decision Making
KPI	Key Performance Indicators
MAUT	Multiple Attribute Utility Theory
TDSRM	Trust Design Science Research Methodology
CITUEF	Cloud Identity Trust Unified Evaluation Framework
AWS	Amazon Web Services
CMS	Content Management System
STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of

	privilege
SMI	Service Measurement Index
CTP	Cloud Trust Protocol
MITM	Man-in-the-Middle
TEMRT	Trust Evaluation Model based on Response Time
PLT	Propositional Logic Terms
CAIQ	Consensus Assessment Initiative Questionnaire
AWSCC	Amazon Web Service Cloud Compliance
SRS	Service Ranking System
SVD	Singular Value Decomposition
MPA	Service Mapper Approach
YCSB	Yahoo! Cloud Serving Benchmark
RDF	Resource Description Framework
W3C	World Wide Web Consortium
CSMIC	Cloud Service Measurement Index Consortium
FIDO	Fast Identity Online
IETF	Internet Engineering Task Force
OASIS	Organization for the Advancement of Structured Information Standards
OIDC-RISC	OpenID Connect Reduced Instruction Set Computing
SACM	Security Automation and Continuous Monitoring
STIX	Structured Threat Information Expression
TAXII	Trusted Automated Exchange of Indicator Information
CyboX	Cyber Observable Expression
RISC	Risk and Incident Sharing and Coordination
OWASIS	Open Web Applications Security Project
ETSI	European Telecommunications Standards Institute
ISO	International Organization for Standardization
PHP	Hypertext Pre-processors
IIS	Internet Information Server
HTML	Hypertext Markup Language
HLPSL	High-Level Protocol Specification Language

CAI	Consensus Assessments Initiative
FIPS	Federal Information Processing Standard
ISMS	Information Security Management System
SDL	Security Development Lifecycle
IoT	Internet of Things

Chapter One

Introduction

1.0 INTRODUCTION

Cloud computing (CC) integrates various computing technologies to provide services to the end users. Goutas et al. (2015, p 90) defines CC as: “an on-demand network service that allows individual users or businesses to access configurable resources.” However, it can also be defined as a service delivery model with an On-demand feature which synchronously provides computer resources for the cloud users. There are three CC delivery models; Infrastructure as a Service (IaaS), Software as a service (SaaS), platform as a service (PaaS) (Stergiou et al., 2018). The (NIST, 2013a, p 2) CC definition is widely applied, and puts that CC has four distinct models of service provisioning which are essential characteristics, service models, common characteristics, and deployment models. Moreover, based on this definition, resource pooling, broad network access, measured service, on-demand self-service, rapid elasticity, and self-service there are five essential features of the CC.

Anything-as-a-Service (XaaS) is a new term which (Ali et al., 2015) discussed and defined in their research. They use this new term as a description of method for the nature of supporting and offering any service for the customers. The XaaS refers to granular requirements of the customers in any scope for any resources. However, Trust-as-a-Service (TaaS) and Identity-as-a-Service (IDaaS) are requirements and examples for the XaaS implementation. These two sub-services are central to this thesis as the management of authentication, authorisation, individual identities, privileges, role of Identity, and Access Management (IAM) are required to provide the trustable environment for customers (TaaS).

The process of creating, managing, providing services, infrastructure provision, and revoking identities, has been defined as Identity management (IdM). Cloud environments require IdM systems that have the capability of exchanging data and resources in a flexible way and collaborate dynamically with other cloud services. However, authentication, authorisation, and accountability are the three main components for any IAM system. Also, Federated Identity Management

(FIM) and Single Sign-On (SSO) are two main advantages of using an IAM and IdM. They have potential for offering greater security in identity management. Therefore, by having SSO and FIM, cloud users, from a single authentication in the home domain or any CIdP, are able to use other services in the same domain or circle of trust. Moreover, Single Sign-off, as a new term, provides the opportunity of closing all sessions of access, with a single logout process (Stergiou et al., 2018).

The FIM is using different tools such as but not limited to SAML (XML-based) (Security Assertion Markup Language) to exchange data between service providers and CIdPs. OpenID Connect protocol is a tool that is using JSON (JavaScript Object Notation) to exchange data between CIdPs and service providers. OpenID Connect as a cloud IAM allows dynamic cloud user registration when the users automatically register themselves at any Cloud Service Providers (CSP). Importantly, a dynamic federation means a provider will trust any users that request and provide it with their information. Besides, “Identity Trust” is the future aim and work of OpenID Connect federations that utilise the use of the federation concept in the cloud identity environment (Hedberg et al., 2018).

On the other hand, security and privacy concerns are paramount when storing and managing user identities for the CSP and required for the CIdUs. Therefore, these two concerns are also vital for the CIdUs to increase their confidence and trust towards a CIdPs and CSPs to mitigate the identity theft. The different challenges for implementing IAM are found when actions occur for authentication, integrated storage of identities, trust choices for providers, the user access to evidence, and the recycling of identities (Kostopoulos et al., 2017). While, every CSPs and CIdUs have a method of managing identities that may address some or all of these issues, but a CIdU requires to know the level of their trust to make a best and a knowledge based decision. Therefore, measurement of their methods and techniques by a trust measurement system can help a CIdUs to make a good (knowledge based) decision.

Trust management is a prominent area of security in the CC because insufficient trust management hinders cloud growth (Noor et al., 2016). Moreover, trust management is one of the key concerns in the adoption of CC. Trust management systems research can help develop innovative solutions to challenges by strengthening protection for identification, privacy, personalisation, integration, security, and scalability. Also, the end user of services can be better informed when

making the best decision regarding the security, privacy, and Quality of Service (QoS). The cloud services attribute encountered by the user abstract into preferences and behaviours that decide usage and a preferred CSP. Consequently, it is clear that CIdUs have the right of assessing the dependability of a CSP and CIdUs. Moreover, CSPs and CIdUs have to be able to factually, transparently, and objectively present the attributes and characteristics of their capabilities. Therefore, by achieving evidence for trust, CIdUs and Cloud Service Customers (CSC) have a basis to make good decisions about whether or not to depend on a particular CSP and CIdP out of many providers (Manuel, 2015).

Therefore, this study is going to focus on finding the trust elements for the CIdPs and consequently proposes a trust framework that has the capability to evaluate CIdPs trust level by gathering information from both providers and the end users. The overall objective is to provide a trust value that represents the overall security, privacy, and reputation strength of the cloud identity service based on the trust elements. Trust value can be assessed by evaluating a list of attributes and characterises for the relevant features of security, privacy, and reputation. The cloud identity service features and specifications are used to assess the trust value in addition to the end user's experience in order to have a valuable and reliable result.

1.1 MOTIVATION

Chew et al. (2008) explained the maturity of a cloud providers' information security program determines the variety of measures that can be gathered successfully. Moreover, the researcher after doing critical and systematic literature came to this point that "You can't control what you can't measure". However, if control plus visibility (Coveillo et al., 2011) is the formula for trust, how do we go about solving for it? Control and visibility are two initial parts of trust in the cloud. Therefore, establishing trust first requires control and second a level of visibility (level of trust) that can be expanded for CSPs. Trust is one of the means to improve federation (one of the main objectives in the cloud) and enable interoperability of current heterogeneous independent cloud identity platforms. Trust management plays a major role in guiding the users to access trustworthy services. Therefore, the establishment of trust between cloud identity consumers and identity service providers is an open and challenging issue.

According to (Manuel , 2015) a trust model acts as a security strength evaluator and ranking service for the cloud and cloud identity applications and services. Therefore, it can be used as a benchmark to set up the cloud identity service research scope and to find the inadequacies and enhancements in cloud infrastructure. Consequently, a tool that evaluates and assesses these security concerns with respect to cloud services before the selection of a service is necessary in a cloud environment. Hence, this lack of trust management (Gonzales et al., 2017) has motivated the researcher to focus on a framework for such an evaluation of service security in a cloud identity environment.

The researchers stated that one of the major obstacles to the adoption of cloud federation is the lack of trust between service providers (anything as a Service) (Gonzales et al., 2017; Noor et al., 2016; Werner et al., 2017). It is essential to assess and evaluate the trust between the providers and to ensure the security of sensitive and critical data of the CSCs, before redirecting the CSCs' requests from one CSP to other CSP. Thus, as trust is the crucial driving force for the federation, it has motivated the researcher to evaluate and assess the trustworthiness of service providers to mitigate identity theft (Ghazizadeh & Cusack, 2016a).

However, in order to resolve identity theft potential, the researcher found that numerous trust models have been established; but they only cover some aspects of trust establishment. None of these trust frameworks are widely accepted by both CSCs and CSPs because they do not support all the essential trust elements (Noor et al., 2016). In addition, several problems even exist in the current cloud trust establishments, particularly the lack of interoperability and standardisation are the primary concerns. Likewise, no comprehensive and common trust model can establish trust in all the layers of the CIdPs, namely infrastructure, software, and platform.

These limitations have motivated the researcher to review the current literature in the body of knowledge in relation to CC, cloud Identity management, security and privacy issues of the cloud. Consequently, by reviewing the current approaches, the researcher came to this point that there are trust issues between identity providers and gap(s) for this study (Gap of the research). However, the ultimate aim of this thesis is to respond to the gap and to address the opportunity by answering the question: "What can be done to mitigate the identity theft by using a trust-based framework?"

Based on the plan for this thesis, finding the trust elements to measure, and consequently controls for the cloud environment, the researcher specified two terms. First, the Essential System Attributes (ESA) are the attributes and features of any proposed cloud trust framework which in this thesis will be identified and categorised. Second, Essential System Characteristics (ESC) are the most relevant trust elements for the particular environment and scope for this thesis (cloud identity area). After evaluating the features of the cloud trust frameworks (ESA) as well as dedicated features of the CIdPs, these two terms are used in the thesis to identify findings for the most relevant framework in the trust computing environment.

The research questions are derived from the literature reviewed in chapter two. These research questions are derived from the literature and are labelled Q1, Q2, and Q3 as follows. Q1: With respect to the ESA and ESC, how are the trusted-based relationship between CIdP and CIdU framed? Q2: How is evaluation done of the trust establishment framework from question one? Q3: How might the framework from question one (by using the evaluation method of question two) affect the decision making of CIdUs and CIdPs? The scope and purpose of the questions is to identify the essential system characteristics and attributes, determine the measurement method that each model is applied to and their outcome which is beneficial to evidence collection. Following are the three hypotheses that are used to test the new cloud identity trust framework. These hypotheses are assertions derived from the literature and are labelled H1, H2, and H3 as follows. H1: A CIdUs' choice of CIdPs is going to be based largely on security, risk, and reputation. H2: The modelling of a trust established in cloud identity needs to incorporate the ESA and ESC in order to produce a measurable trust relationship. H3: The cloud identity trust framework facilitates trust making decisions by cloud consumers. Further description the three hypotheses are in chapter three with the research question. The research question is answered in chapter four, five, and six, and also the testing of the three hypotheses.

1.2 THE APPROACH

The research focus has a complex domain in the common area between CC, cloud identity, and trust computing. The researcher needs to analyse the related work in these areas to understand the current literature as well as current industry methods

that mitigate identity theft. However, these areas have many aspects and different levels which need a sophisticated research method to find the best solution.

Thus, in this research a mixed methodology based on the most common trust methodologies as well as Information System (IS) methodologies, has been utilised. As figure 1.1 shows the thesis methodology is one of the main contributions for this research. In chapter two after capturing the requirements and finding the evidence, the Delphi method is used to focus on the most important issues which enterprises are confronted in the CC, namely, cloud identity, and trust computing areas.

Next, in chapter three, a substantial literature was reviewed to select four different processes groups to create a methodological context in which cloud security artefacts could be formed. The first process group concerned trust and the capability to calculate a trust value for an entity. The second process group calculates a reputation measurement for an organisation. The third process group collects the evidence required by the second process group, and the fourth process group is capable of building and evaluating a security artefact. The fourth process group was guided by Design Science (DS) as an organising framework and philosophy for making and building artefacts. DS has been made relevant to IS research as a methodology, and in this research, the framework is applied to IS security (Fournaris & Keramidas, 2014). The benefit of the approach is that an artefact may be investigated in context and improved through continuous iterations and testing (Offermann et al., 2009). This unique methodology assists the thesis to be aligned with both IS and trust methods to evaluate the research finding (artefact) as well as to contribute the current trust framework by dissemination of the trust for the trust customers, scholarly and professional publication.

The purpose of the DS research methodology is not only to develop an artefact but also to answer research questions. Depending on the characteristics and the goals of the research, a researcher can shape the processes to deliver innovative or confirmatory outcomes (Johannesson & Perjons, 2014b). The research is based on four constructs that group process knowledge for trust value (Håvaldsrud et al., 2012), reputation system (Hoffman et al., 2009), evidence (Sun & Y. Liu, 2012), and Design science (Offermann et al., 2009).

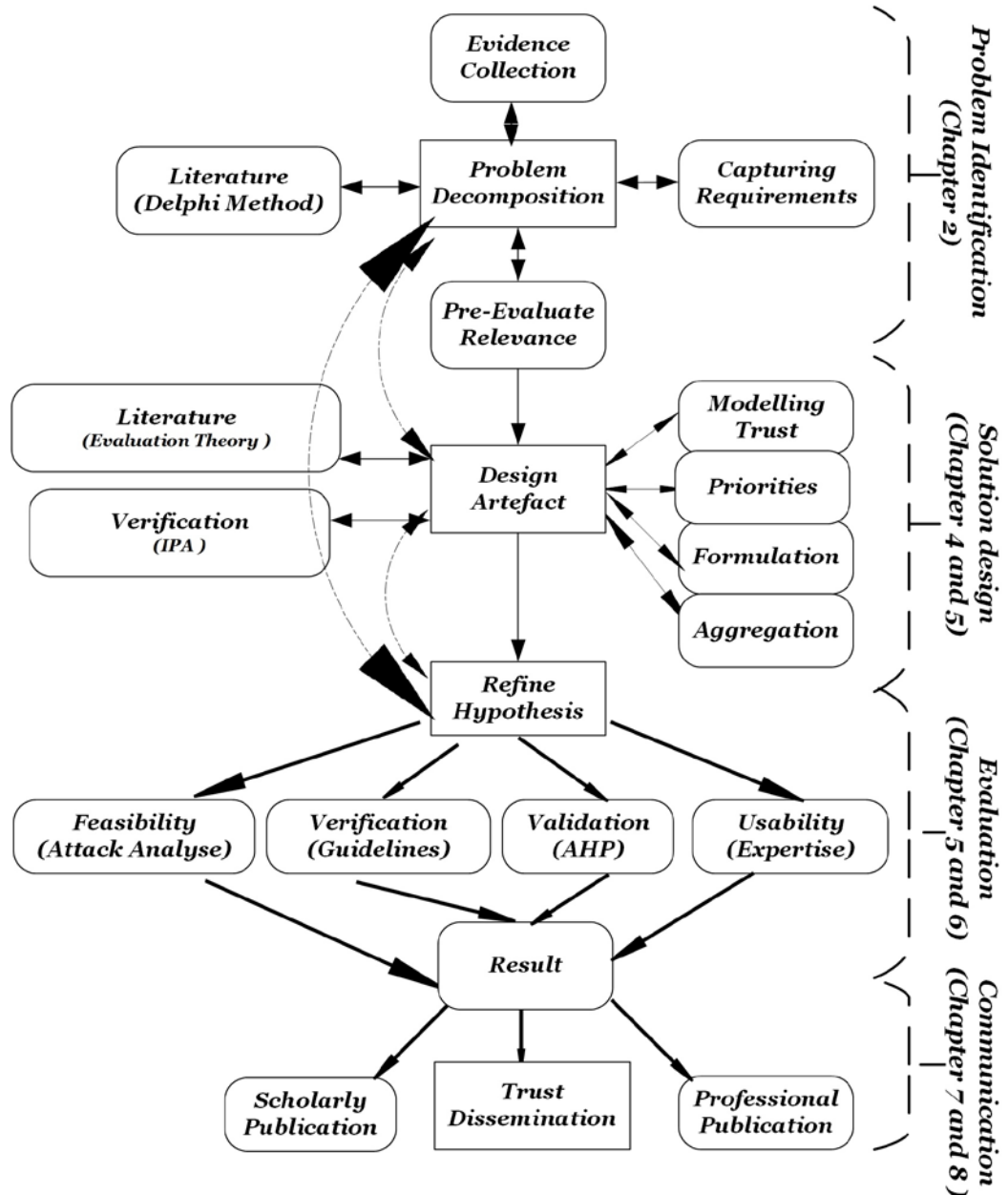


Figure 1.1: Thesis methodology

The researcher believes that the best approaches to achieve the research objective is utilising these four methodologies together which the researcher names, Trust Design Science (TDS). The overview of the TDS phases and steps is given in figure 1.1. Therefore, the methods for this thesis and roadmap is captured in this figure the researcher designed. In each chapter figure 1.1 is taken and by highlighting the particular sections addressed in the particular chapter (noted on vertical) in black background, the reader can follow accurately the execution of the methodology and each process taken to design, test, and evaluate the trust framework. Each phase is divided into steps, and the arrows indicate a transition from one step to another. Problem identification (chapter two), solution design (chapter three and four),

evaluation (chapter five and six), and communication (chapter seven and eight) are the four main steps to achieve the thesis objective.

In chapter four, evaluation theory with Importance Performance Analysis (IPA) have been utilised to revise the trust elements. Moreover, the data is collected from a variety of the resources such as literature, identity management guidelines, STRIDE Threat Modelling, Analytical Hierarchy Priorities (AHP), and industry interviews with expert people to find the answer to all the research questions as well as to test all hypotheses and also to refine the hypothesis. The main criteria for this thesis are an assumption from literature, usability assessment, verification from guidelines, verification from CIdPs and CIdUs, feasibility assessment, and element validation.

1.3 THE FINDINGS

A detailed discussion of the research findings is presented in chapters four, five, six, and seven as per the methodology. In the initial analysis trust computing is the effective method to mitigate the identity theft. In chapter two, after answering the method (Delphi) questions, the researcher summarised the privacy, security, and trust issues of CC in the figure 2.24. Chapter two identifies the limitations of the IAM protocols. The novel methodology is delivered in detail in chapter three. In chapter three, DS use with trust methodologies is elaborated for measuring the trust level of the cloud identities. The integration and application of the DS with trust methods is novel and contribution from this thesis.

In chapter four, the main finding is utilising evaluation theory to derive the trust element. Figure 4.1 shows the components of evaluation theory, and figure 4.2 illustrates the visualised adopted evaluation theory for the cloud identity trust evaluation framework. Therefore, using the evaluation theory and sub-components is another innovation in this thesis. Finding the most common trust frameworks with their essential system attributes and finding the most relevant trust characteristics are the main objectives for chapter four. The subsection 4.5.2 shows that load balancing, SSO, lifecycle, privacy, and risk are the main characteristics for the cloud identity environment.

Evaluation is the crucial step for any research project. However, most of the research papers lacked definitive evaluation methods. Thus, in this thesis, the proposed mixed methodology utilised industry interviews, professional guidelines, implementation, threat modelling, and Analytic Hierarchy Process (AHP) approaches to usability assessment, Verification of Guidelines, Verification from providers and

users, and Elements validation, as an evaluation framework. Thus, the strongest finding for this thesis is in the evaluation method which utilised different methods to evaluate the artefact, which is built and practically demonstrated as a feasible solution for the research problem.

To sum up, the thesis contributes in both theory and practice. The objective and artefact are novel as compared with the other publications and CC practices. The research outcome has also been communicated with an adequate audience (see list of publications) from both academic and industry in the same area and field. It has also been evaluated using the threat mitigation model. The practical finding for this thesis is to mitigate the end user's doubtful about security, privacy, and security practices that might be encountered in the cloud identity area. On the other hand, this framework is the opportunity for the industry (identity providers) to enhance their trust factors to relieve the end user of doubt, and benchmark themselves based on this framework. Last but not least, the proposed model has enhanced the business as well as end-user security, privacy, and trust requirements.

1.4 THESIS STRUCTURE

The thesis is presented in eight chapters. In chapter one an overview of the research is given that includes: the current situation for user decision-making, the researcher's motivations, the research approach, and objectives of the research. These provide an introduction and overview to the research. Chapter two is a theoretical review of the literature. This chapter concentrates on the finding trust, security, and privacy issues in the areas of CC, cloud identity, and trust computing with various types of cloud identity protocols and standards that cloud providers are using. For instance, the OpenID, SAML, OAuth are protocols in order for clients to access server resources on behalf of a resource owner.

The design of the study and research methodology are elaborated in chapter three. The chapter also discusses the problem area identified in the literature and the proposed the solution. The research question is derived from the literature, and a series of hypotheses are given for testing. Chapter four evaluates the existing trust frameworks to derive and prioritise the trust elements for the research. These trust frameworks have been selected and categorised based on their contributing features. For instance, user observation, self-assessment, and computational framework, are evaluated to derive their strengths and weaknesses.

Chapter five discusses the implementation and usability study of the artefact. It is devoted to the implementation design and the usability feedback on the trust management system in distributed and highly dynamic environments of cloud identity. Moreover, the objective of this chapter is to ensure applicability in practice as well as to improve the artefact's quality by including solutions to the problems encountered in the trust, security, and reputation aspects. The chapter reports the DS iteration factor and ends with expert usability evaluations.

Chapter six states the findings of the thesis based on the evaluation approaches for the proposed trust framework introduced chapter three. The evaluation of the artefact elements using AHP, cloud identity standards and guidelines, and feasibility validation (threat modelling and attack patterns) are reported. In chapter seven, the discussion of the findings reports the application of the criteria used in testing of the hypotheses. This is followed by the discussion of each of the hypotheses tested and the result of the tests. The research question is also answered. These results are then discussed, and the implications explored to identify the research contribution. Chapter eight concludes the thesis. The research is summarised, research challenges identified, and limitations of the study are explained. Areas for future study arising are also listed. A full list of references is provided, and the Appendices contain support documents, including the ethics approval to do the research.

Chapter Two

Literature Review

2.0 INTRODUCTION

A holistic view of the CC, identity management, trusted computing, and access control is presented in this chapter. A brief introduction to the evolution of the cloud and identity management is followed by security challenges and risk assessment approaches. Identity management systems are reviewed, and architectures reported.

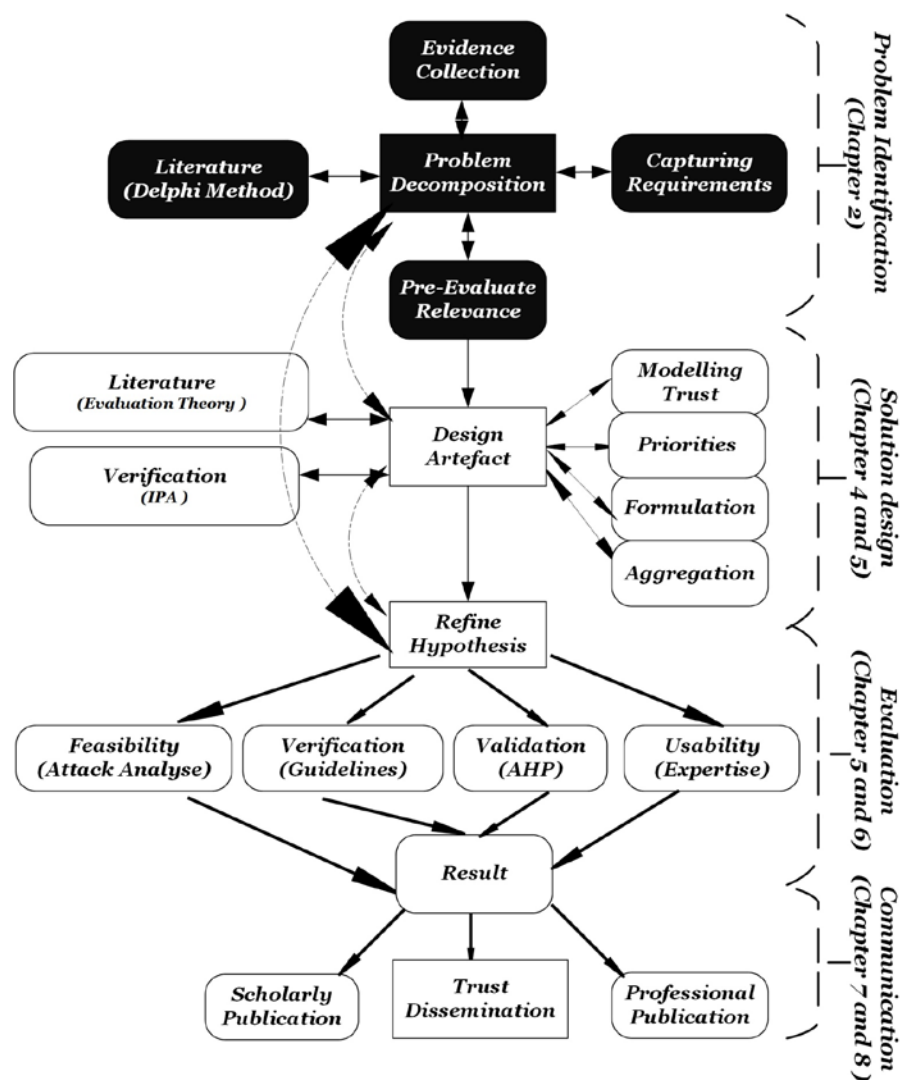


Figure 2.1: Chapter two pathway

Figure 2.1 shows the summary of the thesis plan based on the proposed methodology. It also shows the main focus for chapter two which is problem identification. As mentioned in the section 1.2 the approach is to clarify the pathway

and roadmap of the thesis by highlighting (black areas) the particular steps and sub steps to be achieved in each chapter. Therefore, in this chapter, based on the current literature selected by utilising the Delphi method, the researcher establishes requirements for the research. Next, based on the requirements and collected evidence, the Delphi method helps the researcher to identify and decompose the data to identify gaps and problems within the thesis scope. The most relevant articles are selected after pre-evaluating the selected research papers from the higher ranked Journals.

The chapter is further organised as follows. Section 2.1 identifies the literature method. Next, section 2.2 presents a definition, architecture, security issues, attacks, and cloud challenges. Section 2.3 provides a definition, architecture, model, and security features of cloud identity. The system architecture of cloud identity and federated identity management are discussed in section 2.4. The definition of trust computing, trust and control, cloud monitoring and cloud assessment are presented in section 2.5. The literature summary in the three areas (Privacy, Security, and Trust) is analysed and categorised in section 2.6. The chapter ends with the main conclusion and connection to chapter three in section 2.7.

2.1 THE LITERATURE SELECTION

Based on the Delphi method, this study focuses on the most important issues enterprises are confronting with CC, cloud identity, and trust computing adoption decisions. However, while there are studies that have focused on technological aspects regarding cloud, cloud identity, and trust, the decision regarding whether to adopt and migrate to cloud solutions is additionally complicated by some strategic issues (El-Gazzar et al., 2016). Several types of research have identified that there is a lack of empirical evidence and knowledge regarding which issues are most important for these areas (Schneider & Sunyaev, 2016). This chapter reviews the current literature, and consequently identifies the most important issues related to CC, cloud identity, and trust computing adoption decisions in enterprises. The relative significance of the identified issues is determined, and the importance of the identified issues is ranked.

In this regard, the researcher found that the Delphi method is one of the best ways to identify and prioritise issues for decision making and to sort large volumes

of references. The Delphi Method assists identifying the research questions and issues associated with the research topic. In this study the researcher first identified the below questions and consequently in the rest of the chapter used them to guide the collection of relevant literature.

“Q1: What issues confront entities when adopting cloud, CC, and trust computing?

Q2: What is the relative importance of these issues?

Q3: Why are these issues important?”

The literature contains a selection of academic literature related to CC, cloud identity, and trust computing. Therefore, identifying the most relevant challenges, approaches, issues, and techniques in the research scope is the objective. As a result, this section is designed to identify the method used to select the literature as shown in figure 2.2.

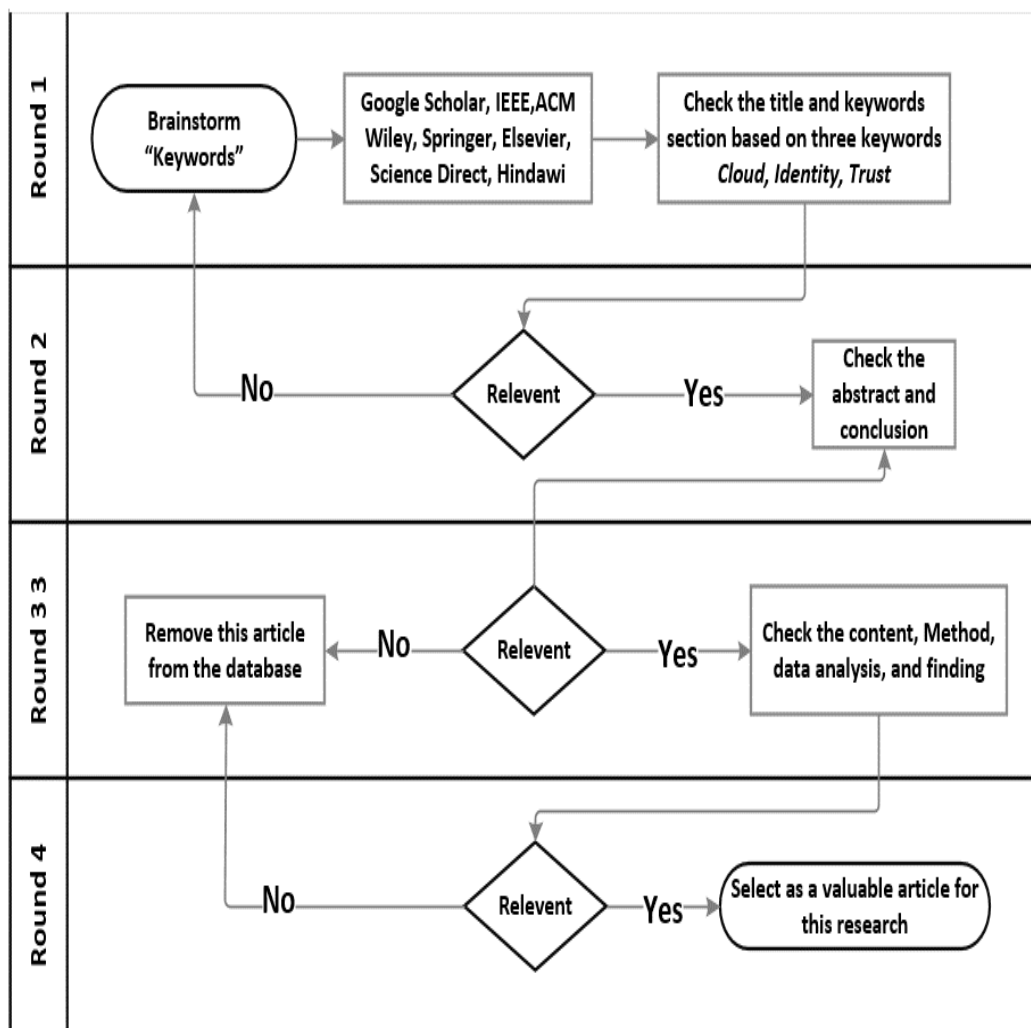


Figure 2.2: Delphi technique.

2.1.1 Delphi Method Definition

The main objective of the Delphi method is to systematically seek the most reliable opinion from a group of possibilities that are usually experts or selected groups within the scope of the research. The Delphi method has good reputation in Information Systems (IS) studies as a tool and a methodology to justify literature selection. It is known to be a qualitative research technique with quantitative elements (Okoli & Nguyen, 2015). The researcher found the method helpful to process the large amount of general literature available in the topic scope, and to select a relevant literature. The iterative rounds refined the target to a point the required themes were clear and the volumes manageable.

2.1.2 Define Method Applications

The aim of this section is to adopt the Delphi method to identify and to figure out the gaps in previous research. Therefore, in round 1, the question is: “What are the issues that enterprises are confronted with when adopting CC services, cloud identity, and trust computing?” A digital library search (IEEE, Google Scholar, Science Direct, Elsevier, Springer, ACM, Hindawi, and Springer) was undertaken to provide issues, as well as to define each issue, justify its importance and consequences, and if possible, add comments for elaboration. So, as per the variety of millions of academic papers, the research method assists finding the most relevant papers. Therefore, the following steps identify the processes involved and the paper selection criteria.

The CC, Cloud identity, Trust computing, Cloud issues, Federated identity issues, and trust issues are used as keywords to search in the title on the eight selected databases. The selected papers are limited between the year 2001 to the year 2017 (the most recent at the time of research).

The next step is to check the quality of the papers based on their abstract and conclusion, and relevancy to the search questions. Consequently, checking the content of the papers which passed the previous step is the final step for the process. This round is finalised with selecting papers. The main aim of using the Delphi method in this chapter is that it allows the researcher to focus on the research problem. Also to systematically gather the latest and up to date scholarly papers is another advantage of utilising this method (El-Gazzar et al., 2016).

2.2 CLOUD COMPUTING

Since the internet became a force in the field of communication, there has been an increasing demand for providing services such as storage, platform and software. CC is the result of the service demand in the last two decades by customers for every aspect of Information Technology (IT) for communication and processing. As a result, CC is easy for businesses to process real-time data by purchasing services that are hosted in the Cloud. The outsourcing mechanisms, on-demand scalability, resource sharing, economic savings, service flexibility and any-where any-time accessibility are some of the cloud advantages (Rittinghouse & Ransome, 2016). CC business use also reduces the total cost of IT and allows the purchase of services on a task by task basis.

CC does not have a commonly accepted definition yet. However, according to the last draft of CC Synopsis and Recommendations which is established by the National Institute of Standards and Technology's (NIST), CC is a computing model which permits all the networks, servers, applications and other elements related to data centers to be available to customers on demand through the Internet. They can purchase the type and quantity of computing services required and when they require it (Mell & Grance, 2011).

2.2.1 Definition

The substantial progress in the delivery of IT and service provisioning is a common explanation for CC. Moreover, descriptions of CC include, the cost, the speed, and efficiency, dynamic scaling, on-demand provision, and access to a shared pool of computing resources in a self-service fashion. On the other hand, diminished efficiency, inflexibility, infra-structure costs, staffing, and low utilisation are some of the disadvantages cited for traditional computing, that CC addresses. CC provides a customised infrastructure and dynamic deployment for users. It allows demand to grow and scale on-demand with an elastic commonality (Anbarasu, 2012). It is similar to other utility-based services such as water and electricity. It allows cloud users to outsource their service requirements and to retain a centralised pool of configurable computing resources. CC promotes advantages such as reducing the time and cost of production, providing better reliability and performance as well as more consistent computing services and efficient performance of the services (Khalil et al., 2014).

NIST also promotes the cloud and CC as energy efficient and in keeping with the migration towards sustainable energy sources. Green savings are one of the most important issues today in the world today with cost savings, power savings and sustainability. Usability related to green savings, and increased agility in software deployment are other characteristics of CC that consumers should consider when they choose cloud services (Badger et al., 2011). Figure 2.3 provides a summary of the NIST defined CC deployment model.

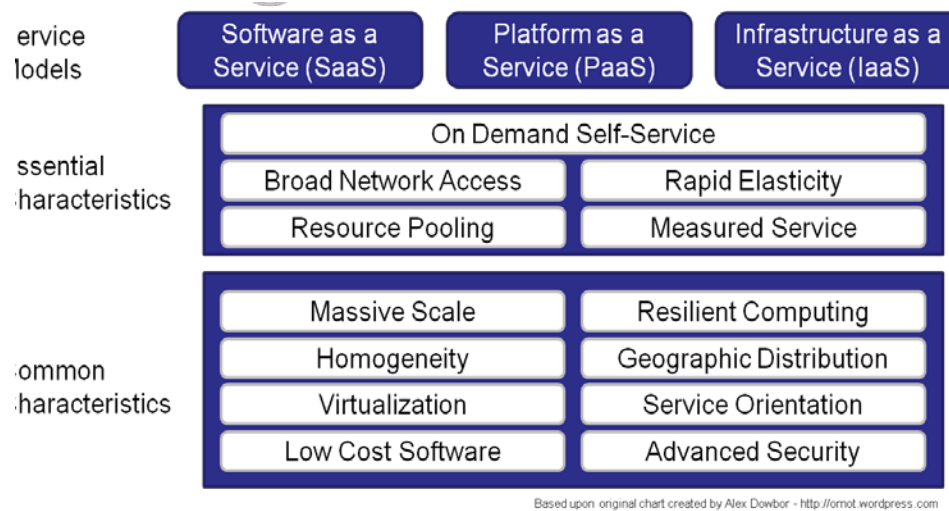


Figure 2.3: Deployment models for cloud computing (NIST, 2011, P. 6).

2.2.2 Architectures

CC integrates numerous computing architectures to provide the best services to the end users. However, there are many issues that are raised around the architecture and design features, security issues being one of them. The NIST definition of CC is widely accepted (NIST, 2013a) and the architecture adopted. Based on the NIST definition, common characteristics, essential characteristics, service models, and deployment models are four essential deployment models of the cloud architecture. However, also there are five essential features of CC are Broad network access, Resource pooling, on-demand, self-service, and Measured Service. In a cloud definition, using computing services deprives a user of any communication with each service provider and the architecture requires mediation agency for delivery. Moreover, broad network access means all services are available through the network although resources have been pooled to serve multiple consumers. This is how resource pooling is defined. Rapid elasticity is archived by capability scaling and elastic provisioning. Furthermore, metering capability or measured service in

the cloud systems automatically control and optimise resources by load balancing algorithms.

Figure 2.3 shows that besides these features, there are three characteristics, which involve the CC that have been named SaaS, PaaS, and IaaS. SaaS delivers to the consumer the ability to use the provider's applications running on a cloud infrastructure. Besides SaaS, as a capability provided to the customer, PaaS is deployed to the cloud infrastructure that is created by the consumer or acquired by tools and applications using programming languages supported by the Platform's provider. Furthermore, IaaS or cloud Infrastructure as a Service is an ability to provide to the consumer processing, storage, networks, and other fundamental computing resources in the network. It is deployed by the customer and run with arbitrary software, which can contain applications and operating systems. Although there are many features which are not part of the NIST definition. However, the NIST definition of CC is generally accepted as the benchmark for cloud architecture.

Barry (2014) argues that along with the NIST service models, Network as a Service (NaaS) is listed as a separate service model. He stated as shown in figure 2.4, NaaS can include the most common features of network such as but not limited to: flexible and extended custom routing, Intrusions Detection System (IDS), Intrusion Prevention System (IPS), Virtual Private Network (VPN), bandwidth on demand, security firewall, multicast protocols, and network content monitoring and filtering.

In addition to the four service delivery models, Ali et al. (2015) say the cloud can support and offer anything in the form of services (Anything-as-a-Service (XaaS)). They argued that this anything could be like Routing-as-a-Service (RaaS), Security-as-a-Service (SecaaS), and Data-as-a-Service (DaaS) which are common in communication areas.

In addition to the elaborated features and services, five models of the CC are called private, community, hybrid, public and Virtual private clouds. Private cloud is the type of the cloud that is run and managed exclusively for a single organisation. Hence, the organisation may not own the physical infrastructure and can be managed by the organisation itself or by a third party. Likewise, a private cloud may or may not be located at organisation's geographical site. The Public cloud is the cloud's physical infrastructure, which is owned by the Cloud Service

Provider (CSP) and is open to a general public and to host private clouds. The resources are shared among all the customers. The customers pay the cloud owner or broker according to the services and resources they use. But a community cloud is shared by some organisations and customers forming a community. The community cloud may be managed by any of the organisations in the community or a third party. Similarly, it may be located on-premise or off-premise.

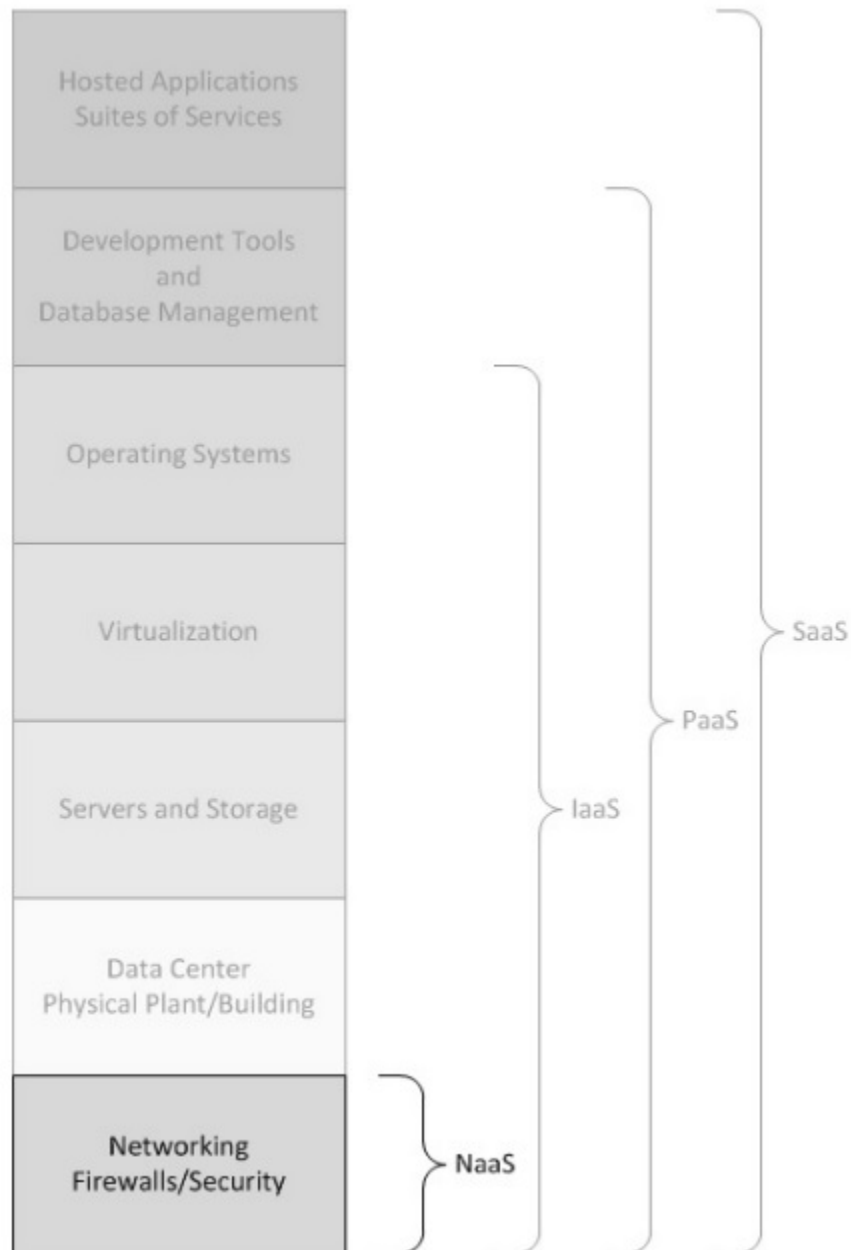


Figure 2.4: NAAS (Barry, 2014, P. 1).

Anbarasu (2012) described the essential parts of the cloud architecture which benefits the cloud customer. He believes that the high-level architecture provides a standard for cloud interfaces. Also, this architecture as shown in figure 2.5

illustrates the cloud functionality and monitoring of all aspects of resources, business insights, business applications and application components of cloud architecture.

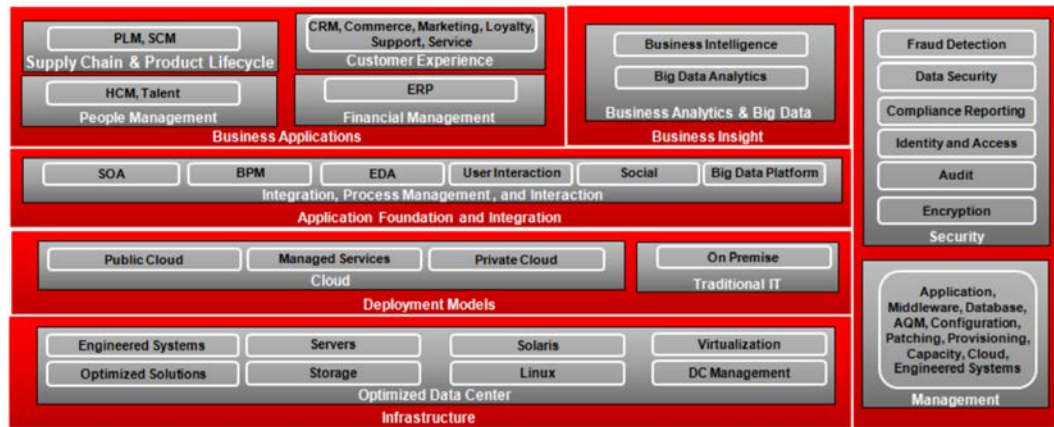


Figure 2.5: Cloud in an enterprise ecosystem (Anbarasu, 2012, p. 5).

2.2.3 Evolving Challenges

In order to gain a reasonable trust level in the cloud, a CSP has to understand and achieve the privacy and security requirements of their customers. Therefore, finding and identifying a common understanding and conceptual foundation of the CSC is crucial for CSP satisfaction. It requires integration of technical known and unknown requirements, technologies and implementation capability. Riquet et al. (2012) claim that “there is no strong solution available to prevent the DDoS attacks.” To validate their claim, the authors experiment to evaluate the effectiveness of their proposed model against common attacks. As a result of their research, no one has claimed to solve or prevent common attacks. However, Cloud Security Alliances (CSA) stated that CSPs do not maintain sufficient control over their system in order to avoid being spammed or hacked. As a summary for this subsection, there are common challenges for the CC which should be considered, such as but not limited:

- Contrast between public and private clouds: It means that several security issues provide good arguments to stay in private clouds.
- Outsourcing storage and computing: It means neither of the CSPs offer a complete set of characteristics that embrace all cloud requirements, such as public verifiability.
- Virtualised: It means that virtualisation still is a complex area of cloud with virtual resources, isolate running components.

- **Malware:** Cloud Malware concerns the CC to be commonly used by the CSCs.
- **Web-based technologies:** There is a wide attack vector associated to deliver applications over the Internet
- **Networking perimeter:** It means the security overlay for network design assumes a secure cloud environment.
- **Trust:** is a barrier that transversely extends throughout the whole of cloud components and stakeholders.
- **Privacy:** On the point of the privacy, there is an increasing government desire to mass supervise data from CSCs in the scope of general data protection policies.
- **Standardise:** It aims to speed up the migration of current cloud environments to interoperable and standardised cloud systems,

2.3 IDENTITY

Nowadays, one of most effective methods to overcome security, privacy, and trust issues of providing public and private cloud between CSCs and CSPs is advanced identity and access management. This system will provide benefits for all those in roles responsible with the providing secure access to cloud resources and to those who want to outsource or create online services. On the other hand, secure identity management is one of the best methods to overcome the security concerns of the CC security issues (Cusack & Zadeh, 2015). However, IAM provides authentication and authorisation based on CSC' identities in order to preserve security and privacy, while at the same time enhancing interoperability across numerous identities. The main objective for IAM in the cloud is to bring a different perspective related to the CSC' interests (Lonea et al., 2013).

2.3.1 Definition

Nowadays considering the increasing number of web users, there are enormous volumes of transaction of data transfer between CSCs and CSPs. As a response to the security concern is a secure identity. Identity means identifying CSC in a system and controlling their access to the cloud resources within that identity management system that associates user rights and restrictions with the established identity system (Ghazizadeh, Shams Dolatabadi, et al., 2014).

M. A. P. Leandro et al. (2012) believed that digital identity is the representation of an entity in the form of one or more elements of information or attributes that enable the entity to be recognised. They believed that there are two main user authentication methods which have been named; Card Based and Address Based. Card Based identity has used a digital token or unique attribute and claim, but the digital address has been utilised by Address Based. Moreover, they have stated that there are five common authentication methods, namely, SMS based authentication, Password and PIN-based authentication, Biometric authentication, Public-key authentication, and Symmetric-key authentication.

2.3.2 Management

IAM is mainly responsible for the storage, maintenance and retrieval of CSC's credentials for either authentication, authorisation or some other function of the cloud. Therefore, CSPs should have an IAM to handle the identity lifecycle from creation to death. The lifecycle includes creating an account, use, and elimination by consideration of identity and attributes that belong to internet users. The identity lifecycle includes the whole process of creation, management of account changes, password management and deletion or de-activation of CSC' identity (Gopalakrishnan, 2009).

M. A. P. Leandro et al. (2012) explained that Identity Management (IDM) is a set of capabilities and functions, such as administration, maintenance, management, and policy enforcement and authentication, utilised to ensure the exchange of identity in a secure method. Also, they clarified that identity lifecycle management is user provisioning, account management, user de-provisioning. Madsen et al. (2005) illustrated that today Federated Identity Management (FIM) refers to a model of distributed identity management in which one provider, in order to provide usability and efficiency for CSCs, agrees to accept authentication operations and identity information from other providers. Therefore, it is essential the management of identities in the cloud, and outside the provider's trust boundary, use a Cloud Identity Management System (IDaaS). However, the term IDaaS is broad, and involves all SaaS, IaaS, and PaaS for both private and public clouds (Subashini & Kavitha, 2011).

2.3.3 Privacy

It is vital to update and synchronised identity information to avoid any conflicts caused by the usage of on-premise user data. Therefore, in term of privacy, it is very important to choose a trustable IAM that best supports the CSC's privacy requirements because IAM is exposed to threats that can compromise CSP's behaviour when malicious users or entities try to subvert the system (Vapen et al., 2015). Furthermore, privacy is a desired feature both CSCs and CSPs, therefore, CSCs seek to keep secret the information of their digital identities as well as CSPs have to deploy mechanisms to preserve CSC' privacy. In this regard, CSPs seek to align with anonymity which means they cannot know the real identity of an CSCs, unlink ability, which means a CSPs cannot link different CSC's accesses. Besides anonymity as privacy characteristic, un-traceability is also another privacy issue which means an CIdPs cannot know the services that one of its end users has accessed (Mármol et al., 2010).

2.3.4 Theft and Attack

According to (Ahmad et al., 2010), the definition of identity theft is the exploitation of other user's individual information to perform fraud. Account fraud is one of the subcategories of identity theft. In the account fraud, an attacker takes advantage of existing accounts, and they make a new action based on the victim account. There are two ways for common identity theft: Diving rooting through garbage for personal information is the first (low-tech method). Hacking into collective computer systems is the second and high-tech method. The attackers steal a laptop including identity information, or they do Phishing attacks and exploit malicious computer code to get the user or system information. Weak cryptography between identity provider, users, and service providers is one of the reasons for identity theft. Therefore, in this environment personal identity information is the most important target.

Currently, much research (Vujin et al., 2014) is focused on Cloud IAM, while, security of IAM in the cloud is an aspect that is still in its initial stages and requires further exploration. Current IAMs are susceptible to various security and performance bottlenecks, which limits their federation adoption as a potential solution for the federation cloud. Therefore, the Cloud-based IAM and security

issues are relevant. The list of attacks that either use identity as a principal tool for the attack or launched against IAMs is as follows:

- Brute-force attack: It means that unauthorised access by an attacker to sensitive identity credentials of CSCs stored in an CIdPs' server using diverse methods to get the ID and password like dictionary attack (Lee et al., 2015).
- Cookie-replay attack: It refers that the attacker steals a cookie containing valid session information along with the identity credential of the CSC (Prasad, 2016).
- Data Tampering Attack: It means that the manipulation of the identification of CSC in an identity data-store at CIdPs (Aldaya et al., 2016).
- Denial of Service (DOS) Attack: It refers to non-availability of the CIdPs due to false authentication or authorisation which has been requested by attackers (Macedo et al., 2015).
- Eavesdropping: It refers to getting access to the identity credentials by attackers while both CIdP and CIdUs are exchanging the credential (Lonea et al., 2013).
- Elevation of Privilege: It refers to the escalation of the privilege by attackers in order to achieve their illegal objectives and may cause severe damage to the CSC' information (Habiba et al., 2014).
- Identity Forgery/Cloning/Spoofing Attack: It refers to the ability of manipulation or copying identity tokens by the attackers (Habiba et al., 2014).
- Identity Theft: Identity theft means that attackers can steal the CSC's identity, with the intent to acquire CSP' resources (Ghazizadeh, Shams Dolatabadi, et al., 2014).
- Phishing Attack: In this attack, the attackers seek to acquire CSC's information such as social security number, name, passwords, and credit card details by redirecting the CSC to enter a fake environment (Ghazizadeh, Shams Dolatabadi, et al., 2014).
- Repudiation: It is referred to lack of maintaining CSC's activity log so no proof exists to prove accountability for actions (Song et al., 2015).

- Side-Channel Attack: It refers the stealing the identity information from the physical implementation by the attackers (N. Zhang et al., 2014).
- Skimming Attack: In this method, the attackers steal the sensitive information from authentication tokens such as smart cards (Habiba et al., 2014).
- Snooping attack: It refers to the techniques to gather victim information through the surveillance methods such as key-loggers monitoring through remote activity (Habiba et al., 2014).
- Sybil attack: It means that the attackers are subverting the reputation of the either CSPs or CIdPs (da Costa Cordeiro et al., 2012).
- Whitewashing attack: It means that the attackers resetting weak reputation levels of the either CSPs or CIdPs (Vu et al., 2014).
- False praise attack: It means that the attackers give more weight to the past reputation levels of the either CSPs or CIdPs (Alzaid et al., 2013).

2.3.5 The New Security Perimeter

The researchers reviewed found that IAM would be efficient and secure by integrating various scenarios and techniques. Therefore, integrating and establishing a trust relationship along with security and privacy techniques brings the efficiency to the cloud environment as well as offering a huge range of features (Tormo et al., 2014). The IAM is the key element in the CC because it is providing centre place of identity management for both CSCs and CSPs. Therefore, IAM seeks to integrate various systems such as distributed systems multi-party computation, and federation to achieve this objective. Therefore, while IAM has been widely accepted, nevertheless, CSCs are more concerned about how their identity is managed (Habiba et al., 2014).

2.4 SYSTEM ARCHITECTURE

Architecture and deployment models for identity, as well as access management for cloud services, is a complex subject. It has to cover three different cloud service models (SaaS, PaaS, and IaaS) in three different deployment scenarios (public, private, and hybrid) and with a variety of communication protocols to address authentication, authorisation, and provisioning. The Cloud Security Alliance has catalogued many different identity ‘standards’, but standards should not drive architecture. System architecture goal is to define an overall architecture, which fits an organisation, and then fill in the appropriate communication standards. It should be a universal model that both abstracts and simplifies the structure from underlying environmental complexities. Single Sign-On (SSO), Provisioning, and Attribute Exchange are three core cloud IAM use cases. Delivering on these use cases requires architectural decisions and workarounds for the various issues (Ghazizadeh, Manan, et al., 2012).

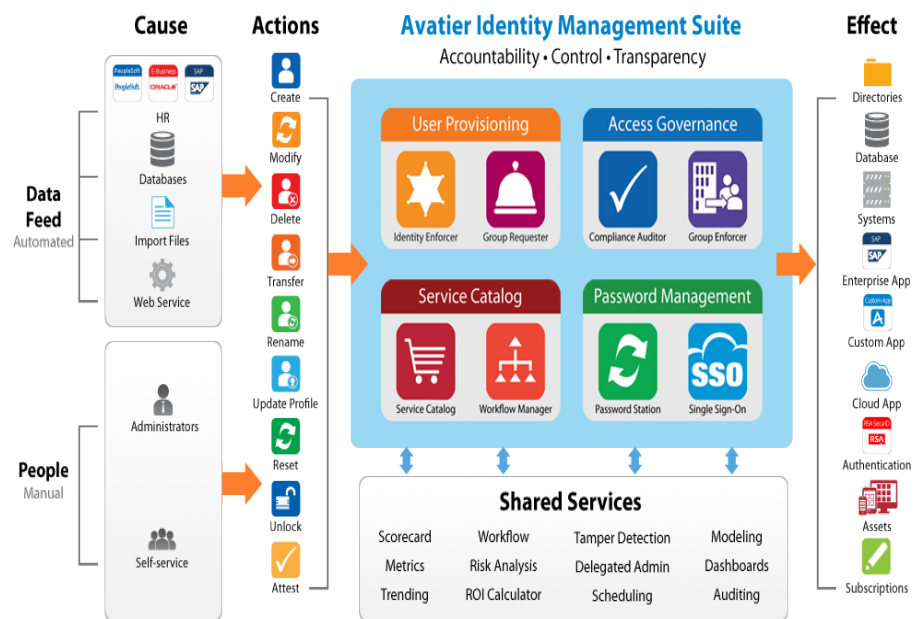
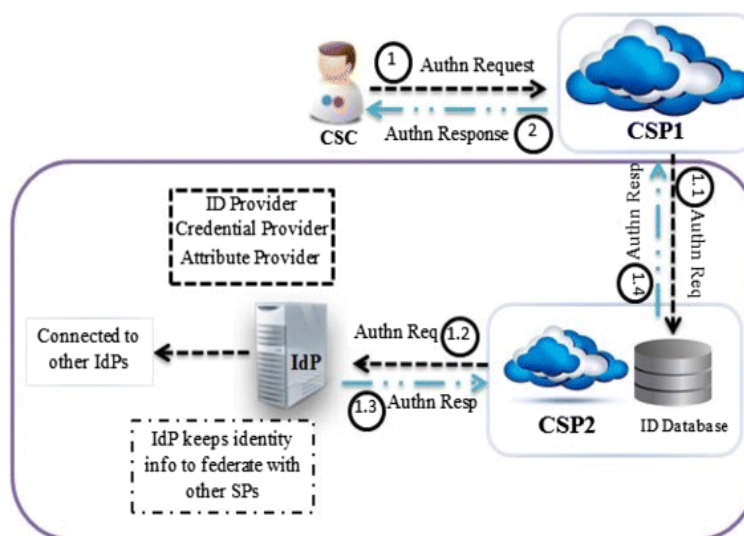


Figure 2.6: Avatier identity management software architecture (Avatier, 2016, p. 3).

2.4.1 Definition

Cloud identity system architecture supports general perspective management for all assets, subscriptions, application access, and physical access for every cloud administrator and user across any enterprise. However, it is based on the concepts of IT configuration and automation rather than development, universal integration and self-service delegated administration to the fullest, therefore, this architecture

should illustrate the universal perspective management of an enterprise application access, physical assets, and IT governance (Tormo et al., 2014).



2.4.2 Cloud Federated Identity

do not need re-authentication for accessing different services while attempting to get access to different domains (Méndez et al., 2016).

2.4.3 Models and Standards

Schäffer (2011) discovered that Isolated, Centralized, and Distributed Digital Identity Management are three different Digital Identity Management models that make use of the roles in digital identity management. First, in the isolated Digital Identity Management model, users have dissimilar identities at the dissimilar Service provider. Besides isolation in the centralised Identity Management model, service providers take advantage of only a central identity provider and a group of service providers trusting the central identity provider. Seamless work and a central point of failure also have been assured by the central identity provider.

Moreover, in the federated environment, all users and service providers should agree to use the same identity provider. Therefore, the distributed Identity Management model supplies the idea of distributed but within federated identity providers. The identity providers are associated which means that all distributed identity providers trust each other. However, in this model centralising of IDP for controlling is not required. It is because of the various distributed components follow the service-oriented architecture. The main goal of this model is that each user has its identity certified by at least one identity provider which is typically not the identity provider of the service provider (Shaikh & Sasikumar, 2013).

Liberty Alliance, Shibboleth, and WS-Federation are three architecture models of federated identity. The Liberty Alliance as a one of the first federated identity services based on the idea of a circle of trust and delivers provisions or digital identity management. The definition of the circle of trust is the idea of conjointly trusting between an identity provider and service provider. As shown in Figure 2.8 the building blocks are the Liberty Identity Web Service Framework (ID-WSF) and Liberty Identity Services Interface Specifications (ID-SIS). The ID-WSF determines a SOAP-based model for detection and registering of identity providers. Simple Object Access Model (SOAP) is a protocol that relies on other protocol such HTTP and SNMP. It is a description for exchanging organised information in the implementation of Web Services in computer networks (Fragoso-Rodriguez et al., 2006).

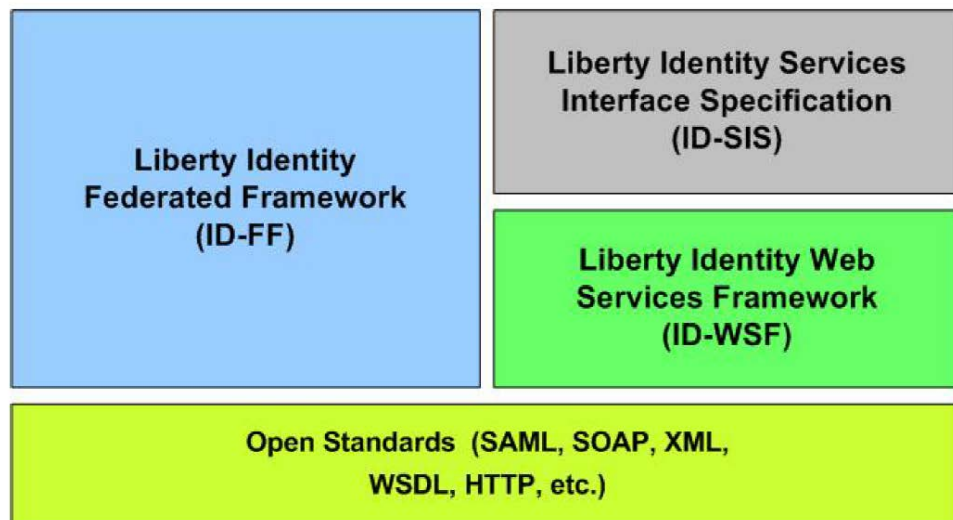


Figure 2.8: The architecture of the liberty alliance and circle of trust (Fragoso et al. 2006, p.3).

Besides Liberty Alliance, Shibboleth also recommends an approach where the main objective is digital recourse between institutions without having to know the user identity explicitly. The building blocks of shibboleth architecture are SSO service, attribute exchange, and where are you from service. The purpose of this architecture is providing security for identity management but also for authorisation purposes. As shown SSO in figure 2.9 is a vital part of Shibboleth with SAML 2.0 as its technical backbone. The aim of Shibboleth is supporting the Liberty Alliance based on guaranteed of personal information.

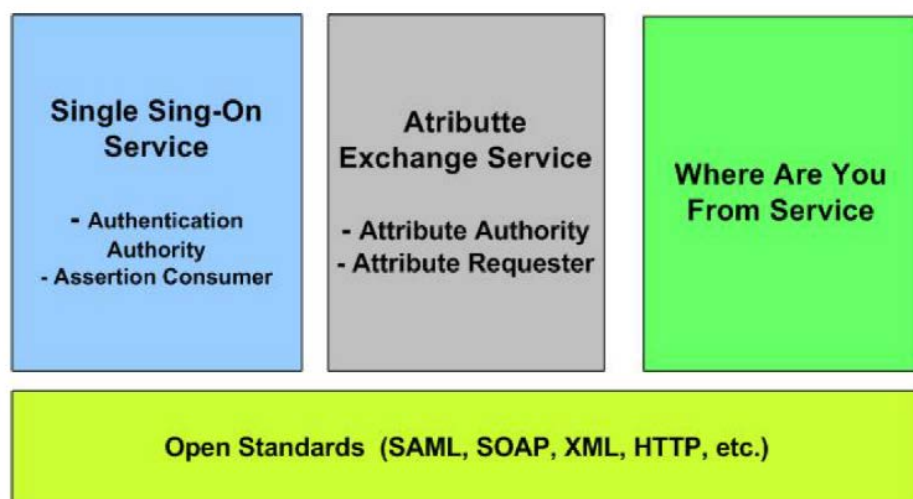


Figure 2.9: Shibboleth (Fragoso-Rodriguez et al., 2006, p. 4).

WS-Federation, as shown in figure 2.10, builds on the WS stack and especially WS-Trust. Especially, the WS-Trust specification is extended to admit and interpret digital identities from other domains into identities trusted and understood in their domain. WS-Federation allows implementing SSO because web users have to acquire an identity only once and the WS-Federation services try to translate the identity if possible.

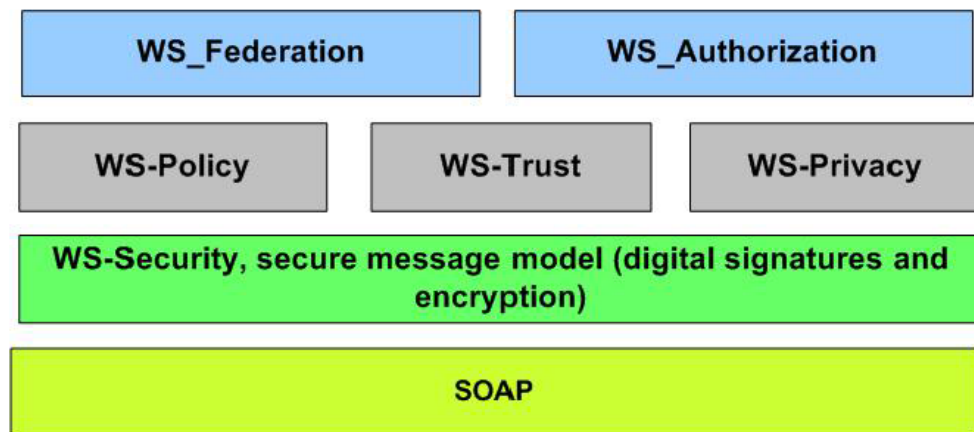


Figure 2.10: WS-Federation (Fragoso-Rodriguez et al., 2006, p. 5).

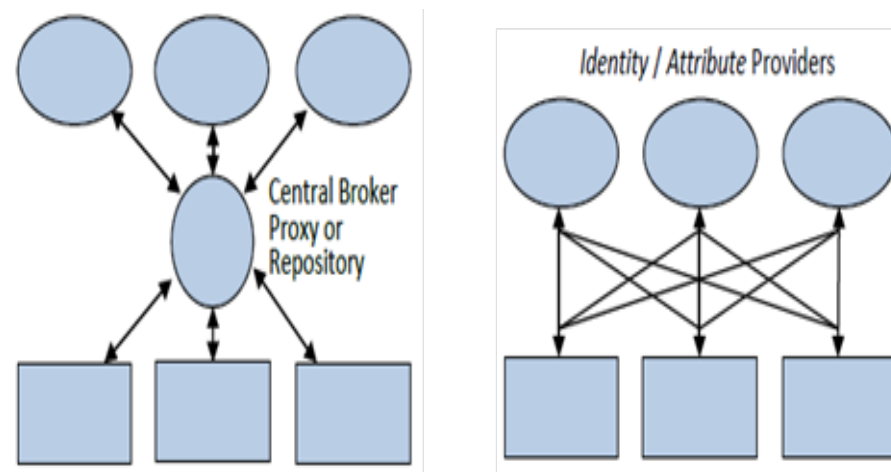


Figure 2.11: Architecture of hub and spoke model and free form model (Alliance, 2011, p. 146).

According to (Alliance, 2011), there are three basic architectures for interfacing to users' identity and attribute providers that have been named hub and spoke model, free-form model, and hybrid model. According to the Figure 2.11, in addition to the Hub and Spoke, Free-Form model is the cloud service and application that is responsible for maintaining the sources of attributes and identity. This model is suitable for public cloud and cloud with a huge number of distinct vendors. Lastly,

free model is suitable for organisations that combined public or private cloud environments with traditional or legacy computing.

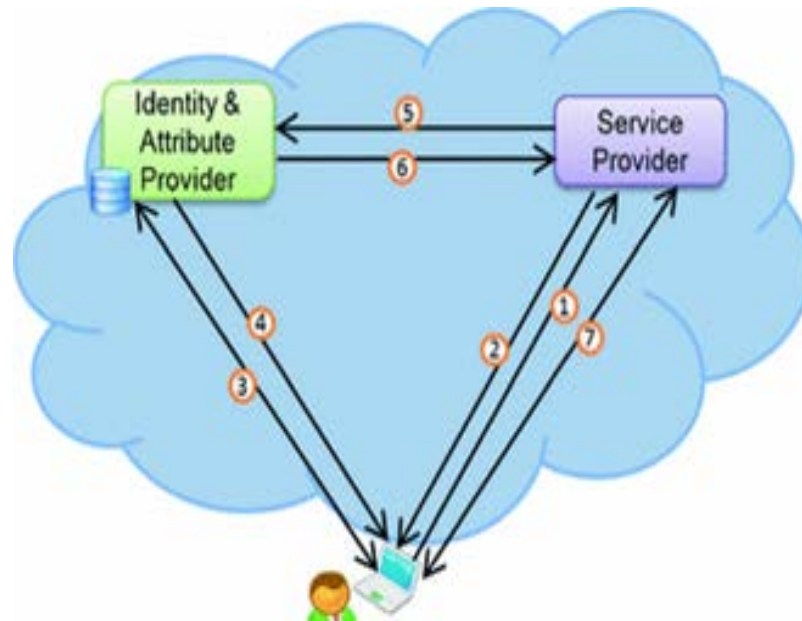


Figure 2.12: FSSO process flow (Tormo et al., 2014, p.183).

In this section numerous IAM and SSO are discussed to identify the technical features. Federated Single Sign-On and Attribute Sharing (FSSO) as shown in figure 2.12 starts with users' information and attributes such as age, postal address, country, and so on. In this method, authentication and attributes could be asserted if they have been issued by an identity and attribute provider (trusted party).

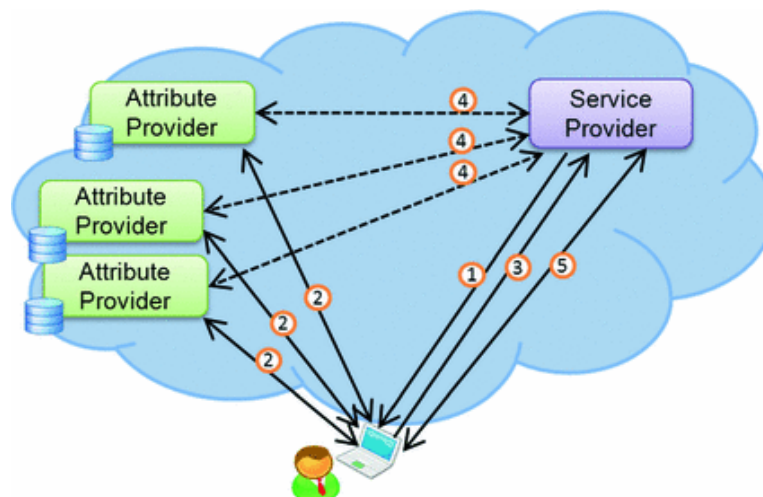


Figure 2.13: AAO process flow (Tormo et al., 2014, p.183).

In Attribute Aggregation and Operations (AAO) as shown in figure 2.13, The user's attributes have been distributed among numerous attribute providers. Therefore, distributed information would be presented to the end user to describe some detailed

information about attribute providers, although a service provider does not assert such information.

Moreover, in Identity Privacy in Shared Environment (IPiSE) as shown in figure 2.14, service providers need end user's attributes either to provide the identity and attribute provider to perform access control or to provide customised services by the service provider.

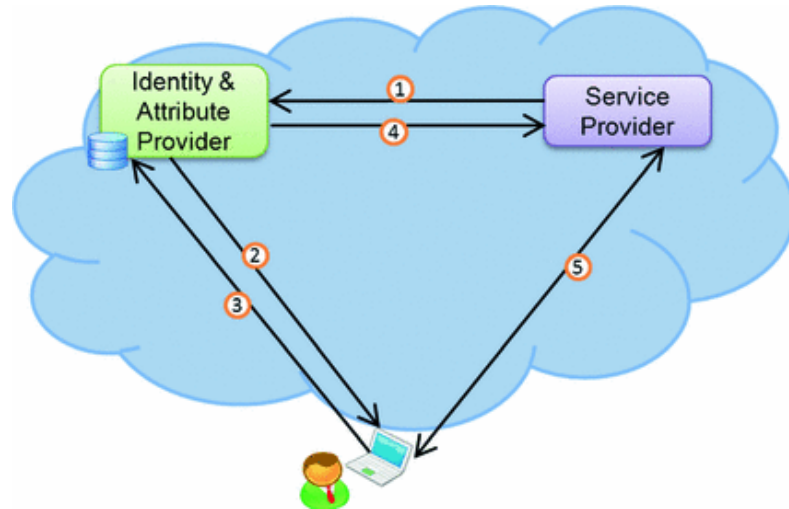


Figure 2.14: iPiSE process flow (Tormo et al., 2014, p.183).

Moreover, in the regard of provisioning and de-provisioning identities in the cloud services, some vendors based on their infrastructure use standards which are listed below:

- Services Provisioning Markup Languages (SPML): It is an XML-based framework which is used for user's identities, resources and services provisioning. Also, Provisioning Service Point (PSP), Provisioning Service Target (PST), and Requesting Authority (RA) are the three main components of SPML (Rolls, 2003).
- Security Assertion Markup Language (SAML): SAML also is an XML framework for exchanging authentication and authorisation information. Assertions, protocol, and binding are three components of SAML (Campbell et al., 2015).
- Simple Cloud Identity Management (SCIM): Open Web Foundation has developed the SCIM protocol to parse the SPML's complicated features to be implemented by the providers (Lonea et al., 2013).
- eXtensible Access Control Markup Languages (XACML): In order to get an access control for communicating policies by providers, the XACML has

been created. It includes policy language which is composed of rules that have a permit or deny actions (Ferraiolo et al., 2016).

- Lightweight Directory Access Protocol (LDAP): To access and maintain the distributed directory information services over an IP, LDAP has been designed to allow sharing of information about users, networks, services, systems, and applications throughout the network (Zissis & Lekkas, 2012).
- JavaScript Object Notation (JSON): JSON by using lightweight data exchange is based on the easily read and write policy (Bray, 2017).
- eXtensible rights Markup Language (XrML): It is designed for managing and securing rights and conditions associated with numerous resources such as digital content or services (X. Wang et al., 2002).



Figure 2.15: OpenID general workflow (Tormo et al., 2014, p.195)

2.4.4 System Access

The most common identity management technologies and solutions to manage end user's attributes analysis is the main aim of this section. Therefore, the advantages and disadvantages of the system access are highlighted in regard to the cloud identity system access.

OpenID, as shown in figure 2.15, as a part of the SSO, is commonly used by cloud service providers for exchanging the identity credentials. It is based on the SAML protocol which is determined by the same requirements for web SSO, but the design goal is different. Especially, the main idea of OpenID is that a user can authenticate by URL and then exhibit their preferred OpenID Provider (Recordon & Reed, 2006).



Figure 2.16: OAuth general workflow (Tormo et al., 2014, p.195)

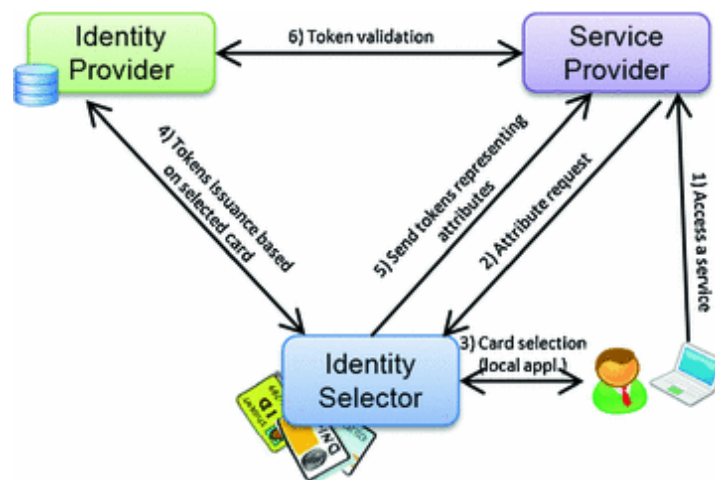


Figure 2.17: Windows CardSpace General Workflow (Tormo et al., 2014, p.195)

OAuth as shown in figure 2.16, defines a protocol in order for clients to access server resources on behalf of a resource owner. It provides a process for end users to authorise third-party accesses to the server resources without sharing the credentials (Hardt, 2012).

Windows CardSpace (figure 2.17) or InfoCard, is the system which has been designed by Microsoft for identity selection. It allows the end users to align with an identity lifecycle and create, use, and manage their identities. The main idea behind it is to manage the digital identities, along with user's attributes same as managing the wallet's cards (Bertocci et al., 2007).

U-Prove is a method that is using the cryptography techniques to encode end users' attributes. Utilising the Zero-knowledge methods is the main feature of the issuing the tokens by U-Prove standards as shown in figure 2.18 (Mostowski & Vullers, 2011).

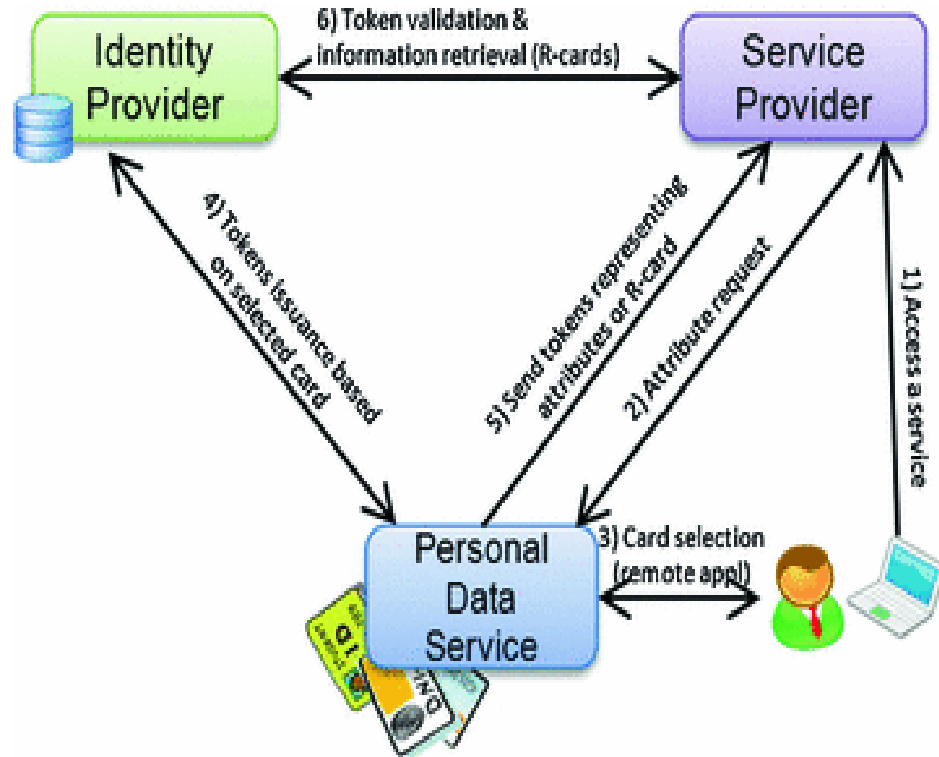


Figure 2.18: U-Prove general workflow (Tormo et al., 2014, p.195)

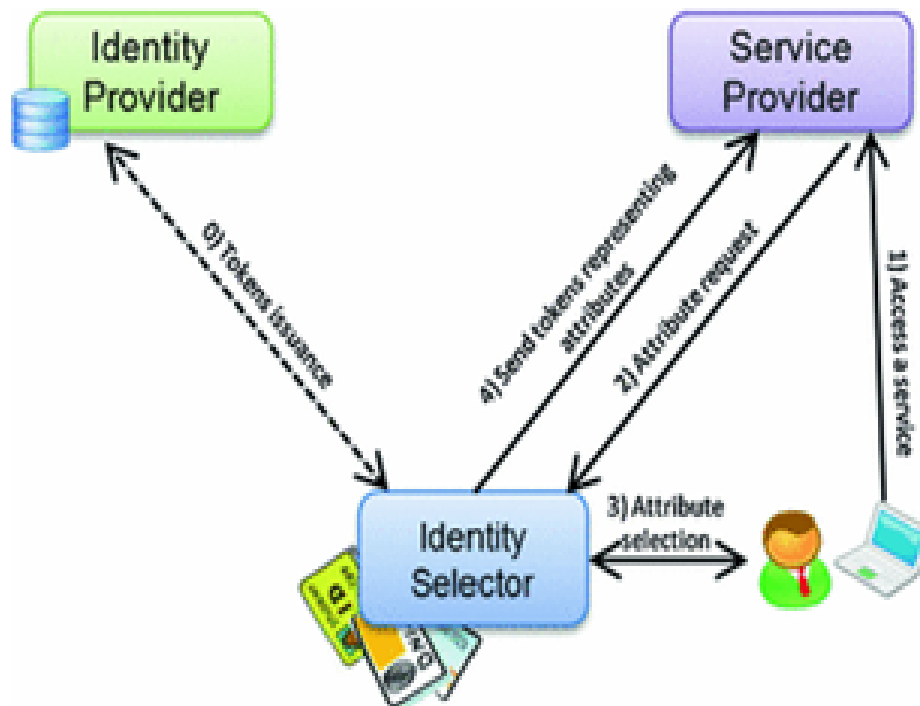


Figure 2.19: Idemix general workflow (Tormo et al., 2014, p.195)

Identity Mixer (Idemix) (figure 2.19) It is similar to U-Prove but focuses on privacy which allows the customers to control the dissemination of personal information and enhances user's privacy (Tormo et al., 2014).

Moreover, Higgins as shown in figure 2.20, is designed to integrate the social relationships information and identity profiles with numerous providers to improve the open source identity framework (El Maliki & Seigneur, 2007).

Besides, OpenID Connect (Sakimura et al., 2014) is based on the OAuth 2.0 protocol is used to simplify the process of identity management. The functionality and workflow of OpenID connect is shown in figure 2.21 and is explained in more detail in chapter three.

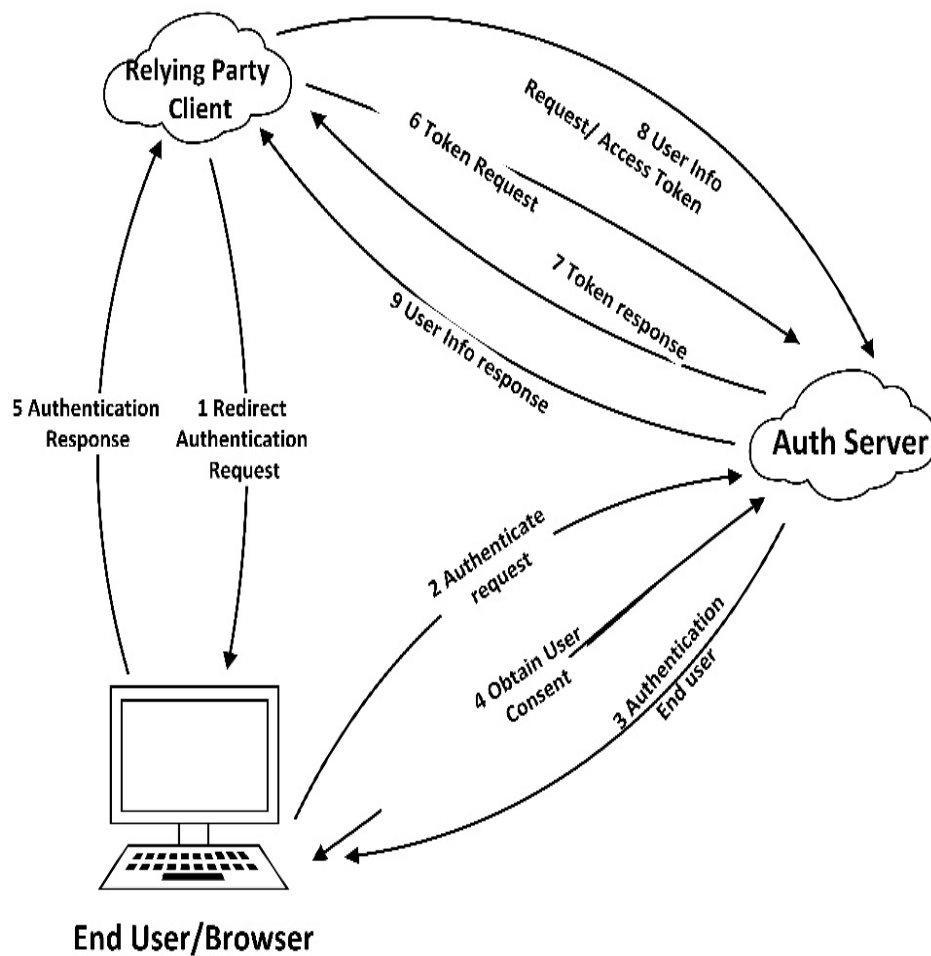


Figure 2.20: Higgins general workflow (Tormo et al., 2014, p.195)

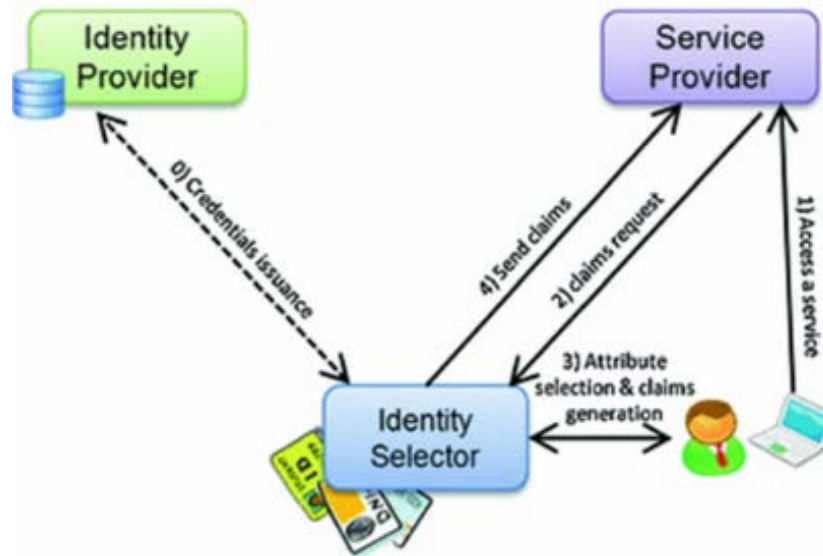


Figure 2.21: OpenID connect general workflow (Sakimura et al., 2014, p. 6)

2.4.5 Limitations of IAM Protocols

Tormo et al. (2014) in their research summarised the features and limitations of the common identity management protocols. They grouped these identity management systems based on their requirement in three main parts: General requirements, User-centric capabilities, and Information management functionalities. They found that there is no ideal common identity management protocol fulfilling all the requirements. Therefore, based on their research, Figure 2.22 indicates the level of requirement fulfilled, and table 2.1 illustrates the current level of security, trust, privacy and the overall weight based on the technical features which is used in chapter five as a method to measure the strengths and weaknesses of the IAM standards.

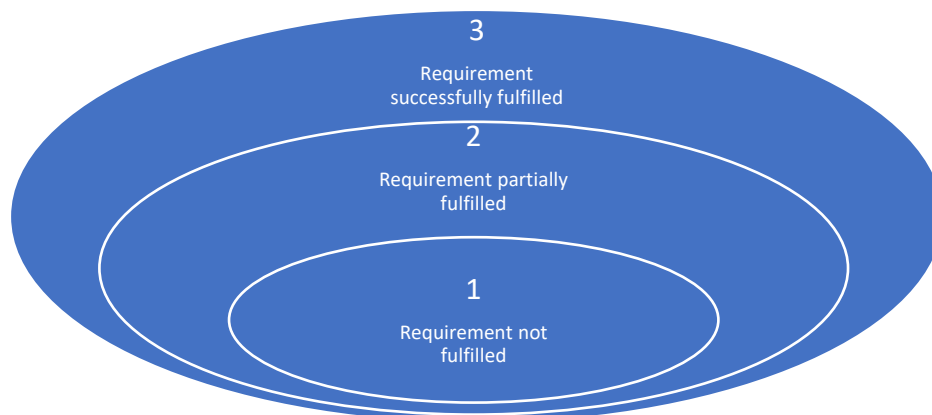


Figure 2.22: Levels of requirement fulfilled

Table 2.1: Comparative of current IAM solutions

Category	Code	Essential functionality/ requirements/ operation	OpenID	SAML	OAuth	CardSpace	Higgins	UProve	Idemix
General requirements	R1	Confidentiality and integrity	3	3	3	3	3	3	3
	R2	Single Sign-On	3	3	3	3	3	3	3
	R3	Logging and Auditing	3	3	2	3	3	1	1
	R4	Strong authentication	2	2	1	3	3	3	3
	R5	Justifiable parties	1	2	3	2	2	2	2
User-centric capabilities	R6	End user consent	3	1	1	3	3	3	3
	R7	Control of accumulated data	1	1	3	3	3	3	3
	R8	Usability	3	3	3	2	2	1	1
Information management functionalities	R9	Off-line mode	1	1	3	1	3	1	1
	R10	Attribute aggregation	1	1	1	1	1	1	1
	R11	Attribute revocation	3	3	2	2	2	1	1
	R12	Self-asserted attributes	2	1	2	3	3	3	3

Category	Code	Essential functionality/ requirements/ operation	OpenID	SAML	OAuth	CardSpace	Higgins	UProve	Idemix
	R13	Minimal disclosure information	3	1	2	2	2	1	1
Overall			29	25	29	31	33	26	26
Average			2.23	1.92	2.23	2.38	2.54	2	2

2.5 TRUST COMPUTING

Trust is a complex concept, which there is no universally accepted scholarly definition. Trust is a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behaviour of another (Pearson, 2013). Moreover, trust is a broader notion than security as it includes subjective criteria and experience. Correspondingly, there exist both hard (security-oriented) and soft trust solutions. ‘Hard’ trust involves aspects like authenticity, encryption and security in transactions, whereas ‘soft’ trust involves human psychology, brand loyalty and user-friendliness. An example of soft trust is reputation, which is a component of online trust that is perhaps a company’s most valuable asset (Ghazizadeh & Cusack, 2016b; Wang & Lin, 2008).

Therefore, trust has the crucial role in assisting the CSCs in the selection of trustworthy and strong trusted providers to identify the most reliable providers and soft-security. Trust has different definitions in different fields, and its properties also different from context to context. In this research, these properties are:

Intransitive: if agent X trusts Y, and Y trusts Z, it is impossible to conclude that X also trusts Z. However, under some conditions, X can trust Z.

Asymmetric: a member may trust another member more than he (she) is trusted back (Yaniv & Kleinberger, 2000).

Dynamic: trust value may change over time, and the most recent value of the trust is more informative thus, it needs to be updated. Subjective: when a cloud user chooses to trust or distrust a provider, it is a personal choice. Each user has its preference or interests (subjectivity) that influence their trust reasoning (Fang et al., 2012).

Context-aware: It means different scenarios have different types of trust (Zhang & Zhang, 2012).

While in term of data protection, security might be the main area, but, trust is a much stronger concept that goes beyond availability, confidentiality, integrity, and non-repudiation (the basic security attributes). Trust aims to conduct a proper relationship between service providers as well as customers. However, in the point of IT, trust is not only about securing the communication channel or authenticating the data sender but also the validity of the data is important (Fournaris & Keramidas, 2014). People often find it harder to trust online services than offline

services because in the digital world physical cues are absent and there may not be established centralised authorities. The distrust of online services can even negatively affect the level of trust accorded to organisations that have been long respected as trustworthy. Some would argue that security is not even a component of trust and they argue that the level of security does not affect trust (Pearson, 2013).

“Trust, but verify” (Huang & Nicol, 2013) is respectable guidance for the relationship between CSPs and CSCs. Even though, after establishing the trust and using the CSP’ service, the CSC requires to re-evaluate and verify the CSP’ trust level. Therefore, based on the current literature, QoS monitoring (Manuel, 2015) and Service Level Agreement (SLA) (Na & Huh, 2014) verification are some of the important trust attributes basis for trust management in the CC area. RSA announced Trust as a Service (TaaS) and Cloud Trust Authority (CTA) (Coveillo et al., 2011) which provides a single point for managing and configuring the security of CSPs from numerous providers. Enabling single sign-on among multiple cloud providers, identity service, and compliance are three initial profiling services of CTA. CTA aims to promote the CSCs to view the security profile of federated cloud providers against a common benchmark.

2.5.1 Cloud, Trust, Control and Visibility

As organisations struggle to leverage cloud service providers more widely, there is a cause for concern related to the cloud (Alabool & Mahmood, 2015). These organisations do not have the level of trust that they enrolled in their infrastructure, and this causes them to limit the adoption of cloud services (Gantner et al., 2015). Trust emanates of control and visibility over IaaS, PaaS, and SaaS (Kanstrén & Evesti, 2015). On the other hand, trust is control and visibility over identity, infrastructure, and information elements in the cloud. The identity perspective concerns and questions are:

- How will enterprise users securely do federate single sign-on and be federated onto cloud services?
- Is on-site enterprise directory be used?
- Will they use duplication and use the repositories?
- Will there be strong authentication over the internet as enterprise users access sensitive assets in the cloud with strong authentication?

However, regarding infrastructure integrity, geographic location, and hardening are three main concerns. Hardening infrastructure means a basic control that needs to be in place to ensure a system is patched, and the protective network is defensible. The confidence is that these processes are in place and those controls are in place for the organisation to be secure. The common concerns of information security are the confidentiality and privacy of sensitive data in the cloud. It has these questions.

- Who has access to this information?
- Can service provider abuse this information?
- Do other tenants share that infrastructure has access to my data and information?
- Is my data going to be when I need it?
- Who can access to this data and use these data?

Finally, organisations are required to maintain compliance regardless of where the infrastructure is run or secured, and they must ensure the service providers are following the correct compliance practices. Therefore, based on these trust and security concerns, cloud providers do offer security options along with their services to address some of these concerns, but no service provider offers all. In addition, security transparency from provider to provider is different, and these cause a lot a burden on the end customer who has to put together a picture and a consistent process across all the service providers they use.

Essentially the combination of these security and trust issues leads to slowing down a broader adoption of the CC. Therefore, lack of trust especially causes a lack of adoption. In addition, a systematic problem needs to be addressed. How these multiple organisation, users, and service providers would interact which each other? Also, it leads to having a trust relationship when thousands of these organisations have interaction with millions of cloud services. It is a many to many scenario and makes a very complex set of integrations, which are burdensome. The cost of initial and ongoing interaction leads to a new model that allows the security concerns to be systematically addressed and this why it is intended in this research to develop a cloud identity trust framework. This framework will not only comprehensively address these concerns but also establish the right balance between them.

2.5.2 Cloud and Assessment

Organizations are being encouraged to adopt the CC solutions before implementing assessment tools. To support this evaluation requirement, “Cloud First” (Kundra, 2011) provides evaluation for a variety of cloud attributes before the user makes any decision and investment. Therefore, an objective third party assesses and authorises cloud providers through a risk assessment and security measurement program. Consequently, CSC can select an authorised CSPs to host their assets. The trusted third party would benefit from a technique for independently validating the effectiveness of security controls that have been asserted to be in place. Threats to cloud need consideration for efficient security controls. To provide secure service, the Cloud users’ perspective should be considered for evaluation in all entities as shown in figure 2.23.

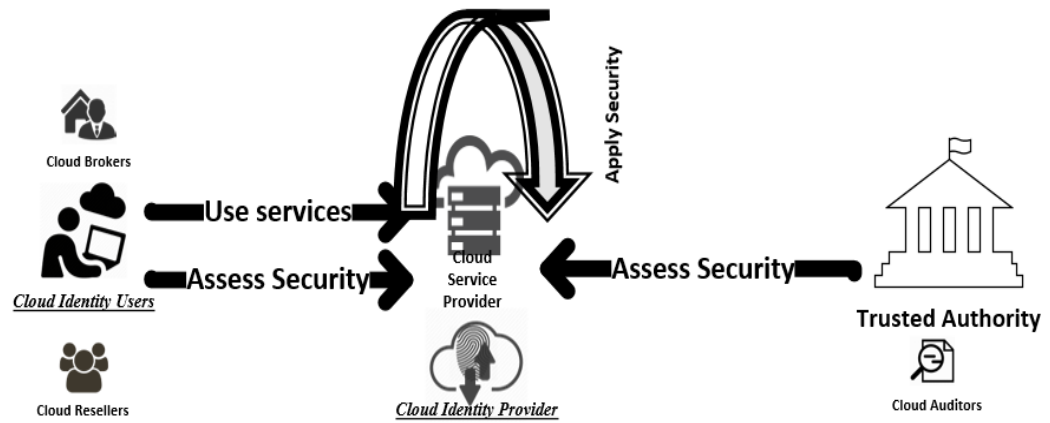


Figure 2.23: Visibility of the security in the cloud (Hilgers & Auger, 2015, p. 6).

Figure 2.23 shows Cloud customers who should assess service providers as well as trusted authority. The aim of the (Hilgers & Auger, 2015) research is to develop a trusted model for public CIdPs and proposed novel methodology for objectively assessing CIdPs’ trust level from an end-user perspective as well as the trusted third party.

2.6 LITERATURE SUMMARY

As a summary for this chapter, the problems and issues in the IAM area based on the current literature are identified to find the essential gaps of the IAM in a cloud environment. Several issues and threats that can compromise the IAM’s behaviour when attackers try to destabilise the cloud system are listed. Therefore, Privacy, security, and trust are three main issues and threats to be analysed in the following sub-sections.

2.6.1 Privacy Conclusions

Privacy is a coveted element of any correspondence system. However, CSCs desire to secretly store their identity and information, but, on the other hand, the CSPs need to know the information about their customers. Though some CSPs do not need to know the real identities of their customers, but they want to gather the most relevant information about them. Therefore, to fulfill both providers and customers expectation, IAM have to preserve customers' privacy by implementing strong privacy methods which provide anonymity (lack of the knowing real identity of the CSCs by the CSPs), unlikability (lack of link between numerous CSCs accesses by the CSPs), and intractability (lack of knowing the services which have been accessed by the CSCs).

Moreover, new policies by policymakers, the concept of fairness, and emphasised by the governments (Nicolaidou & Georgiades, 2017) are pushing for major changes in regards to privacy for individuals compared with the common pragmatic approach. The draft US Privacy Bill of Rights (Parker, 2017) and the EU General Data Protection Regulation (GDPR) are two examples of changes to privacy concerns. Moreover, they offer numerous and crucial changes for CSPs that need to meet various global privacy regulations. Trans-border data flow restrictions and geographic regulation are two most common privacy issues for the CC environments. The analysis of the privacy issues in this research showed that a lack of user control, lack of training and expertise, unauthorised security usage, complexities in regulatory compliance, trans-border data flow restrictors, and legislation are common privacy issues which have been shown in section 2.2.3.

2.6.2 Security Conclusions

CSP is the same as any computation system is exposed to various security risks which can compromise the security of their system. It is obvious that attackers by utilising the malicious intents with novel methods are trying to attack any service providers by knowledge and enumeration methods. The security issues are crucial for CIdPs because they manage CSC's sensitive data (digital identity). Therefore, in respond to security issues, IAMs need to provide a concrete system to protect digital identities and mitigate the identity theft.

Based on the discussion in the previous sections, there are different attacks and security vulnerabilities for both CSPs and CIdPs. Some of them are coming

from the traditional computing, but some of them are new. These attacks need new methods and research to mitigate the threats (Sethi & Sruti, 2018). As a summary for the security issues (figure 2.24) the researcher found that unwanted access, vendor lock-in, inadequate data deletion, compromise of the management interface, backup vulnerabilities, isolation failure, missing assurance and transparency, inadequate monitoring, inadequate compliance, and inadequate audit are the most common issues which have to be considered.

2.6.3 Trust Conclusions

The main aim of any IAM (business objective) is to establish the trust between their customers and themselves. Moreover, simplifying the CIdP's selection is another aim of the IAM by exposing their characteristics and attributes to help their customers make a good decision. Furthermore, the CSC and CIdUs are looking for the specific and particular identity providers based on their different security and privacy perspective. However, based on the trust definition if one of the providers acts maliciously, then the rest of the providers have the potential of the risk. Therefore, IAM is required to deploy and adopt the best practices to allow providers to trust each other.

Trust boundaries in a traditional security model means a place that stores sensitive data and provides self-control over computing resources. However, this model does not work for the public and hybrid cloud because of their complex features. On the other hand, in order to obtain the service, CSCs need to extend their trust to the CSPs, and this is a point of friction that requires further consideration. Moreover, it is vital that technological and social mechanisms should be integrated to identify the level of trust for any providers to produce persistent trust. Furthermore, the research found that at the centre of security and privacy solutions trust has an essential role. Based on the systematic analysis of the literature, this section has found that the crucial inhibitor to adoption of cloud services is the lack of consumer trust. On the other hand, CSCs are concerned about who can access it and how it is used, and also who can share and copy their data. Therefore, weak trust relationship, is another trust concern for the CSPs and CIdPs because the migration to the cloud is a trade-off between security, privacy, compliance, costs and benefits for the CSCs. Furthermore, trust mechanisms are another trust issue which is required to be considered by the CSP and CIdPs to provide a strong and

reliable trust management method to gain the trust between all parties. As a summary, a lack of the consumer trust, weak trust relationships, and trust management approaches, are the main trust issues in the cloud environment which is summarised by the researcher in figure 2.24.

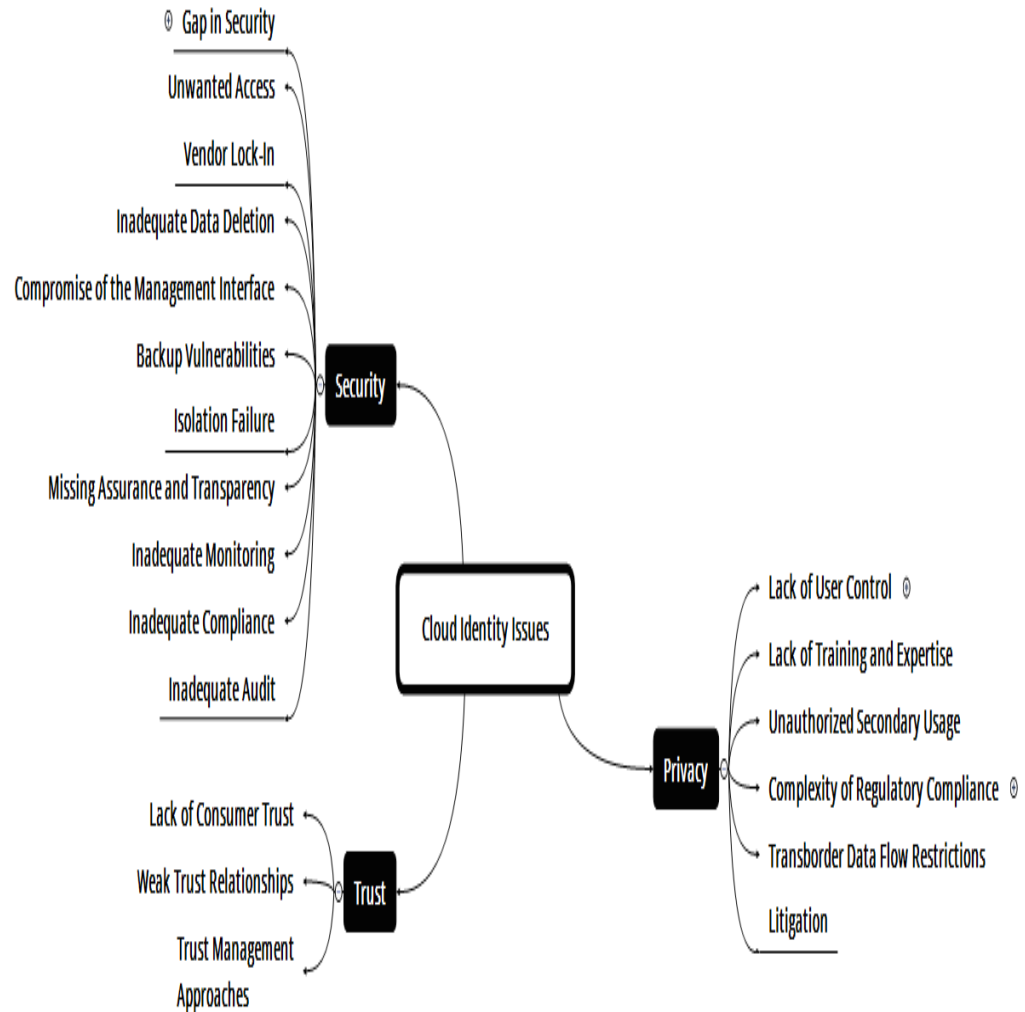


Figure 2.24: Privacy, security, and trust issues

2.7 CONCLUSION

In conclusion, with utilising the Delphi method, this study focuses on the most important issues enterprises are confronted with CC, cloud identity, and trust computing adoption decisions. In this regard, the researcher found that the Delphi method is one of the best ways to identify and prioritise issues for managerial decision making for this thesis. Therefore, the researcher first identified the questions below and consequently in the rest of the thesis these assist to guide the research:

Q1: What issues confront entities when adopting cloud, CC, and trust computing?

Q2: What is the relative importance of these issues?

Q3: Why are these issues important?

Therefore, this chapter identified the current issues in the research scope (CC, cloud identity, and trust computing). It also prioritised the relative importance and performance of the current issues. The researcher after systematic analysing has found that while there are studies that have focused on the technological aspects of cloud, cloud identity, and trust, still the decision making to adopt and migrate to cloud solutions is complicated for the cloud users. As a summary, in chapter two the key points are identified and contributed to the thesis:

- Cloud security issues and their technical controls (Evolving challenges)
- Cloud identity issues from provision to de-provision (lifecycle)
- IAM theft and attacks
- Architecture and deployment models for identity
- Centralized, Isolated, and Distributed Digital Identity Management
- Cloud identity system access
- Limitations of IAM Protocols
- Comparative of the current IAM solution as discussed in table 2.1
- Analyse the cloud, trust, control, and visibility and their role in the knowledge base decision making
- Privacy, security, and trust conclusions

This chapter is preparing the current literature and gaps for the chapter three. Therefore, in chapter three, the problem statement and methodology in response to the problem is discussed (response to the gaps). Chapter three is concerned with the methodologies (method to response to the gap), research questions, hypotheses, and steps to get the research objectively focused on the issues that have been explored in chapter two.

Chapter Three

Methodology

3.0 INTRODUCTION

Chapter two has reviewed the theoretical and technical contexts for trust computing in CC by focusing on cloud identity management and trust computing. Chapter two defined the cloud, cloud security, privacy, trust issues, cloud identity, cloud identity issues, trust and trust computing solutions in the cloud. In chapter three the main problem is stated, and consequently, the solution model proposed. A mixed method of trust and DS methodology is innovated and developed as the methodology for this research.

Therefore, in section 3.1 the proposed trust framework based on the figure 3.1 is explained. Section 3.2 is evaluated the trust establishment. The research questions, and hypotheses are followed by the problem statement in section 3.3. Trust system methodology in section 3.4 is explained and justified. In the following sections, the design to identify the answers to the questions and test the hypotheses, evaluation methods, and communication are elaborated in section 3.4. In section 3.5, systematic literature, section 3.6, implementation and usability checking, section 3.7, expert evaluation, section 3.9, data analysis, and in section 3.9, communication are justified.

3.1 PROBLEM STATEMENT

In chapter two, by using the Delphi theory, the issues of the CC regarding security, trust, privacy, and monitoring have been identified. In addition, cloud identity, federated identity access management, and access control have been analysed, and their security, trust and privacy issues have been outlined. Chapter two has concluded by the importance of integrating the trust computing definition and proposing trust framework between CIdUs, CSPs, and CIdPs, which entails trust between providers as well as cloud users. Furthermore, chapter two revealed that still there are some questions that should be answered by the researcher to identify the cloud security and trust issues. Therefore, the research aims to answer these questions. However, as a science research as the (Hevner & Chatterjee, 2010)

indicated any design science research like this research should be able to answer the following questions:

- What is the research question (design requirements)?
- What is the artefact? How is the artefact represented?
- What will design processes (search heuristics) be used to build the artefact?
- How are the artefact and the design processes grounded by the knowledge base? What, if any, theories support the artefact design and the design process?
- What evaluations are performed during the internal design cycles?
- What design improvements are identified during each design cycle?
- How is the artefact introduced into the application environment and how is it field tested?
- What metrics are used to demonstrate artefact utility and improvement over previous artefacts?
- What new knowledge is added to the knowledge base and in what form?
- Has the research question been satisfactorily addressed? (Hevner & Chatterjee, 2010, p.20)

Besides of the answering these essential questions, reliability and validity of the research are two common methods to state how research is adequate (M. Berndtsson et al., 2008). Therefore, these questions are answered by elaborating and modifying previous methodologies and adopting them based on the complexities in the cloud environment. These questions are an outline of the research methodology and show the main problem (s) which should be solved in this research (Haber, 2006). Therefore, the aim of this chapter is articulating the research questions based on the previous chapters (chapter two and problem statement (3.1)). Furthermore, to achieve the best outcome and trust management framework in a security and privacy context research questions and hypotheses have been identified. Based on the (Ghazizadeh & Cusack, 2016a), there four different question categories which should be answered. The first category is cloud *security* issues. In this category, there are the following questions:

- How are safety mechanisms provided to monitor or trace the cloud server?
- How data is kept confidential for individuals and sensitivity?

- How to avoid a malicious insider's illegal operations through the potential lack of transparency into provider process and procedural environments?
- How to avoid service hijacking, where phishing, fraud and exploitation are well-known issues in IT
- How to manage multi-instances in multi-tenancy virtual environments, when all instances are assumed isolated from each other.
- How to develop appropriate law and implement legal jurisdiction, so that users have a chain of evidence against their providers when required.

Next category is cloud privacy, which means the ability of an individual or group to control themselves or information about themselves and thereby reveal themselves selectively. The privacy issues differ according to different cloud scenarios (Xiao & Xiao, 2013), and can be divided into four subcategories as follows:

- How to make users retain control over their data when it is stored and processed in the cloud, and avoid theft, nefarious use and unauthorised resale.
- How to guarantee data replications are in a fixed jurisdiction, a consistent state, and has no data loss, leakage and unauthorised modification or fabrication.
- How to identify the party that is responsible for ensuring legal requirements for personal information?
- How to check and verify cloud sub-contractors, which involved in the processing of data?

Trust in social science is vital to building the relationship between and in the computing are is crucial for building security mechanisms in the CC environments. Reliability, confidence, belief, dependability, trustfulness, and honesty are soft attributes of trust (Manuel, 2015). However, trust evaluation is a multi-faceted and multi-phased phenomenon based on multi-dimensional factors and the trust evaluation cycle. Trust establishment is trying to find the answer for the “With which service providers should use and interact with, and which I should not?” Bezzi et al. (2011) categorised the CC trusts into four sub-categories:

- How to define and evaluate trust according to the unique attributes in the CC environments?
- How to handle malicious information when trust relationships in clouds are temporary and dynamic?
- How to consider and provide a different security level for service according to the trust degree?
- How to manage trust degree change with interaction time and context, and to monitor, adjust, and to accurately reflect the trust relationship dynamic?

Monitoring issues in the CC environments are the last category in this section. The questions in this area can be divided into four subcategories, and their answer could help the researcher to find the requirement for proper and accurate monitoring and measurement techniques (Dondio & Longo, 2011).

- How to best monitor and measure provision of scalability, load balancing, Quality of Service (QoS), service continuity and application performance?
- How to guarantee SLAs?
- How to realise the best measurement for management of large-scale, complex and federated infrastructures?
- How to evaluate the causes of end-to-end performance?

Therefore, based on chapter two, to overcome many of the security, privacy, trust, and monitoring issues in the cloud area (Ghazizadeh & Cusack, 2016b). However, establishing trust relationships (chapter two) with trust attributed between providers and customers, IAMs offer a huge range of features both for CIdUs and for CIdPs regarding controlling and exchanging information related to end users' identity (Ghazizadeh & Cusack, 2016c). Therefore, researching these problems and attempting to find the solution (answering the questions) by building a trust framework along with trust elements that enable CIdPs to have a trustable identity environment for cloud customers. As a result, in the next section, research questions for this thesis are identified. These research question state what I want to learn and investigate in the cloud area and hypotheses are the experimental and rational answers to the research questions.

3.2 ESTABLISHING TRUST

The gap that can be acknowledged in the literature for this study is that no effective and unified cloud identity trust framework is developed to help cloud users to identity trustworthy CUdPs. This study shows the character of the CC focusing on identity management and the problem identified in chapter two. As a result of in-depth analysis of various IAMs in chapter two, especially in section 2.3 and 2.4, and also based on the result, which reveals most of the systems do not offer support to all the essential security, privacy, and trust features of IAM, and they have weaknesses. None of the discussed techniques heuristically cover all the security, privacy, and trust features. Furthermore, the current gaps, challenges, new security perimeter, and risk assessment have been identified which related to IAM that must be considered by the CIdPs and CIdUs. In section 2.4, trust computing, trust features, and its applications have been discussed. How can trust computing help CIdUs to make a good decision based on the CIdPs' trust attributes? Also in this section the requirements to locate the trusted computing with cloud IAM is described. OpenID connect is selected because it is one of the latest and common IAM for the CC.

OpenID Connect is the new emerging standard for cloud IAM and identity provision in cloud environments. It is based on the browser-based, simple JSON-based identity tokens (JWT), and delivered via the OAuth 2.0 protocol for the web. The workflow of the OpenID Connect has been shown in figure 3.1, and it is as follows:

- Request CSP resources
- Discover the CIdPs
- Redirect CIdU to SSO service provider (CIdP)
- Request and Response identity checking
- Request Assertion to the CSP
- Exchange code for access token and ID Token between CIdP and CSP
- Obtain user information from the ID Token between CIdP and CSP
- Authenticate the User by the CSP
- Moreover, based on this workflow there are three main steps as below:
 - Authorization request and grant between CIdU and CSP
 - Authorization grant between CIdU and CIdP

- Access token and protected resource between CIdU and CSP

In OpenID connect there is a comprehensive shift of responsibility of authorisation, controlling and maintaining the identity from CSPs to CIdPs. However,

CIdPs have control of the CIdUs identities while CSPs have no control over these assets (Sakimura et al., 2014). Therefore, this shift of responsibility causes trust concerns between CIdUs and CIdPs. The trust concern stems from a lack of control, lack of visibility and lack of governance over the identities of CIdUs. As such CIdPs should show the capability of offering assurances which are beyond the functional and non-functional properties. They could be trust attributes such as integrity, security, privacy, accountability, reputation, competence and ability, predictability and assurance. CIdUs will consider CIdPs trustworthy if the providers are able to fulfil the assurances on these trust attributes. Therefore, CIdUs have faced two issues as shown in figure 3.1.

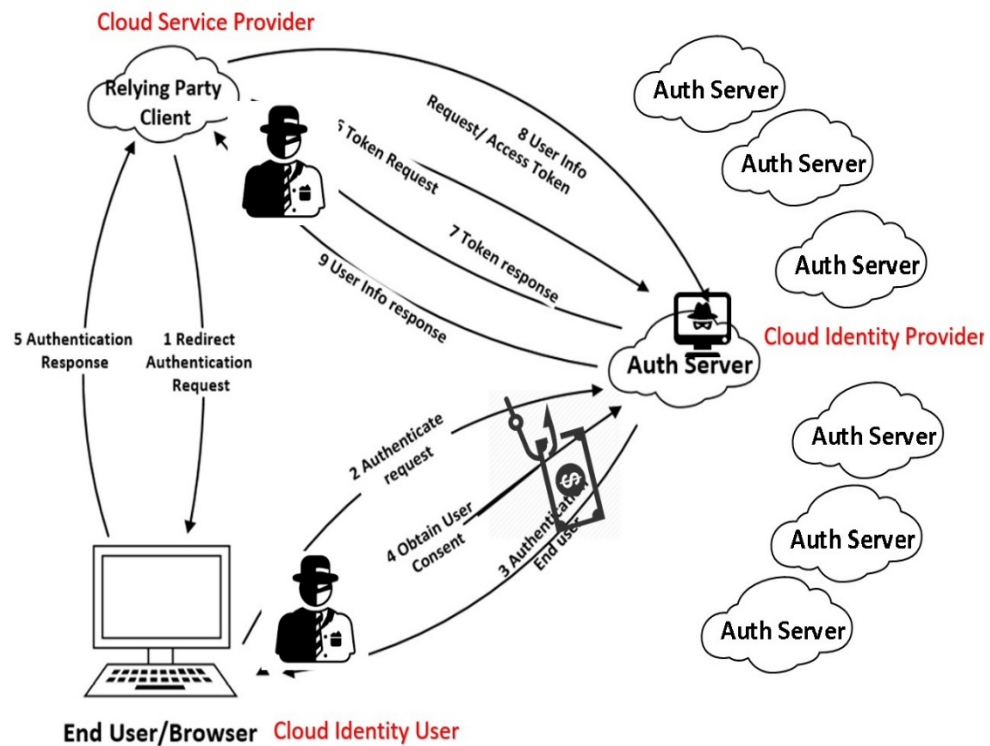


Figure 3.1: Workflow of OpenID connect and trust issues

First, they are faced with provider decision making, but, it is very difficult to make a good decision unless it is based on the results of a trust evaluation. Evaluating trust levels in the cloud identity environment could play an important role in understanding how CIdPs could prepare the trust level based on the trust elements and help the CIdUs to make a good decision. Furthermore, identifying the un-

trustable CIdPs can maximise the level of trust and minimise the level of risk to an acceptable level. Hence, the CIdPs not only have a clear sense of whether their service trust level is high or low but also how to improve the level of trust. However, the issue of how CIdPs' trust level could be evaluated became more significant and is focused on when improved service update is required.

Second, based on figure 3.1 if any attack or identity theft which has been mention in section 2.3.4 will happen the SSO credential is lost, and hackers can use it for other service providers (Ghazizadeh & Cusack, 2016b). The problem here is that CIdUs put all the tokens (SSO) in the one container (CIdP), but this makes security management more challenging. When hackers are able to access the request, delete one piece of requested information and re-insert it in some other identity providers, then the whole CC system is compromised. In this way, they also could log in, and potentially make purchases, using that person's account.

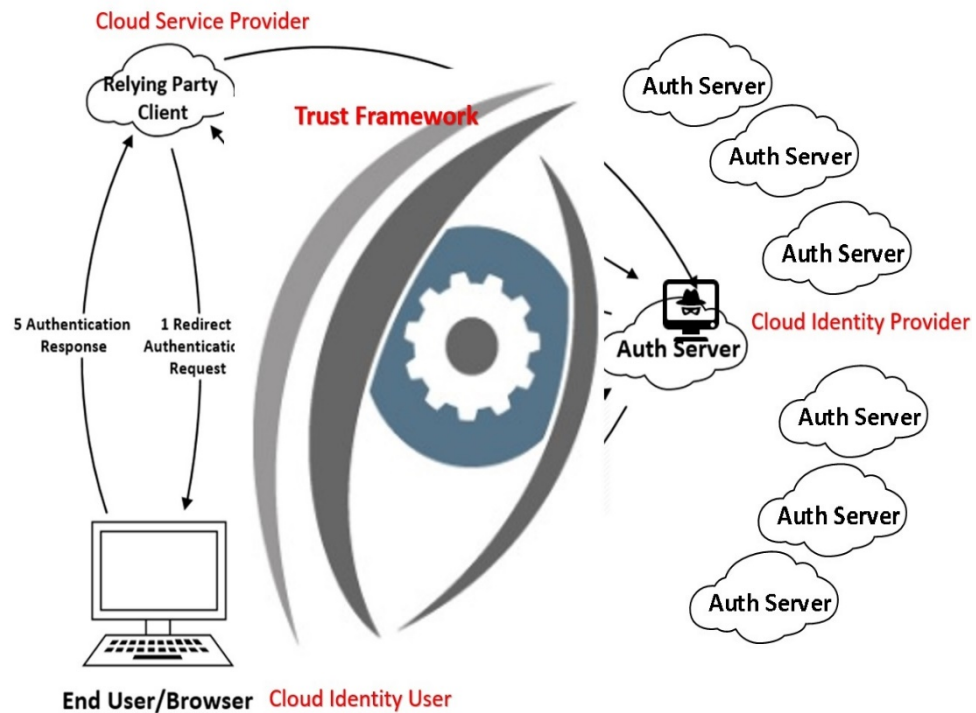


Figure 3.2: Proposed trust framework

Therefore, these issues addressed are leading to build a framework for evaluating and ranking the trust level of CIdPs to be used between cloud identity customers (CIdUs and CSPs) and identity providers (CIdPs). Figure 3.2 shows the general view of the thesis proposed model. Although, evaluating trust level of CIdPs is not a straightforward process; several framework's sub-issues require to be identified for evaluating and ranking the trust level of them, and it is addressed in the next

chapter because, without sufficient evaluation of trust criteria, the trust level will fail to identify and correct the threats or risks that might happen with CIdPs. Additionally, providing insufficient trust evaluation criteria, an accurate trust level of CIdPs cannot be obtained. Therefore, this trust framework needs to identify a number of trust evaluation criteria to ensure that they cover valuable identity assets and offer the maximum level of trustworthiness. Moreover, this trust framework should (features of the framework and the proposed model):

- Deal with many possible layers of access control.
- Associate with user authentication and access control lifecycle.
- Provide a trust level for numerous users from different organisations with different access control policies.
- Improve decision-making process to retain control over users' identity.
- Help Cloud user directly, without involving IT experts.

Furthermore, because of the criticality of many identity services and their complicated tasks, some CIdUs cannot make decisions based solely on web-based reputation scores. So, the decision needs to be based on numerous trust mechanisms, which are more certain, more accountable, and more dependable.

3.3 THE RESEARCH QUESTION AND HYPOTHESES

The thesis research questions are based on the systematic literature review. So, the proposed study aims to answer these questions, which have been labelled Q1, Q2, and Q3:

Q1: With respect to the Essential System Attributes (ESA) and Essential System Characteristics (ESC), how are the trusted-based relationship between CIdP and CIdU framed?

El-Najdawi and Stylianou (1993) identified that to qualify any research problem there is a need for quantifiable dimensions (ESA and ESC) which provide criteria for evaluation. The Cloud identity environment has certain unique characteristics (criteria) and uses techniques (trust framework) that have raised several new (alternative) solution trust frameworks and the need to re-evaluate and redefine many well-defined past trust frameworks. The mechanism of framing different attributes, characteristics, assessments, certifications, and evidence like performance, security, and privacy trust judgment could be complex, due to a

possibly large set of elements (ESA and ESC) to consider and a possibly long chain of trust relations. To answer this question, best practice trust framework and trust benchmarking have been reviewed, and the result is verifying in the work of this thesis.

Q2: How is an evaluation done of the trust establishment framework from question one?

This question is based on the “you cannot control what you cannot measure” (Hillary & Madsen, 2002, p.1). Therefore, for controlling trust the essential part is measuring, consequently, for the measuring, the crucial part is defining attributes and characteristics to be measured. Moreover, the Management Information System (MIS) provides analysis for essential elements for the organisation by adopting the mathematical model to better understand the issues (Sprague Jr, 1980). There are ad-hoc approaches to support the consumers in selecting trustworthy services such as SLA, Auditing, Measuring and Rating, and Self-Assessment but still because of the new features of cloud and cloud identity, they need new measurement methods.

Q3: How might the framework from question one by using the evaluation method of question two affect the decision making of CIdUs and CIdPs?

El-Najdawi and Stylianou (1993) identified that the structure of the evaluation method should be defined by the system users (decision makers). Moreover, it is better to use the reflection of the users (decision makers) to improve the existing framework and adequacy of measurement. However, informed decision making is important to manage the user’s assets (Information, Identity, and Infrastructure). Power et al. (2015) defined that decision making is based on the statistics and scientific studies and not only based on personal judgments, intuition, and ingenuity. Therefore, statistics and scientific processes should use correct data resources to better understand the organisation requirement. Khodashahri and Sarabi (2013) categorised three types of decision makers which are Independent, Sequential dependence, and Convergent dependence, and in this thesis, all three types are considered. Furthermore, the trust elements and characteristics of CSPs need to be verified before use for decision-making. However, it is expected assertions from independent professional users will also be valuable. The primary goal of the trust framework is to provide decision makers (CIdUs and CSCs) with

trust-related information and as complete as possible. Therefore, to answer this question, the feedback of the decision makers could help this thesis to verify, improve, and update the proposed trust framework. Moreover, it can help develop innovative solutions to challenges such as identification, privacy, personalisation, integration, security, and scalability as long as it helps decision makers to make the best decision regarding the security, privacy, Quality of Protection (QoP), and QoS concerns.

Chapter two presented the common cloud identity security, privacy, and trust issues. The following hypotheses speculate the answers to the previous questions. Based on theory (Haber, 2006) they are considered a method to validate (test) methods which are theoretical (section 3.2). Three hypotheses were developed to be evaluated and tested in the following of this thesis; these hypotheses are assertions derived from the literature reviewed in chapter two. To sum up, the three hypotheses are labelled H1 to H3 as follows:

H1: A CIdUs' choice of CIdPs is going to be based largely on security, risk, and reputation.

H2: The modelling of a trust establishment in cloud identity needs to incorporate the ESA and ESC in order to produce a measurable trust relationship.

H3: The cloud identity trust framework facilitates trust making decision by cloud consumers.

Research questions and Hypotheses are the two main parts of any thesis and scholarly research, and these two pillars are the basis for this thesis. Obviously, these research questions and hypotheses were developed based on the literature reviewed in the chapters two and analysis in section 3.1, and section 3.2.

3.4 TRUST SYSTEM METHODOLOGY

Design Science (DS) is an organising framework and philosophy for making and building artefacts (Fournaris & Keramidas, 2014). It has been made relevant to Information Systems (IS) research as a methodology and in this research is applied to IS security. The benefit of the approach is that an artefact may be investigated in context and the artefact improved through continuous iterations and testing (Offermann et al., 2009). The purpose of the DS Research Methodology (DSRM) is not only to develop an artefact but also to answer research questions. Moreover,

Depending on the characteristics and the goals of the research, a researcher can shape the processes to deliver innovative or confirmatory outcomes (Johannesson & Perjons, 2014a). In this thesis, the DSRM (Offermann et al., 2009), Trust and Reputation system (Hoffman et al., 2009), Reputation system (Y. L. Sun and Y. Liu, 2012), and DeSPoT trust system (Håvaldsrud et al., 2012) have been adopted to design a suitable research methodology as shown in figure 3.3.

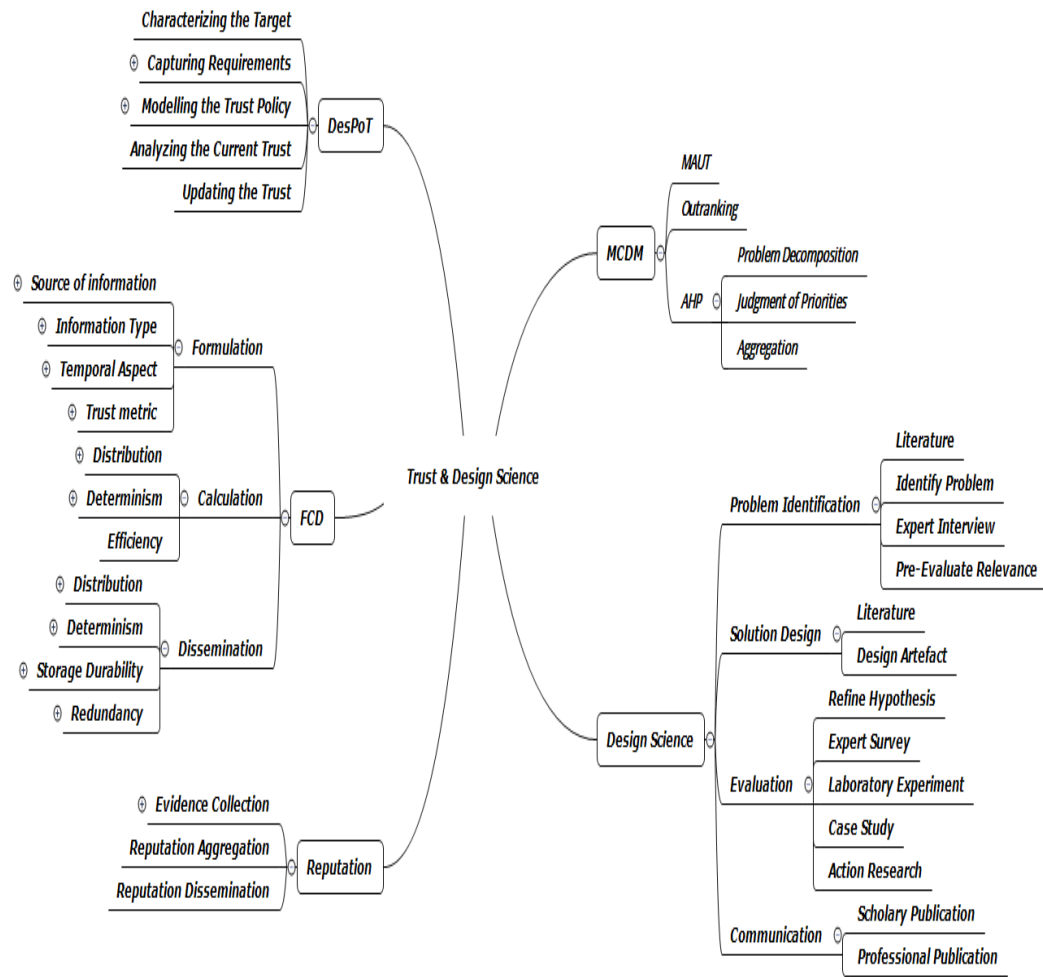


Figure 3.3. Summary of adopted methodologies (Håvaldsrud et al., 2012; Hoffman et al., 2009; Offermann et al., 2009; Sun & Y. Liu, 2012).

Development and Specification of Policies for Trust (DeSPoT) negotiation is a method for the trusting behaviour which tries to realise opportunities while keeping risks at an acceptable level (Håvaldsrud et al., 2012). The five-step process of the trust domain internally is a vital part of this method trust build for any provider. The overview of the five steps of the DeSPoT process is given in figure 3.3. This method is independent of specific trust negotiation protocols and does not assume such protocols to be predefined.

The overarching goal of a trust and reputation system (Hoffman et al., 2009) is to produce a metric that encapsulates the reputation for a given domain for each identity within the system. This model is based on Formulation, Calculation, and Dissemination (FCD) of trust attributes which have been received from numerous types of sources. Therefore, based on the input, a valuable reputation is calculated by using the validating algorithm. Once calculated, reputation metric values are then disseminated throughout the system in advance or on demand as the metric values are requested. Finally, higher-level systems or users can then utilise these reputation metric values in their decision-making processes for penalties or rewards in order to achieve the goals of the user application. Figure 3.3 presents the general structure of a trust and reputation system, including the location of each of the fundamental dimensions and demonstrates how each dimension of the trust and reputation system can be comprised of different components.

Reputation system (Y. L. Sun & Y. Liu, 2012) collects evidence about the properties of individual objects, analyses and aggregates the evidence and disseminates the aggregated results as reputation scores. From the defence points of view, the first step is to control how much extra information to release and when to release it, setting barriers for attackers gaining knowledge that facilitates advanced attacks while not affecting the experiences of users. The second step is to encourage honest feedback in the evidence collection phase through various incentive mechanisms. The third step is to design an attack resistant evidence aggregation algorithm, which can detect the presence of dishonest feedback.

Multiple Criteria Decision Making (MCDM) means the complexity of ranking the CC provider with many Key Performance Indicators (KPI), many attributes, and sub-attributes. However, Outranking, Analytic Hierarchy Process (AHP), and Multiple Attribute Utility Theory (MAUT) are three important approaches to solving MCDM problems (Garg et al., 2013).

AHP as an MCDM selected method for this thesis and is an approach that reduces the complexity of the decision making by positioning the deciding factors in a hierarchical structure. It is based on pairwise comparisons of main decision elements which allows the decision maker to identify the weaknesses and strengths between criteria. This method based on the (Saaty, 2005) research is flexible and also able to check inconsistencies which is important for this research in chapter six.

The authors of (Offermann et al., 2009) explained that “problem identification”, “solution design” and “evaluation” are three phases of the DSRM. These three phases can interact with each other within the research process. However, each phase is divided into steps and sequentially; also, they refer back to each other. In the first phase of the DSRM, a problem is identified. Next, the solution is designed. Once the solution reaches a sufficient state, its evaluation can be started. Thirdly, in the communication step, the below questions might be answered:

- How to establish the process and move forward?
- How to balance between action and reflection and how to enable equal participation?

The consequence is that evaluation balances any action that is taken, and the outcome of the evaluation can deliver forward broadcast to the next phase or a return to an earlier phase for improvement. Moreover, developed DSRM (Peffer et al., 2007) as shown in figure 3.4 is based on the (Hevner et al., 2004) research methodology. This figure shows the nominal process stages and points of iteration improvement.

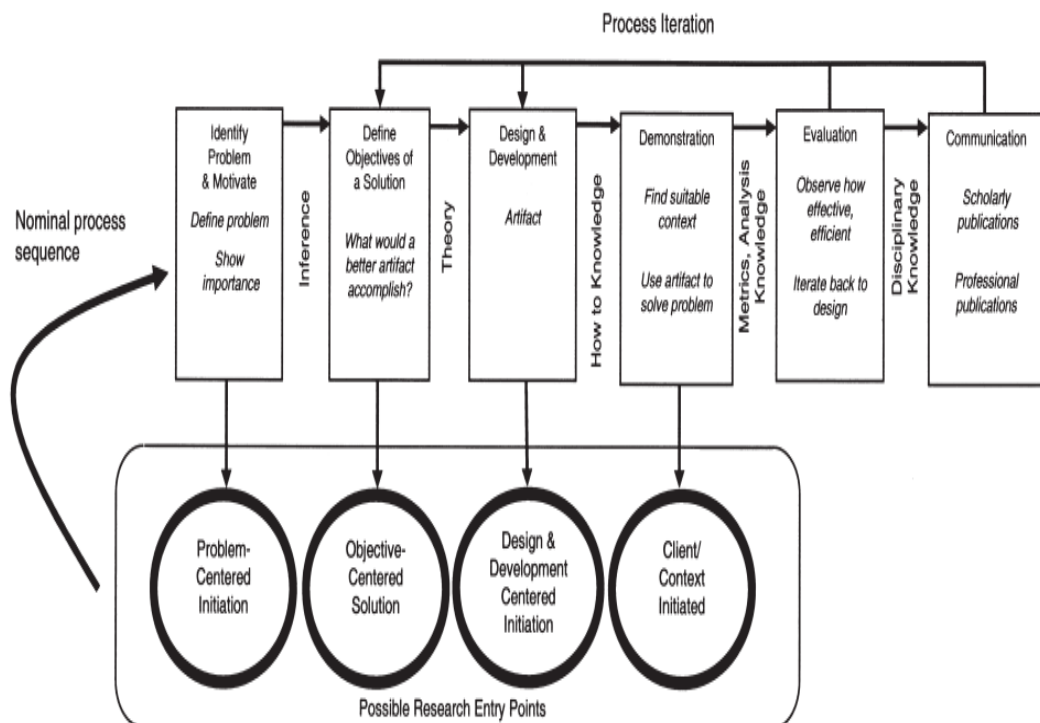


Figure 3.4. DSRM process model (Peffer et al., 2007, p.54).

To sum up, this research is based on the integration of the above trust and design science methodologies which has been shown in figure 3.5 and has been named

Trust Design Science Research Methodology (TDSRM) (Ghazizadeh & Cusack, 2016c). The process of TDSRM is structured into four main phases: problem decomposition, solution design, evaluation and communication. DSRM is chosen for this study because it is solution oriented and not problem-oriented and focuses on the creation and refinement of the artefact to get a good quality solution. As mentioned before, in the course of establishing trust towards CIdPs, the CIdUs are faced with some challenges. The purpose of the TDSRM is first to identify these challenges, answer research questions, and test the hypothesis which has been mentioned in the research question and hypothesis section.

3.4.1 Methodology/Research Methods

Trust computing, especially in the identity environment, has a multifaceted nature, and therefore, it needs multi-disciplinary skills and capabilities. Thus, this study employs a mixed research methodology as the methodology to address these issues and guide the research. Since this study is aimed to yield a new trust framework for the cloud identity area, this mixed methodology (TDSRM) is a suitable research methodology because the DS along with the problem statement the important part is how to produce a new solution. Also, the solution emphasis is on the evaluation method and the necessities for validating the research results (Alturki et al., 2013). An overview of the TDSRM phases and steps is given in figure 3.5.

TDSRM is a search process to realise an effective solution to a problem. The design of this study is based on the four steps that were chosen to guide the research. The design (figure 3.5) shows the three major processes of the research in the problem identification are capturing requirements, literature, and evidence collection.

Consequently, developing an artefact, which is a trust framework for cloud identity environment, is the next step of the TDSRM. The implementation of the artefact is used to demonstrate the artefact and evaluate the proposed solution. An iterative feature is implemented within the “processes” section of the design of this study to apply the result of the evaluation or even the second literature review to evaluate and enhance the artefact. The final part of the TDSRM is designed to include the development of the outputs for this study. These are the professional papers and dissemination of the result of the study to the CIdUs.

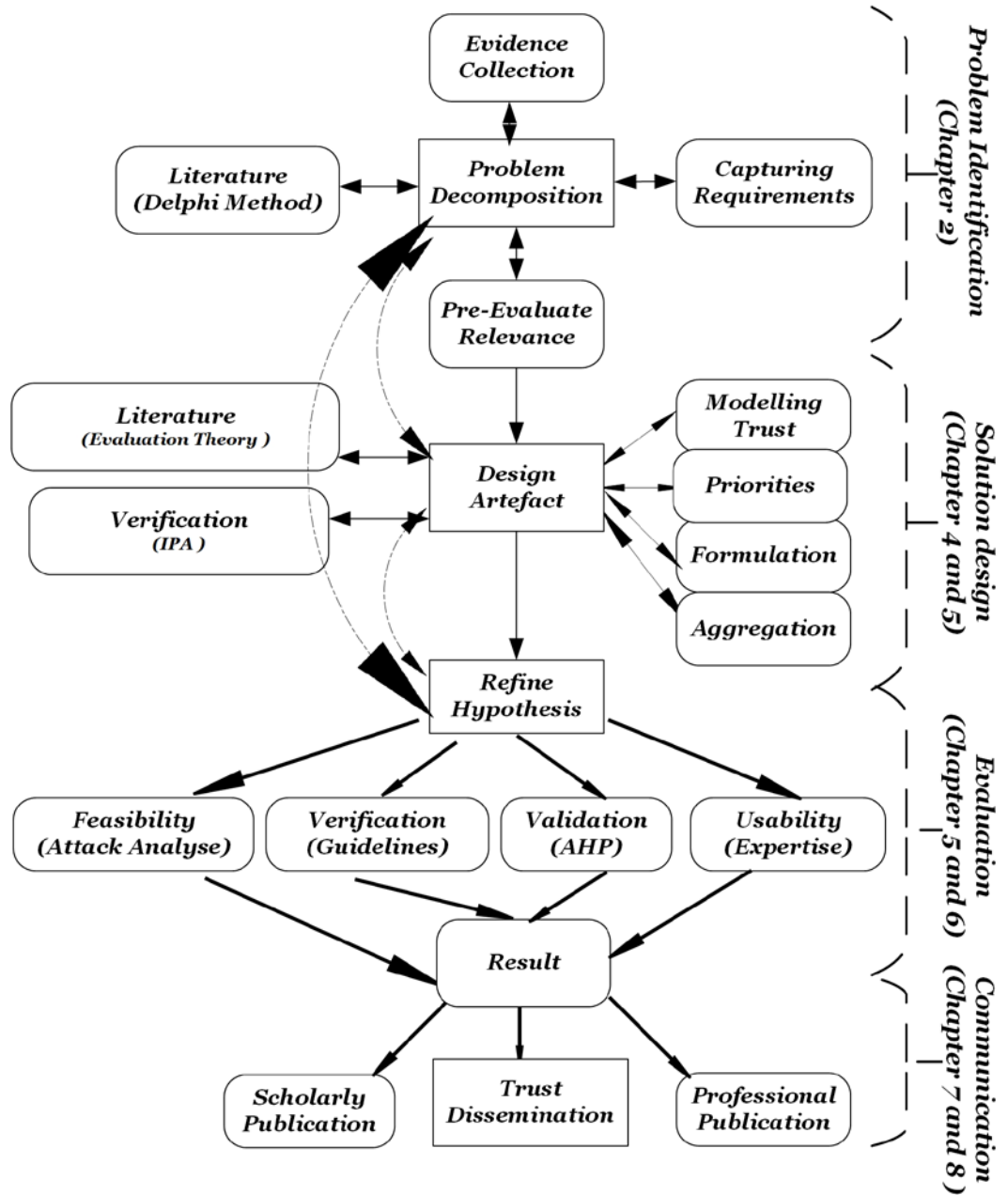


Figure 3.5: Trust design science research methodology (TDSRM)

3.4.2 Method Application in Brief

The design and development of the TDSRM concerns the support the CIdUs in reliably identifying trustworthy CIdPs. This system provides means to identify the trustworthy CIdPs regarding different attributes assessed by multiple sources and roots of trust information. The scope of research is narrowed to cloud identity standards with respect to CSPs, which has been mentioned in the cloud identity section.

An overview of the TDSRM phases and steps is given in figure 3.5. Each phase is divided into steps, and the arrows indicate a transition from one step to another. The application of the methodology is elaborated by following and responding to each requirement starting with problem identification. The following subsections elaborate the application of the methodology to the trust problem of cloud identity management.

3.4.2.1 Problem Identification

The problem identification required input from the literature review and the requirements assessment. It is often termed the first entry point for research. According to the methodology, the first entry point has been completed for the thesis as the literature has been reviewed and analysed. The result is a problem and a gap identified for study.

However, this step aims to identify the ESA of trust establishment between CSPs, CSCs and ESC of published trust establishment method between CIdPs and CIdUs. An in-depth analysis of various CSPs has showed that most of the systems do not offer support for all ESAs. However, Risk, authentication, network-based security, computational based security, accuracy, integration, privacy, traditional trust solution, QoP, QoS, dynamic, custom algorithm, high-level monitoring, low-level monitoring, SLA, attack resistance, and CSCs' feedback are ESAs for CSPs based on the critical literature. Therefore, CFIAMs assume that trust relationships are well-known, so, they usually need the CIdU's attributes to be asserted by a reliable entity.

Moreover, based on the literature these ESCs are balancing, SSO, life cycle, privacy, risk, and standards which will be exploring in chapter four. This identifies a problem for end users who must find a way of assessing CIdPs and make a rational trust decision.

3.4.2.2 Solution Design and Design Artefact

In contrast to the literature used in the previous sub-sector, the focus of this section is to find a solution for a trust cloud identity environment and design a usable artefact for this area. The design artefact aims to answer the question three which is: "how is a trust-based decision framework built?". The resultant artefact is the Cloud Identity Trust Unified Evaluation Framework (CITUEF) (figure 3.6) that includes: CIdPs, CSPs, ESAs, ESCs, and CIdUs (objects).

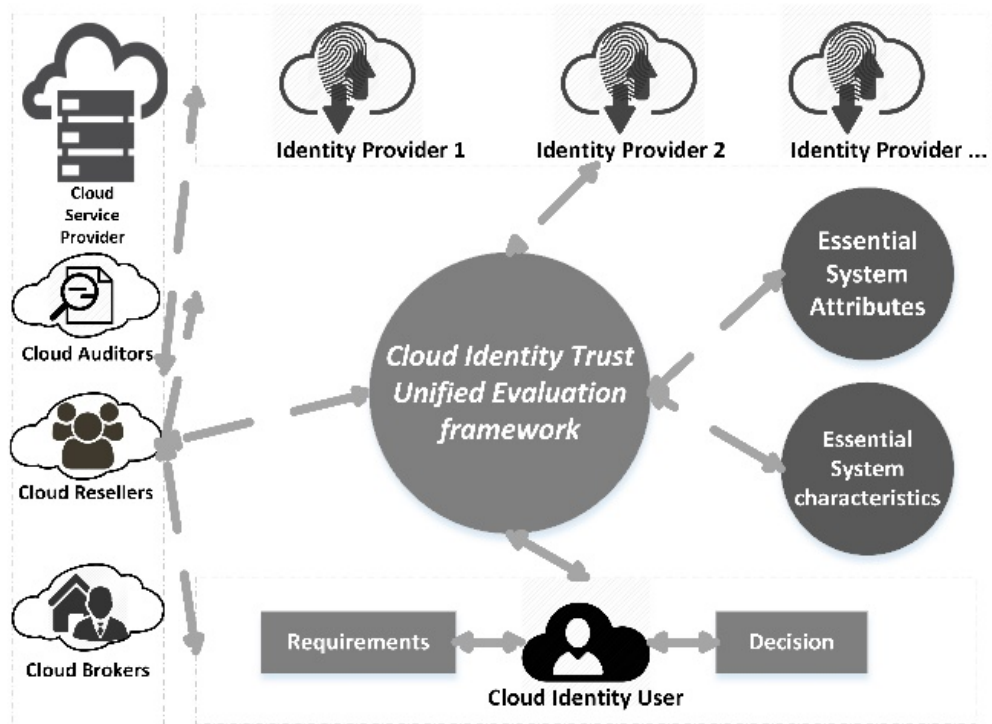


Figure 3.6: Cloud identity trust unified evaluation framework

The CITUEF manages and aggregates most trust-related information from different sources (CIdPs, CSPs, ESAs, ESCs and CIdUs); which are often available and relevant when assessing the trustworthiness of an CIdPs based on the object-oriented concept. This structure is based on existing work and presented in the literature that helps the CIdUs to find the particular trust model that fulfils users' requirements. The main objective in this section is to provide novel concepts and mechanisms for trust establishment in a cloud identity environment. The trust model incorporates various security challenges and is used to evaluate the security weaknesses and strengths of the CIdPs. Modelling trust framework, priorities of attributes and characteristics, formulation and aggregation of these attributes and characteristics are four sub-steps for building a trust framework.

However, one input into the design artefact is the modelling of trust. The first task is to specify the attribute description and attribute value. A trust formation rule defines what may form evidence and how this evidence should influence the target's trust level with respect to the CIdPs. The attributes are received from CIdPs and CIdUs and can be anything that may give insight into this vendor's capability. Next, in priorities of attributes and characteristics, because of rational make decisions across the boundaries of different attributes and characteristics based on the critical analysis priorities by synthesis. Consequently, the formulation is the

mathematical method which specifies how the available information should be transformed into a reasonable, understandable and usable metric.

Moreover, the specification may be made through a clear equation, or implicitly through describing an algorithm that will result in the correct values. Trust aggregation and calculation as a fourth input, calculates the reputation scores of CIdPs based on the collected evidence. This sub-set aims to be able to compute trust scores that accurately describe the quality of CIdPs.

Logical Argument	An argument with face validity.
Expert Evaluation	Assessment of an artifact by one or more experts (e.g., Delphi study).
Technical Experiment	A performance evaluation of an algorithm implementation using real-world data, synthetic data, or no data, designed to evaluate the technical performance, rather than its performance in relation to the real world.
Subject-based Experiment	A test involving subjects to evaluate whether an assertion is true.
Action Research	Use of an artifact in a real-world situation as part of a research intervention, evaluating its effect on the real-world situation.
Prototype	Implementation of an artifact aimed at demonstrating the utility or suitability of the artifact.
Case Study	Application of an artifact to a real-world situation, evaluating its effect on the real-world situation.
Illustrative Scenario	Application of an artifact to a synthetic or real-world situation aimed at illustrating suitability or utility of the artifact.

Figure 3.7: Evaluation method types (Peffer et al., 2012, p. 402)

3.4.2.3 Evaluation

Evaluation is the most crucial part of any research especially in the complex environment such as cloud and cloud identity. Therefore, it is important to evaluate the cloud provider's trustworthiness, by considering the knowledge on the architecture of the systems and the trustworthiness of its components and subsystems. According to (Offermann et al., 2009) when solution artefacts reach the acceptable level, it should be evaluated against research defined criteria. Offermann et al. (2009) identified that case study, action research, surveying expert, laboratory experiment, functionality, consistency, accuracy, performance, accessibility, and completeness are examples for evaluation methods.

(Peffers et al., 2012) classified evaluation method as shown in figure 3.7 prototypes, illustrative scenarios, case studies, and action research. They identified that prototypes are the implementation of artefacts to demonstrate artefact utility; illustrative scenarios apply the artefact in a synthetic or real-world situation to demonstrate its utility; and case studies implement the artefact in a real-world situation to evaluate not only its utility but also its effect on its environment; action research also implements the artefact in a real-world situation to evaluate its effect on the environment, but does that in the context of a research intervention. Logical arguments and expert evaluations are also part of the evaluation method classifications.

Moreover, based on (Alturki et al., 2013) advice, to ensure the quality of the artefact external and internal evaluation have been adopted. Evaluation is the third phase of the TDSRM; this involves observing and evaluating the proposed trust framework for answering the question and validating the proposed trust elements. In this phase, the evaluation and observation results are compared with the objectives of a solution (criteria). It is possible to iterate back to design for the artefact or even identify the problem if necessary and bring quality improvement.

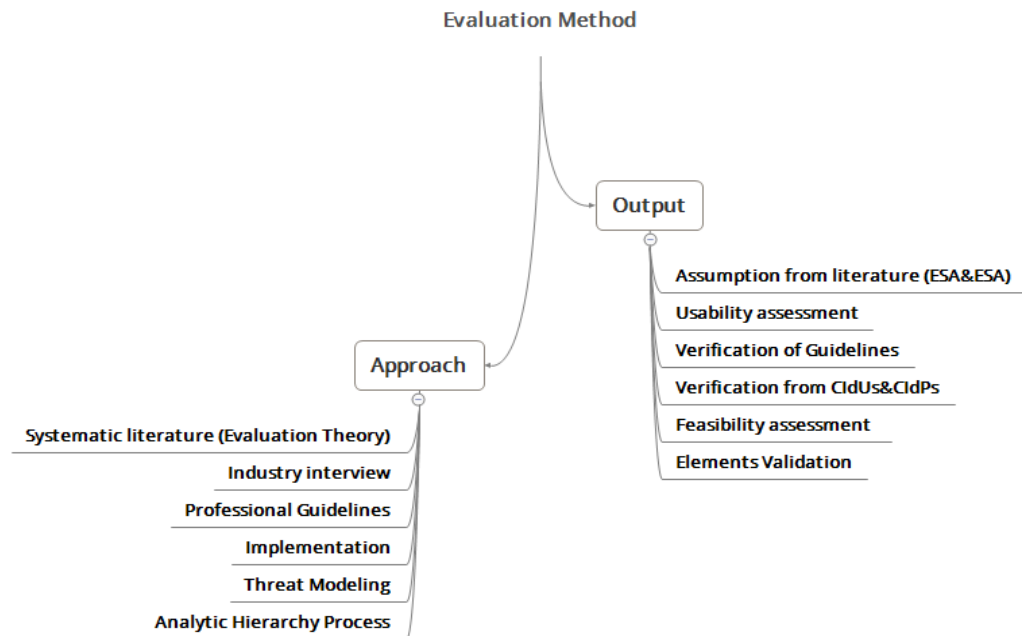
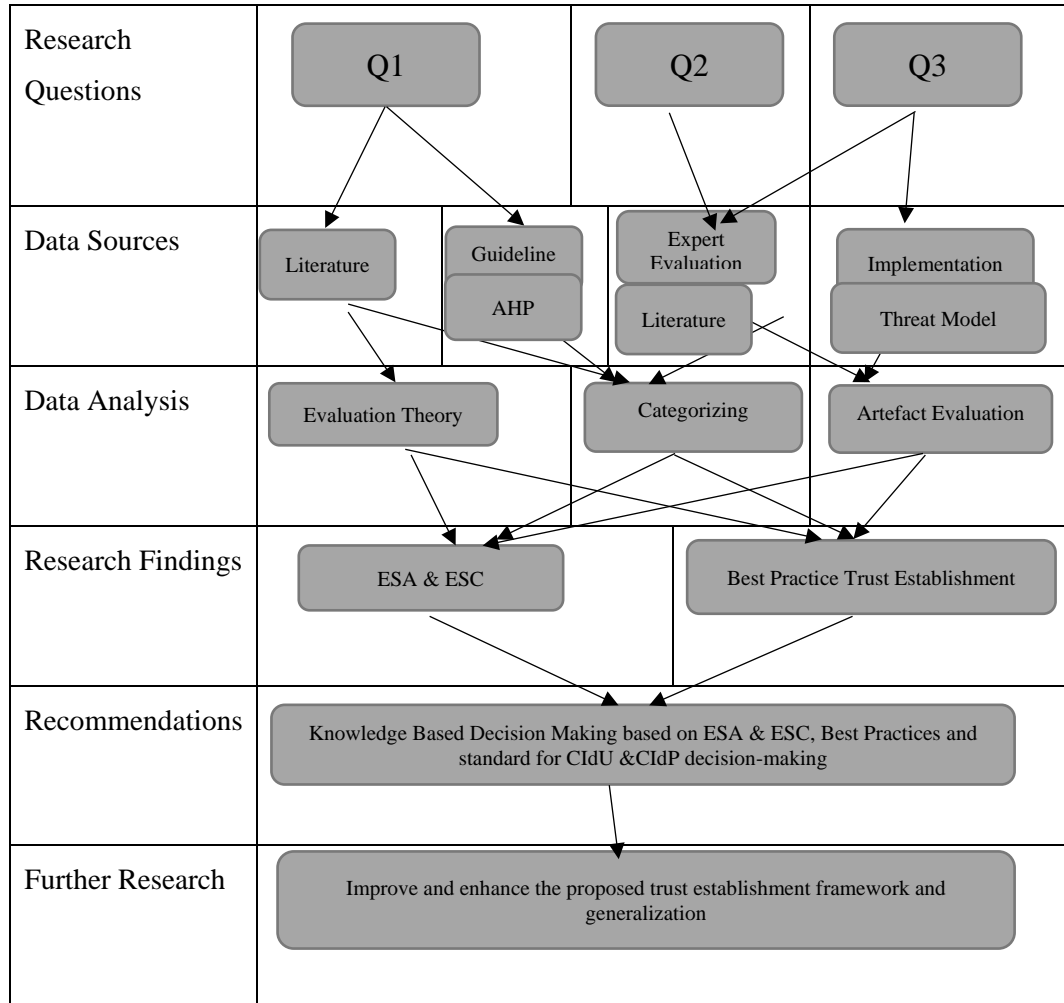


Figure 3.8: Evaluation inputs and approaches

Based on the DS definition, data are required for the evaluation step. However, at this point, the system has both the trust and its requirements. In the evaluation, it looks for possible gaps, exceptions and errors.

Table 3.1: The research data plan



Once the solution reaches a sufficient state, its evaluation can be started. Every trust formation rule forms trust based on attributes and characteristics with a specific value. It can, therefore, be easily checked against the corresponding trust formation rule requirement which specifies the highest acceptable trust to be formed. Hypotheses are related to the artefact properties and based on the DSRM (Offermann et al., 2009), The refined hypotheses should be mutually exclusive and collectively exhaustive about the general hypothesis. It means if all refined hypotheses are supported, the general hypothesis should be supported as well otherwise detect the deviation between evaluation finding and artefact. In this research rather than ‘proof of concept’ it evaluates the proposed artefact from the functional perspective. The general hypothesis makes a trustworthiness framework to evaluate CIdPs if they provide an identity for the cloud by using FIM services regarding the domains. For the evaluation, in this research, the general hypothesis

is split into smaller hypotheses that were simpler to evaluate and has been mentioned in section 3.3.

Adequacy for the cloud is one of the main problems when looking at any new model to adopt for the cloud. *Does the proposed trust model cover all the aspects of security relevant to CIdPs?* However, Data collection which is one of the hardest parts (Yin, 1984) in this research is based on the interview, implementation, literature, and guidelines. The evaluation is to be achieved by means of a literature review, expert interview, implementation, threat modelling, elements verification, and professional guidelines (Table 3.1 and figure 3.8). The inputs for these evaluation methods are an assumption from literature, usability assessment, verification from CIdPs and CIdUs, feasibility assessment, and verification from guidelines, which shown in figure 3.8.

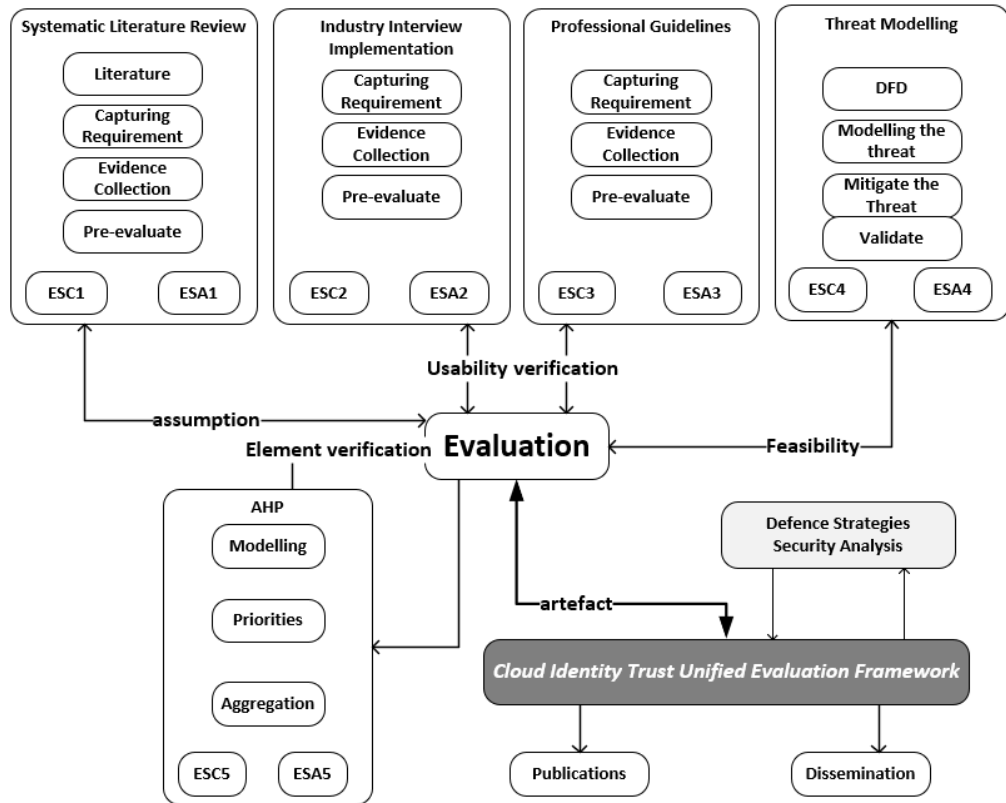


Figure 3.9: The workflow of the TDSRM.

Expert and academic feedback after implementation is one of the main data inputs for this research. Systematically, the assumption from literature, usability assessment, verification from guidelines, verification from real cloud users, feasibility assessment, and element validation are main methods to gather data to evaluate the artefact for this thesis. However, systematic literature analysis by adopting evaluation theory, industry interview, cloud identity professional

guidelines, implementation, threat modelling, and AHP as shown in figure 3.8 are the evaluation methods used for this thesis. Furthermore, based on figure 3.9, which shows the workflow of the methodology, literature and industry interview contribute to the understanding trust of CSPs and CIdPs by providing a review of their essential attributes and characterises. Since there are no deterministic factors affecting and measuring the cloud identity trust based on the literature, the appropriate method is chosen to be interviewing with industry experts that have familiarity with cloud identity to test the hypotheses. Expert people as the main CIdUs contribute to the result of the research by giving their feedback and prioritising the trust elements and trust frameworks. Three main guidelines for the cloud identity area aid this research to identify the result of the trust elements. Moreover, threat modelling assists this thesis to validate the feasibility of the proposed framework. So, in the following section, these methods and their details are identified by explaining the rationale between the proposed framework and their granular techniques.

3.5 SYSTEMATIC LITERATURE

To test the first and second hypothesis, critical literature is used. A critical analysis tries to make an argument about extending cloud trust evaluation to the cloud identity attributes to improve the level of trust between CIdPs and CIdUs. A comprehensive analysis and evaluation have been carried out on the trust management systems implemented in the CC (Chapter four based on the evaluation theory). The trust management systems proposed for the CC have been extensively studied with respect to their capability and applicability. However, there are several trust models proposed for the cloud; but, they have not been used or tested in cloud identity environments by the researcher. Hence the suitability of these frameworks for use in the CC cannot be recommended without an extensive evaluation. The researcher aims to use the proposed framework to measure the security strength of cloud identity services and applications. Therefore, to improve the result of chapter four, IPA identified the most relevant element to be measured for this thesis. As a result, this section tests both hypotheses one and two by identifying the security, trust, and reputation elements; with relevant ESA and ESC to measure the trust elements.

3.6 IMPLEMENTATION AND USABILITY CHECKING

To test the third hypothesis, the aim is to ensure applicability in practice as well as to improve the method's quality by including solutions to problems encountered in the trust and reputation. The implemented realisation of the trust management system is developed to assess the assertions of the framework that will evaluate CIdPs based on the ESA and ESCs.

Additionally, implementation of the trust model requires first preparing a test bed that the researcher has chosen from the Amazon Web Services (AWS) portal. To prepare the test bed, the first step is toward research implementation. Various tools are used as a part of implementation to check usability. The proposed method provides a graphical interface for measuring trust elements as well as showing the level of CIdP's trust level. AWS, windows 2012 r2, opensource Content Management System (CMS), and an opensource database engine (MySQL) are used to build the website up and to run. Scalable, reliable, and secure global computing infrastructure with AWS virtual backbone are some of the advantages and motivation to use this portal for this thesis. However, the main objective is to quantify the measurement into a trustworthiness score with complementary numerical and graphical opinion representations.

Therefore, the researcher has to implement the proposed architecture of the Trust Evaluation Model and its overall workflow to calculate the trust level of CIdPs. This framework is based on clearly defined and simple measurement assumptions. Also, this high-level architecture is based on object-oriented architecture to deliver trust as a service for the CIdU. As a summary, figure 3.10 shows the conceptual structure of the novel trust model with the individual parameters elaborated and their relation to other CIdPs and consumers.

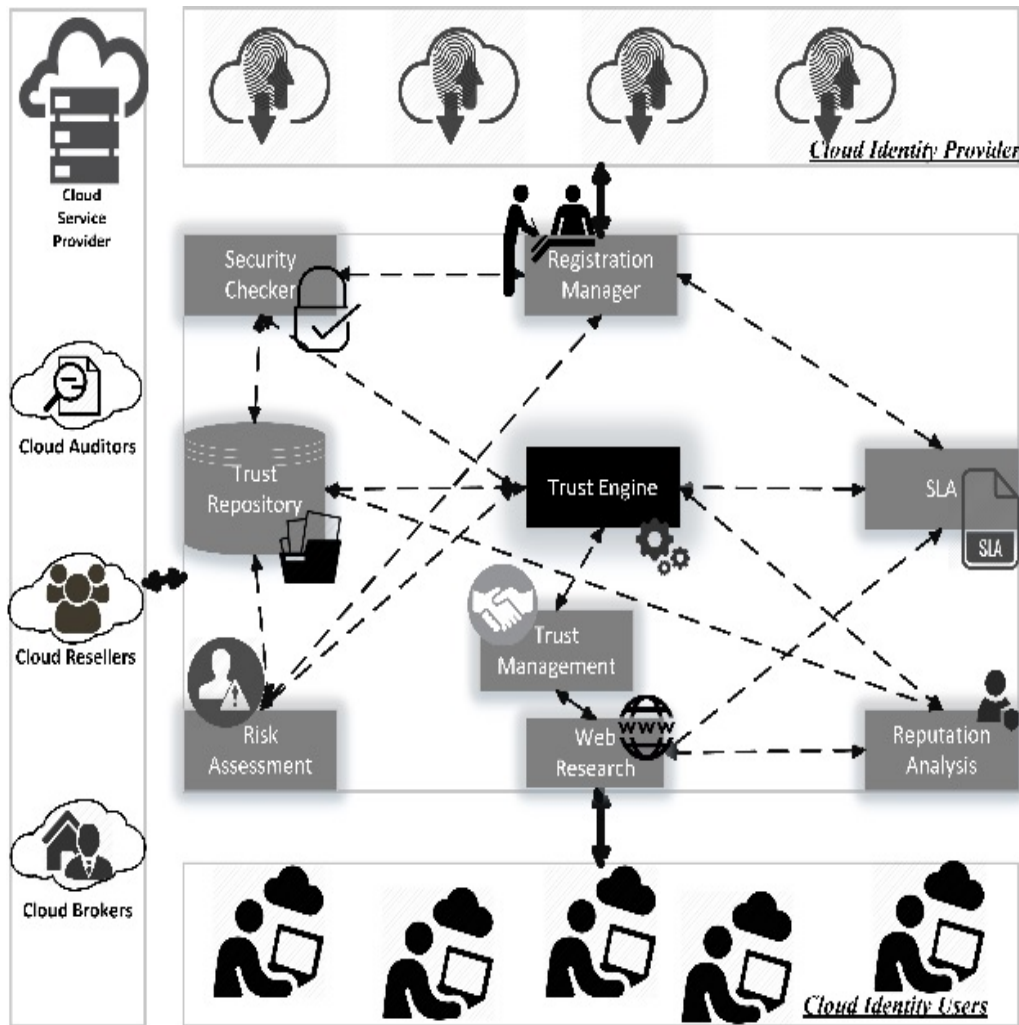


Figure 3.10: Architecture of the CIdP's trust framework

Moreover, figure 3.10 shows the design overview of a trust system, also, shows the location of each of the essential elements. The overarching goal of this framework is to produce a metric encapsulating trust for better decision making for each identified user within the cloud identity system. Therefore, as figure 3.10 shows, the trust framework receives input from various types of sources. Based on this input, a system produces a metric with a calculation algorithm. Once calculated, metric values are then disseminated throughout the system in advance or on demand as the service provider requests the metric values. Finally, higher-level systems or users can then utilise these metric trust values in their decision-making processes to achieve the goals of the assessing the risk of using an identity provider. The thesis found that the proposed method should include nine components, namely the security checker, Trust repository, Registration manager, Trust engine, SLA, Trust Management, Risk Assessment, Web Research, and Reputation Analysis.

3.7 EXPERT EVALUATION

This evaluation method is based on the DS phases (Peffer et al., 2012). The procedure is to evaluate the artefact and check validation (Alturki et al., 2013). Expert feedback from Cloud advisors, Cloud security advisors, Information Security consultants, and senior IT managers informs the research to evaluate and improve the artefact. Moreover, the characteristics and attributes validation by feedback in both interview and usability checking of the artefact, strengthens the validity of the thesis. These experts have enough knowledge and experience in both cloud and the cloud identity area to contribute credible opinion (Mantelaers, 1997). The background of the nominated experts (Based on their LinkedIn profiles) is checked and matched to the task. Mantelaers (1997) identified that expert opinion is like practical guidelines (Compare with professional guidelines). In the systematic literature, qualitative document analysis of major research in this area has been completed and subsequently, expert evaluation by interview is the validation and evaluation method to rate the trust measures identified in the systematic literature.

Five cloud identity experts are asked for interviews. They are provided with the artefact to use. The conversations are recorded and transcribed; consequently, coded and visualised in the table to better understand the feedback. The interviews are conducted as semi-structured interviews, which took between 25 and 60 minutes and consisted of two parts. In the first part, the interviewee is asked about ESA and ESC and about the role of trust for cloud identity. They are asked to rate the importance of ESA and ESC which has been found in the systematic literature. The rate and guidance of the expert assists to verify the trust elements by using the AHP method. In this regard, the cloud identity service selection is chosen as the application case. The case aims to evaluate how cloud identity customers prioritise trust elements affecting CIdPs selection. Moreover, a simple three-level hierarchical structure is the first step to gain insight into the end user method. Therefore, initially, the number of levels is determined, and the variables identified to check the consistency of the trust elements as well as validate the elements.

In the second part, in terms of usability, by using the table 3.2, it is discussed with the expert and the focus areas of trust identified in the qualitative document analysis. Usability is considered to be one of the most important quality factors for

the artefact, along with others such as reliability and security (Fernandez et al., 2011).

Table 3.2: Interview questions from trust elements and measurement

General	<p>Q1: What are the confronting issues regarding organisation when adopting cloud, cloud identity, and trust computing?</p> <p>Q2: What is the relative importance of these issues?</p>
Trust	<p>Q1: Between cloud provider and cloud consumer, what are the Essential System Attributes (ESA) of trust establishment?</p> <p>Q2: Between CIdPs and CIdUs, what are the Essential System Characteristics (ESC) of published trust establishment method?</p> <p>Q3: What are the weight of the trust elements?</p>
Trust Establishment	<p>Q1: How can trust attributes be measured?</p> <p>Q2: What measurement methods for trust are you using?</p> <p>Q3: What impact will trust framework have on future cloud identity management?</p>

Therefore, the working question is: “what usability evaluation methods have been employed by researchers to evaluate web artefacts, and how have these methods been used?” Particularly in this thesis, usability means benefits of the artefact for specified users (CIdU and CIdP) to achieve specific goals (Trust framework for cloud identity are) with customer satisfaction. In this view, usability implies the interaction of customers with the artefact implementation and can be seen as the capability to meet a customer’s expectation. Usability is one specific characteristic that affects the quality of a project.

Fernandez et al. (2011) classified usability assessment into two different types: inspection methods and empirical methods. Empirical method, which is used in this research, is based on capturing and analysing usage data from real end-customers (CIdP and CIdU). Prat et al. (2014) proposed a hierarchy of evaluation criteria for IS artefacts organized according to the dimensions of a system (goal, environment, structure, activity, and evolution), a model providing a high-level abstraction of evaluation methods, and finally, a set of generic evaluation methods which are instantiations of the model. Therefore, based on the usability definition

and evaluation criteria in table 3.3, the usability of the artefact is investigated by asking these questions of expert identity users.

Table 3.3: Question of artefact evaluation

No	Questions
1	How effective is the application in managing trust in the cloud?
2	How reliable is the trust level?
3	Is this application adequate?
4	How easily is this application used?
5	Is this application capable of including all required trust elements?
6	Can this application use the output of the other application (Monitoring, Benchmarking, SLA, Reputation, and computational)?
7	Will this application meet the customer expectations?
8	Do you find any usability issues with the application?
9	Is there any area for improvement?
10	Does this application provide enough detail and instruction for use?

3.8 DATA ANALYSIS

Analysing data gathered by qualitative interviews, guidelines, and literature involved shifting data, filtering out the significant information, identifying patterns, and constructing a framework for communicating the essence of what was found. Analysing qualitative data is often a vague time-consuming, and muddled process. Moreover, qualitative data is characterised by its comprehensive text-based information, richness, and subjectivity (Haley et al., 2017). Traditionally, researchers utilised coloured pens to analyse the categorised data. However, NVIVO, the qualitative data analysis software is the innovative software technology for analysing qualitative data in the user-friendly and simplifying method. Moreover, NVIVO by validating the input data can improve the rigour of

the analysis process. Therefore, the researcher is utilising the NVIVO software to analyse unstructured qualitative data (open-ended survey responses, articles, interviews, web content and social media) (Niedbalski & Ślęzak, 2017). NVIVO helps this thesis to organise and manage material and find insights in its data and analyse them based on the patterns and themes (Bazeley & Jackson, 2013; Welsh, 2002).

Qualitative data analysis is applied for this thesis (Edwards-Jones, 2014). As shown in figure 3.11, in the first step, all the guidelines are imported to the NVIVO. Next, the step is classifying the guidelines, which is classified based on the publishers. The third step is code and annotate. Exploring, coding, and annotating are three main processes in this step. After that in forth step, the query is used to gather attitudes based on the demographic attributes or to explore the connection between them. Creating a linked memo and analysing all the guidelines is the last step for this process. This section focuses on attributes and characteristics in all of the guidelines and seeks understanding of the relation from the perspective of CIdUs and CIdPs.

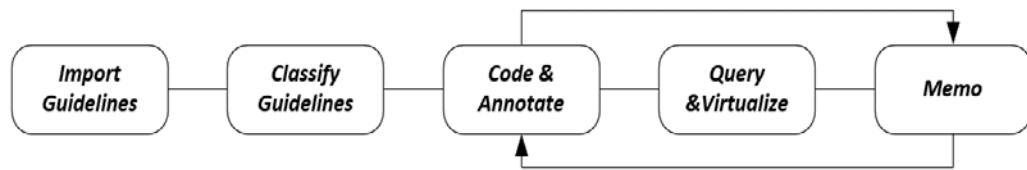


Figure 3.11: Guidelines review process

3.9 FEASIBILITY ASSESSMENT

STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege) threat modelling is used for identifying risks to architecture and design level of the artefact. However, in this method, hypothesising potential security threats, evaluating the threats, ranking the threats, and suggesting mitigation strategies are four steps which are considered important to execute. Therefore, based on the thesis assumptions, artefact evaluation and trust framework validity are the four activities (data flow, data store, processes, interactors) to be assessed. The justification table is a tool that assists the thesis to assess the feasibility of the proposed trust framework by analysing the rational between trust elements and threats.

3.10 COMMUNICATION

The final phase of TDSRM is known as Communication. In scholarly research, publications (contribution of the research) will use the deliverables of this research to inform conference or journal papers (as listed in the front of the thesis). This is to publicly communicate the trust problem and its importance, the trust framework artefact, its utility and novelty, the rigour of its design, and its effectiveness. To disseminate the trust level of the proposed framework for professional use and for secure methods, the SAML is adopting between providers and customers. On the other hand, once trust has been calculated by the framework, it should be accessible to all customers. Therefore, the calculated values of trust level and results must be effectively disseminated to other recipients or made available upon request. The responsibilities of the trust system fall within the dissemination dimension.

3.11 CONCLUSION

Chapter two has reviewed the theoretical and technical contexts of the CC, traditional and cloud identity management, and trust computing. Moreover, chapter two identified that there are still security issues and problems in the cloud identity area. Chapter three started with the analysing of the current issues and the current industry and academic questions in the thesis scope; and, the chapter has evaluated the methods for response to the problems. Research methodology is the heart of any thesis and figure 3.5 is the heart and guidelines of this chapter. Figure 3.5 is the pathway for whole thesis that is shown in the four main steps. Figure 3.5 is therefore the reference map for the methodological steps throughout the thesis.

In section 3.1 after systematic analysing it is shown that while there are studies that have focused on technological aspects of cloud, cloud identity, and trust, decision making to adopt and migrate to cloud solutions is under-reported and a problem for the cloud users. Consequently, customer questions in four main areas have been identified and analysed. The main advantage is to find the central concerns (questions). Hence, to answer these issues by proposing methods and solutions to mitigate the issues has been done. Section 3.2 after analysing one of the cloud identity management system (OpenID Connect, figure 3.1) proposed the solution as depicted in figure 3.2. Likewise, section 3.3 identified the research questions and hypotheses. Design science has the iteration steps to refine the hypothesis which will help the researcher to refine the hypotheses at any stage of

the research. Figure 3.3 shows granularly all methods which have been analysed for this thesis. Figure 3.6 is the proposed framework with all the relevant elements. Therefore, the methodology first compares and evaluates the proposed methods with current industry guidelines by utilising evaluation theory (chapter four), and then by evaluating and approval from real industry users as well as contemporary evaluation methods (chapter five and six).

Evaluation is the most crucial part of any research project especially in the complex environment such as cloud and cloud identity. Therefore, it is important to evaluate the cloud provider's trustworthiness, by considering knowledge of the architecture of the systems and the trustworthiness of its components and subsystems. In this regard, figure 3.8 depicted all the selected approaches to evaluate the thesis hypotheses as well as answer the research questions. Moreover, table 3.1 has shown the research data plan for this thesis and figure 3.9 the overall workflow of the trust design research methodology.

Overall this chapter has identified how to overcome the cloud identify trust issues by using the adopted methodology with novel techniques. Therefore, in chapter four, based on this methodology, the evaluation theory and IPA method to identify the ESA and ESC is justified. Chapter four is the first step to identify and evaluate the proposed method by comparing it with the latest cloud trust frameworks as well finding the essential system attributes and essential system characteristics of the thesis trust framework. Therefore, in chapter four, after analysing the latest and current trust frameworks, the IPA method is used to find the best trust element for the proposed trust framework to be used in the cloud identity environment.

Chapter Four

Evaluation Theory

4.0 INTRODUCTION

In chapter three, the methodology was specified and in the following chapters, including chapter 4, the plan is followed through to answer the research questions. As has been mentioned Figure 4.1 is the pathway for the thesis, and the highlighted part is the part which will be covered in this chapter. Therefore, this chapter will cover the literature, verification from the literature, design artefact, modelling of trust, priorities, and obviously refine the hypotheses.

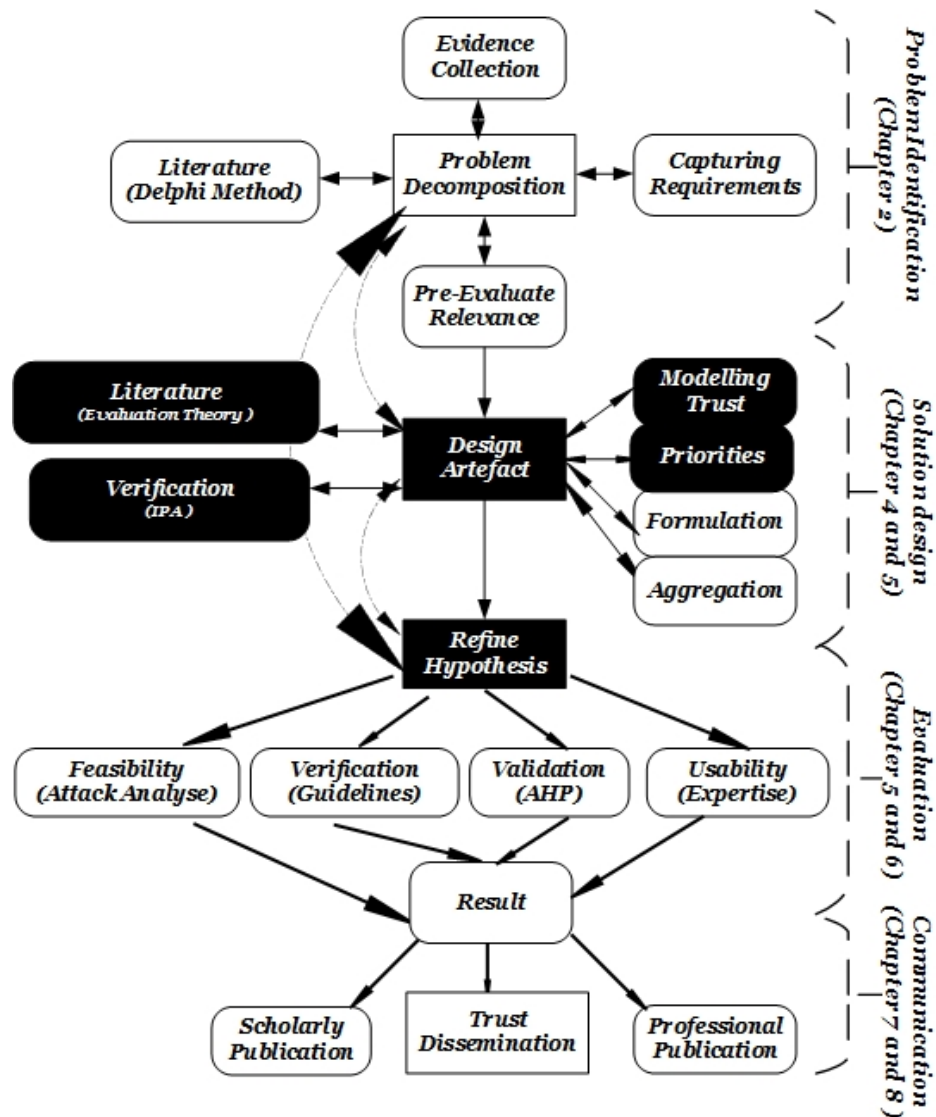


Figure 4.1: Chapter four pathway

The focus of chapter four is the design a solution. Therefore, in the first step, in this chapter will focus on adopting evaluation theory to identify the trust elements (ESA and ESC) and consequently prioritises them by using the IPA method.

In chapter three, the argument was that the trust model acts as a security strength evaluator and ranking service for the cloud and cloud identity applications and services. It also might be used as a benchmark to set up the cloud identity service security and to find the inadequacies and enhancements in cloud infrastructure. A framework is proposed that evaluates and assesses these trust concerns with respect to cloud identity services before selection in the cloud environment. Hence, the trust elements for measuring trust level of any CIdP are proposed. In this regard, evaluation system architecture and a critical literature review is adopted to answer two questions respectively:

- Between cloud provider and cloud consumer, what are the Essential System Attributes (ESA) of trust establishment?
- Between CIdPs and CIdUs, what are the Essential System Characteristics (ESC) of the published trust establishment method?

The following sections respectively review trust management, evaluation system architecture, evaluation criteria, an evaluation yardstick, data gathering methods, synthesis techniques, and evaluation processes based on the IPA method. These steps are aligning with the solution design steps. From the literature analysis the artefact is designed based on the current trust frameworks and past experience. Moreover, the framework synthesis and critical interpretive synthesis are two methods to prepare data for the evaluation process. The evaluation process is approached by doing the preparation process, the examination process, the decision-making process and prioritising the results of the trust modelling.

4.1 TRUST MANAGEMENT

Trust management had been established by Blaze et al. (1996) to deal with security issues of centralised systems. The aim of their system was overcoming the inflexibility of a complex trust relationship, and centralised control of trust relationships. Trust management has been considered by many researchers especially in the area of Peer to Peer, E-Commerce, Wireless Sensor Network, Grid Computing, and The CC (Calheiros et al., 2011). There are several trust definitions but, in this thesis, trust means the extent to which CIdU and Cloud Service Providers

(CSP) are willing to depend on a CIdPs and Cloud Service Customers (CSC) provisioning and de-provisioning their service and expect qualities that CIdPs promise are met.

Moreover, Trust management is the smart way to assess and establish a trusted relationship between CIdPs and CIdUs, and in this research, the focus is on the cloud identity customers' perspective. The recommendation, policy, reputation, and prediction are four basic trust management techniques which have been cited in (Noor et al., 2013) and are used in this thesis.

Recommendation: This method is a trust management technique that is common in the cloud area (Habib et al., 2012). The main reason for this technique is that feedback and customer's knowledge about the providers is a valuable trust element. Psychologically one idea influences another person's trust and impacts the perception factors that create a trusting environment. *Transitive recommendation and explicit recommendation* are two types of trust recommendation.

Policy: This method is one of the most popular trust management techniques to establish trust between customers and providers (Yao et al., 2010). In this method, the minimum threshold of trust is identified, and both parties are following the approved policy.

Reputation: In this technique the feedback of the consumers might influence positively or negatively the reputation of any CSPs (Noor & Sheng, 2011). Moreover, reputation can have an indirect or direct influence on the trustworthiness of a CSP (Al-Sharawneh & Williams, 2010). Unlike the recommendation method, reputation has no trusted relations in reputation systems, and customers do not know the source of the trust feedback. eBay, Amazon, Aliexpress, and Epinions are some examples of online reputation-based systems and review systems where the consumer's opinions and reviews on specific products or services are expressed.

Prediction: In this trust management technique there is no prior information regarding the CSP's interactions (Skopik et al., 2010). The basic idea behind prediction is that similar minded CSPs are more likely to trust each other. Noor and Sheng (2011) propose a similarity technique to determine credible feedback from the misleading ones. It can be used to refine the trust results and to increase the credibility of trust feedback.

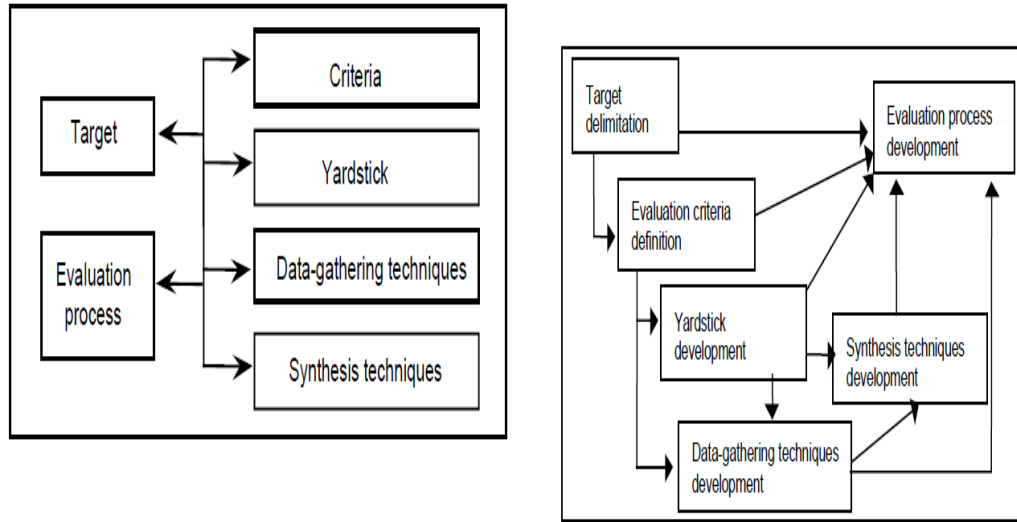


Figure 4.2: Components of an evaluation and their interrelations (Lopez, 2000, p. 6)

4.2 EVALUATION SYSTEM ARCHITECTURE

Evaluation is a key analytical process in all intellectual, disciplines, and service providers (Alabool & Mahmood, 2015). Also, it is possible to apply different types of evaluation methods to provide knowledge of the complexity and ubiquity of the cloud service providers. This chapter aims to obtain a set of basic evaluation components based on the (Lopez, 2000). Moreover, this chapter aims to propose a framework that can be used to develop trusted computing with the purpose of improving the previous trust methods. In particular, the evaluation system architecture method had been applied to review the trust establishment frameworks using the identification of the evaluation components and the analysis of their weaknesses and strengths. Therefore, the thesis seeks to highlight related works for trust frameworks developed based on trust theoretical and practical foundations. In this section, evaluation theory (Lopez, 2000) is considered as a theoretical foundation for developing a cloud identity trust framework and its processes are shown in figure 4.2.

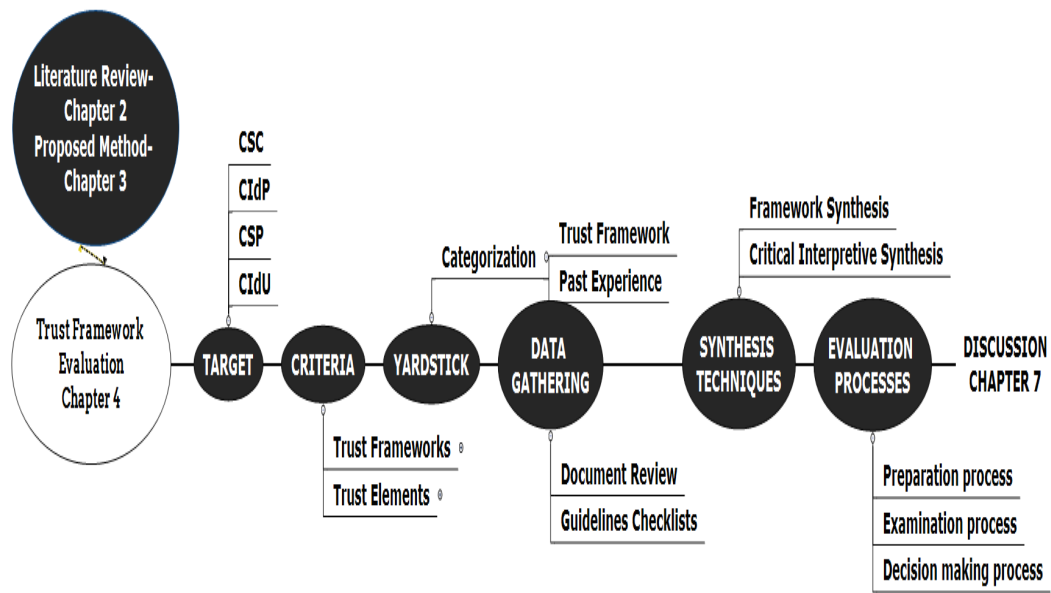


Figure 4.3: Cloud identity trust evaluation framework

Also, reaching a comprehensive and reliable trust level is the main reason to use an evaluation theory. Moreover, the method offers a clear and formal description of the evaluation' concept. Therefore, figure 4.3 shows the pathway for this chapter which has been adopted for this chapter and is discussed in the following sub-sections.

- **Target:** Trust between CIdPs and CIdUs
- **Criteria:** Trust elements of the CIdP and CSPs that are to be evaluated.
- **Yardstick or standard:** the ideal trust framework against which the current trust framework is to be compared.
- **Data-gathering techniques:** Critical or systematic literature review needed to obtain data to analyse each criterion.
- **Synthesis techniques:** These techniques are used to assess each criterion, therefore, to assess the target, obtaining the results of the evaluation.
- **Evaluation process:** It means a series of tasks and activities which are used to perform the evaluation.

4.3 THESIS TARGET

The first activity and step as shown in figure 4.3, is identifying and ascertaining the evaluation target. A target is the element under evaluation that provides information about what the element is and presents a general description of the objective

domains and functions. Therefore, the level of trust for CIdPs has been selected to be the object under evaluation. It has been chosen because CSPs have not yet adopted an all technical features of cloud identity and they require identity federation in order to provide not only SSO but also agile and secure access controls between internal and external services. To enable communications amongst CIdPs, CIdUs, CSPs, they must be able to establish trust with one another and exchange identity information. Therefore, cloud an identity trust framework has been developed to help CIdUs to make a good decision based on the trust elements.

4.4 EVALUATION CRITERIA

Criteria definition is the second critical and essential step for developing a cloud identity trust framework. To having ascertained and delimited the target (CIdP), it is essential to recognize what characteristics (trust elements) of the target (CIdP) are important for evaluation purposes. These characteristics are referred as evaluation criteria. Alabool and Mahmood (2015) specified the value in using as many criteria as possible to make better trust element coverage for evaluation. These criteria also can pertain to diverse sub-elements, and each sub-element can also be broken down into several elements. A critical literature review (overview of published materials) study has been completed to answer two questions.

- First, what is the current state of trust computing knowledge about these issues and problems (Looking for the methods and trust framework as shown in figure 4.3)?
- Second, what are the current trust computing elements in the theoretical or policy issues and debates related to trust, the CC, and cloud identity management systems (Looking for elements and cloud identity trust elements as shown in figure 4.4)?

4.4.1 Trust Framework

To answer for the first question, there was a need for a determine a module to communicate with CSCs effectively. Attributes of a CSPs are used as data to make trust assessment on their service or services, and those attributes need to be distributed in a trustworthy way. Hence, it had motivated (as a finding) the build of a hybrid model for trust management in cloud identity computing environments. Current approaches and existing trends in the field of trust establishment need to be

categorised in a knowledgeable and detailed way to identify and analyse the current cloud trust establishment method. In this regard, User Observation, Auditing and Risk Assessment, Self-assessment Questionnaires, Benchmarking and Monitoring, Service Level Agreement (SLA) Based Trust framework, and Computational Trust Framework have been systematically categorized as trust models on the basis of their diverse attributes and techniques for calculating the trust score as a source of evidence and figure 4.4 shows the selected categories for this thesis.

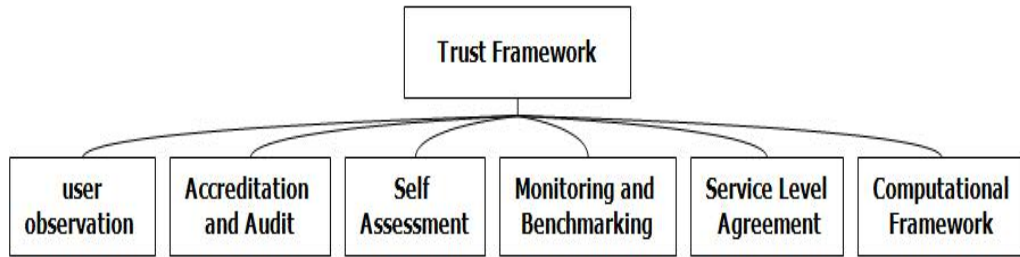


Figure 4.4: Types of trust frameworks

User Observation: Users opinion, social network, and reputation-based approaches are some of the user observation frameworks. The reputation of a CSP is the aggregated opinion of CSCs towards that provider and the services whereas trust is between two entities. Usually, a high reputation value indicates high trust and customers who need to make trust assessment on a provider, may use the reputation to estimate or calculate the trust level of that provider. The result is a comprehensive score reflecting the overall opinion of the CSCs, or a small number of scores on several major aspects of performance (Huang & Nicol, 2013). Hence, when a cloud user has only limited direct experience with a cloud service, other users' opinions could be an important source of cloud attribute assessment.

Self-assessment: It is a free publicly accessible method which allows CSPs and CIdPs to share self-assessment of their security controls, in either a questionnaire or a matrix. It shows and determines how CIdPs and CSPs align with the security guidelines (Samani et al., 2014).

Accreditation and Audit: Generally, the trust elements and characteristics of CSPs need to be verified before use for CSCs' decision making. Therefore, it is expected assertions from third-party independent professional organisations. A trust solution provides cloud users with a solution where the overall processes of cloud trust management can be delegated to the third-party professionals. Though, similarly, the basis for cloud customers to trust them needs to be established.

Therefore, one possible solution is formal accreditation and audit for the trust mechanism problems. So, auditing is considered in this thesis as a category of trust establishment and independent authority in the identity area. Therefore, external audits, attestations, or certifications for the more general purpose have been used in practice.

Monitoring and Benchmarking: The most common method to measure the reliability, power usage, performance, and application behaviour is monitoring and benchmarking. Moreover, this method assists to improve the security operation of systems and applications.

Service Level Agreement: By assessing the fulfilment of SLAs, practically the customers can understand the provider's level of trust, because it validates and monitors the defined schemes to quantify the system offered by providers (Saleh et al., 2014).

Computational Framework: It focuses on mathematically formal frameworks for measuring the level of trust, including modelling, languages, and algorithms for computing trust. It is an integrated method of previous methods and new methods to elaborate trust elements, prioritise, formulate and disseminate the level of providers' trust (Huang et al., 2016).

4.4.2 Trust Elements

To answer the second question, in this analysis step, the researcher seeks to draw upon key findings from related work on the CC, federated identity management, and trust computing. The aim is to extend these trust elements through identifying characteristics and attributes of cloud and CIdPs. To do so, question number two has been split into two questions:

- Between cloud provider and cloud consumer, what are the Essential System Attributes (ESA) of trust establishment?
- Between CIdPs and CIdUs, what are the Essential System Characteristics (ESC) of published trust establishment method?

The components of the trust framework based on (L. Wang et al., 2015) are organised as shown in figure 4.5. This framework provides features such as service selection based on trust requirements and ranking of CSPs and CIdPs based on previous real-time performance and user experiences. Likewise, a provider's trust value is assessed based on indirect information and direct observations, such as

recommendations. In this regard to help evaluate the elements, the trust evaluation's key elements based on the current research are defined as follows:

Cloud entities: it is responsible for understanding customer's application needs, interaction with them and performs ranking and discovery of suitable trusted services.

Monitoring and history information: The main goal for this section is satisfied user needs in the different perspectives. Next, it closely monitors direct and indirect trust with the providers' history records.

Computing service network structure and catalogue: One of the vital features of the provider is their service network and their features which advertise themselves into different classes.

The framework and previous researchers (Hallappanavar & Birje, 2016; Huang et al., 2016; Shaikh & Sasikumar, 2015), give two important points in building the framework that are: the measurement of various service trust evaluation, and the trust evaluation of service providers. However, these dimensions as shown in figure 4.5 and figure 4.6, are identified by considering the distributed and highly dynamic nature of cloud and cloud identity environments. Therefore, in this section, the main criteria for the evaluation has been categorised into three separate areas (figure 4.6) which are explained in the rest of this section.

Cloud Entities: Cloud brokers, cloud resellers, cloud consumers, and cloud auditors are four primary entities in the cloud evaluation environment (Chhabra & Dixit, 2015). They each play a different role and were identified by NIST (NIST, 2013b). However, in this sub-section, five cloud entities' trust evaluation issues are reviewed, and their trust relationship is identified.

Credibility: It refers to the quality of the service or information that establishes cloud entities trust of the service or information (Rannenbergh, 2015; Wu et al., 2013). The credibility evaluation appears in several forms including the entity's credibility and the feedback credibility. For instance, the trust management system can easily suffer attacks such as Sybil attacks, if no appropriate identity systems are deployed (Pecori, 2016).

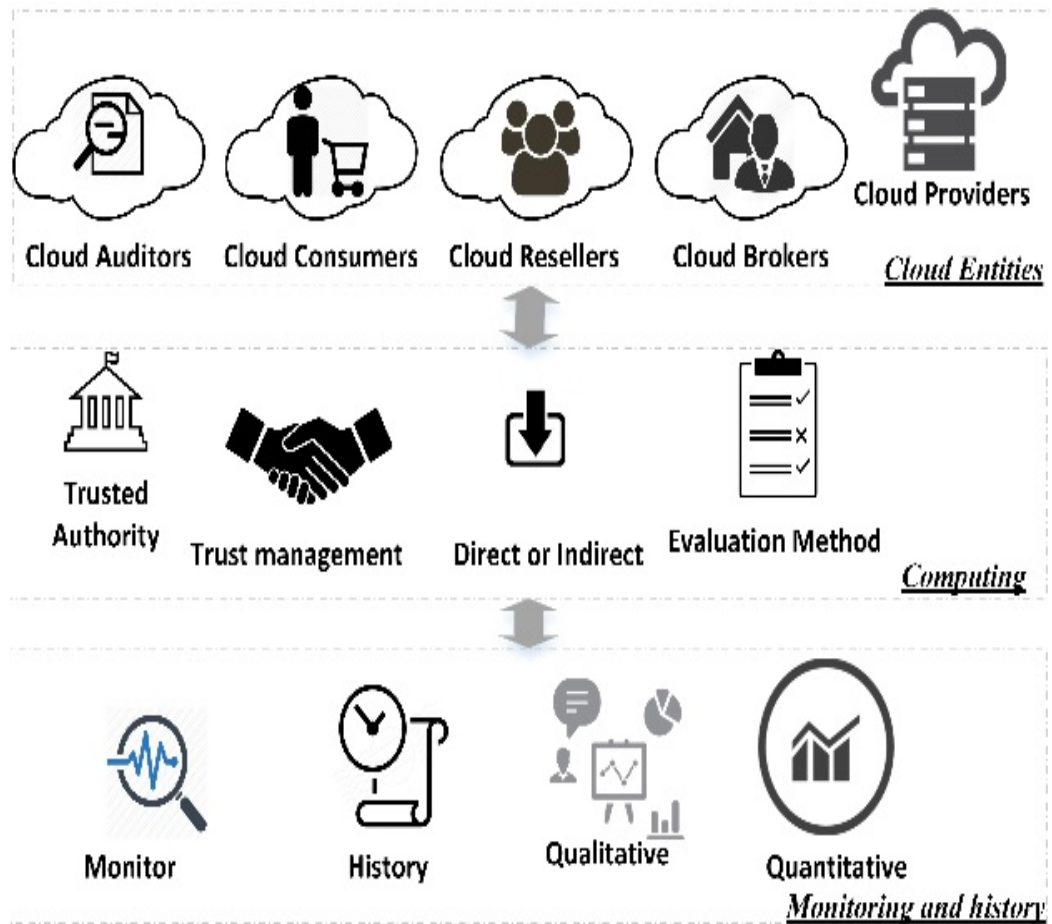


Figure 4.5: Service trust evaluation system architecture

Privacy: Refers to the degree of sensitive information disclosure that the cloud service entities might face during the interactions with the trust management system such as Trust & Assurance Registry (CSA STAR), the CSA, or Service Measurement Index (SMI). However, leaks of the cloud entities' sensitive information or CSP critical information are two examples of privacy breaches. However, Cryptographic encryption techniques will decrease the data utilisation

due to its distributed nature and highly dynamic nature of the cloud (Alaqra et al., 2016).

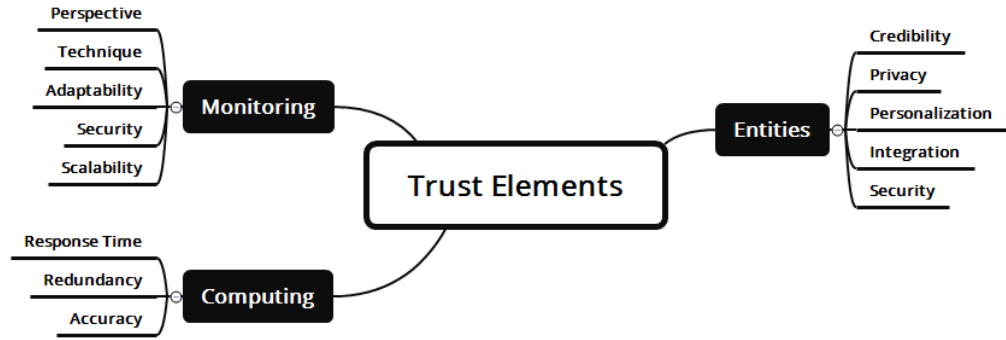


Figure 4.6: Trust elements

Personalization: Autonomy and its degree are the key points for personalization, and it is one of the main rules for the trust management. It means that selecting and choosing their provider based on their personal techniques and preferable elements. Therefore, to implement this method, the trust management framework should have fully autonomous collaboration. However, because of the complex features of the trust framework, it is hard to have a fully autonomous collaboration (Aguirre et al., 2015).

Integration: It is difficult to integrate numerous trust management techniques and perspectives. However, with different techniques and perspectives, CSPs and CIdPs can give their trust elements character and differentiation. Therefore, integrating numerous trust management characteristics brings accuracy to the trust level of any trust management system (M. Zhang & Huo, 2013).

Security: The level of protection that CSPs and CIdPs can provide against any threat is considered critical. For example, the Cloud Trust Protocol (CTP) (DiMaria, 2016) is the security mechanism which assists to generate evidence-based and knowledge-based protection elements.

Computing: A trust evaluation system should be able to evaluate and compute the trust relationships between CSPs and CSCs, which will significantly affect the level of trust. On the other hand, identifying trust computing methods and their perspectives, techniques, adaptability, security, and scalability remain an important, and challenging issue in the trust management area (Alshehri & Hussain, 2015; Hallappanavar & Birje, 2016). Therefore, in this subsection, the importance of these issues is explained.

Perspective: While some trust management frameworks consider the CSC's perspective, some others focus on the CSP's perspective. Consequently, it is important to consider both perspectives comprehensively and to utilise them in the trust frameworks (Noor et al., 2013).

Technique: It is vital to use strong techniques to assess the level of the trust. The technique that has been adopted by the trust framework is important for the acceptable and useful result. Moreover, adopting different techniques for trust management can bring accuracy of the trust results (Huang & Nicol, 2013).

Adaptability: Adoption is crucial for any new framework, therefore, how quickly the trust framework can adapt to changes in the complicated cloud environment is important. In addition, as per the highly dynamic nature of cloud updating the level of trust is crucial for any trust framework (Noor et al., 2016).

Security: The level of trust assessment functions to measure robustness against any security threat and attacks. There are two different security levels that attacks might happen; computing function (self-promoting, whitewashing, and slandering) and communication levels (Man-in-the-Middle (MITM) attack and Denial-of-Service (DoS)) (Luo et al., 2015) (Duncan et al., 2015).

Scalability: The CC is highly dynamic with distributed nature; therefore, it is important that the cloud trust frameworks would be scalable. The level of maturity in one or more trust elements is important for Scalability (Lehrig et al., 2015).

Monitoring and History: A trust evaluation system should be able to measure the truthfulness of entities based on the qualitative, quantitative, semi-qualitative, entities' history, and monitoring methods (Habib et al., 2012; Hallappanavar & Birje, 2016; Noor et al., 2016; Shaikh & Sasikumar, 2015; Wu et al., 2013). Hence, a reliable trust management system depends on the response time, redundancy, and accuracy and capability of collecting and filtering the trust's essential attributes and characteristics.

Response Time: It is important that the trust frameworks response time to handle trust inquiries, calculate them, access another source of the trust elements, and disseminate them to the trust framework users, is efficient (Dane et al., 2012; Pearson, 2013).

Redundancy: The level of redundancy in order to assess and manage the trust feedback is crucial. However, assessment redundancy and data redundancy are

two redundancy methods in the cloud environment. In assessment redundancy, multiple trust assessment inquiries are issued sequentially for the same CSPs while in the data redundancy it is used to avoid monitoring and scalability issues (Messina et al., 2014).

Accuracy: Refers to the degree of correctness of the monitoring, history, quantitative or qualitative results that can be determined through one or more attributes such as the unique identification of trust characteristics and using the proper techniques to disseminate the trust level. Poor identification of characteristics can lead to inaccurate trust results (Huang & Nicol, 2013).

4.5 EVALUATION YARDSTICK

In the evaluation theory, it is important to define the ideal target. In this chapter a trust framework for the cloud identity area is the main target. Therefore, the yardstick is defined as the trust identity management framework. However, a yardstick (Lopez, 2000) is a measure of the standard used for comparison or to judge a certain target. For instance, defining the group of criteria and consequently comparing them one by one with the ideal cloud target is one of the best practices for evaluation theory. Therefore, in this study, criteria are categorised and evaluated depending on the cloud trust framework and past experiences and knowledge and finally, compare with the yardstick.

4.6 DATA GATHERING

With “You can't control what you can't measure (Hillary & Madsen, 2002, p. 1)” researcher find out that measurement are the crucial part to control and mitigate the identity theft. However, based on the researches measurement, assignation, and opinion are three main data-gathering techniques used in most evaluations in the IT environment. They are required to obtain data to analyse each evaluation criterion (Lopez, 2000). Measurement involves the use of the appropriate documents and guidelines to extract the criteria. For the assignation, documentation inspection has been chosen. Also, observation techniques for getting subjective criteria data have been applied for an opinion step. The primary goal of this section is to provide decision makers (CIdUs and CSCs) with information as complete as possible. While, a checklist refers to a series of commands and instructions for verifying that the product has been operated correctly (Quinn et al., 2011). This study used the

proposed categorised frameworks as shown in figure 4.3 and the proposed ESA which is explained in detail in the next sub-section.

4.6.1 Data Gathering and Trust Framework

With the continuously growing interest of the CC services, many researchers (Corradini et al., 2015; Habib et al., 2012; Jahani & Khanli, 2016; Noor et al., 2016; Sun et al., 2011) have started to compare and evaluate CSPs' services in order to improve CSCs' decision making and help them to select appropriate services. A typical computational trust solution follows the high-level architecture depicted in Figure 4.7 that is modelled after a secure trust engine (Dondio & Longo, 2011). The defined trust based for the decision making is a multi-steps process, therefore, finding the most relevant and suitable data is the first step. Both provider as well as customers give these data to be used in the computational trust solution. The next step is technically choosing the trust elements as evidence for trust level calculation and also, discarding the other trust elements. Consequently, after evidence selection, measuring, and computing the trust element the crucial step for the trust level establishment is completed.

Accordingly, formalisation is the next step to provide reasonable and a valuable trust level. As a finding and contribution to this thesis other factors such as user's opinion, the risk of the providers, and standard can also be considered. Finally, the level of trust is presented to the users through the quantitative trust values (Dondio & Longo, 2011).

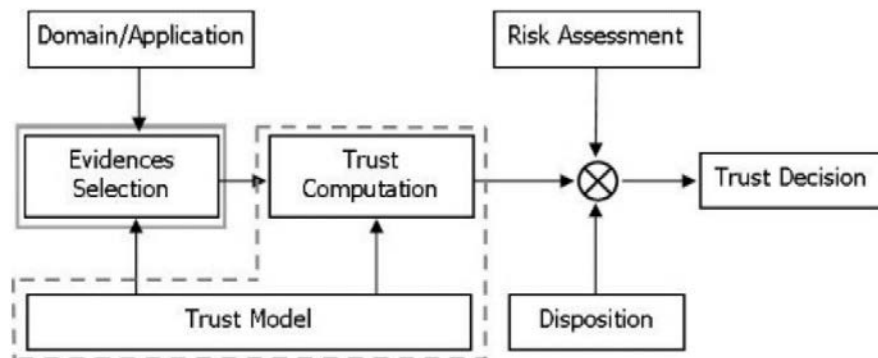


Figure 4.7: Computational trust solution (Dondio & Longo, 2011, p. 116)

Because of the criticality of many identity services and their tasks, numerous CIdUs cannot make decisions about choosing an identity service based solely on informal trust mechanisms such as web-based reputation scores. Therefore, these decisions

need to be more accountable, more dependable, and certain based on formal and informal elements.

These trust elements of CIdUs are used as an evidence for the user's trust judgment on the CIdPs, and their belief in those elements is based on these trust features. These features are categorised as a functional and non-functional feature in (Kanwal, Masood, Shibli, et al., 2014) which have been presented in figure 4.8 and is used in this thesis as assessment criteria to evaluate the existing trust models in the Cloud domain. The aim of a functional features' taxonomy is to satisfy and ensure efficient trust evaluation in the dynamic Cloud environment. Additionally, non-functional features aim to find the key features of existing trust models.

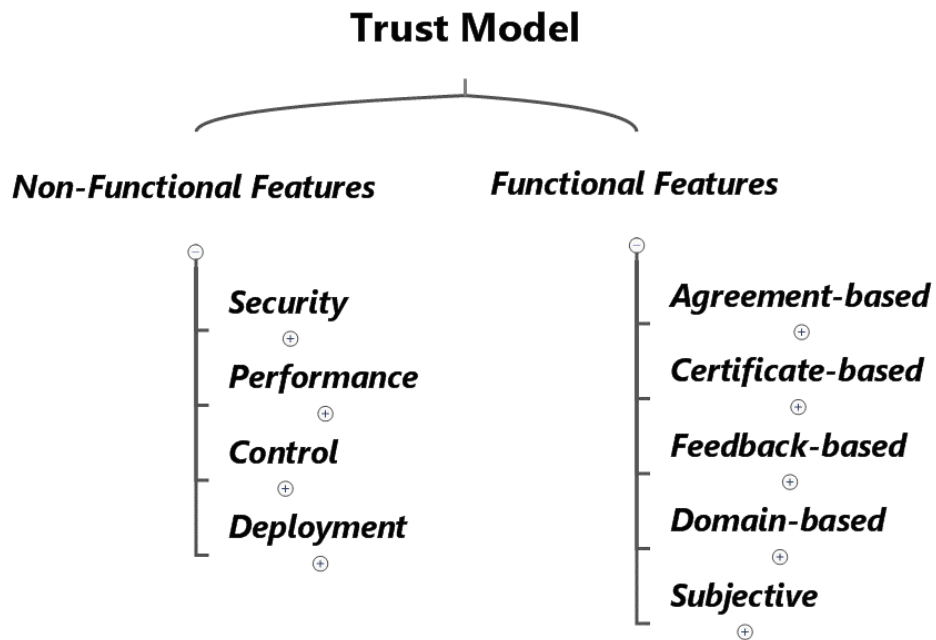


Figure 4.8: Trust model (Kanwal, Masood, Shibli, et al., 2014, p. 2)

Furthermore, Huang and Nicol (2013) categorised trust features as a performance and belief based on the customers' expectations. Trust in performance is trust about the performance of the trustee, whereas trust in belief is trust about belief of the trustee to perform. The trustee's performance could be the truth of what the trustee says or the successfulness of what the trustee does. In contrast, trust in belief is transitive, but trust in performance is not transitive. In addition, trust in performance can propagate through trust in belief. In this section, trust mechanisms in the cloud and cloud identity are explained, and their features are discussed based on the previous categorisation.

As a finding for this section and literature, most of the trust frameworks consider one factor and they are missing other relevant trust factors. However, these trust frameworks are considering either functional and technical features or the user feedback for establishing trust on CSPs. Therefore, these methods can not present a comprehensive trust level to either customers or providers.

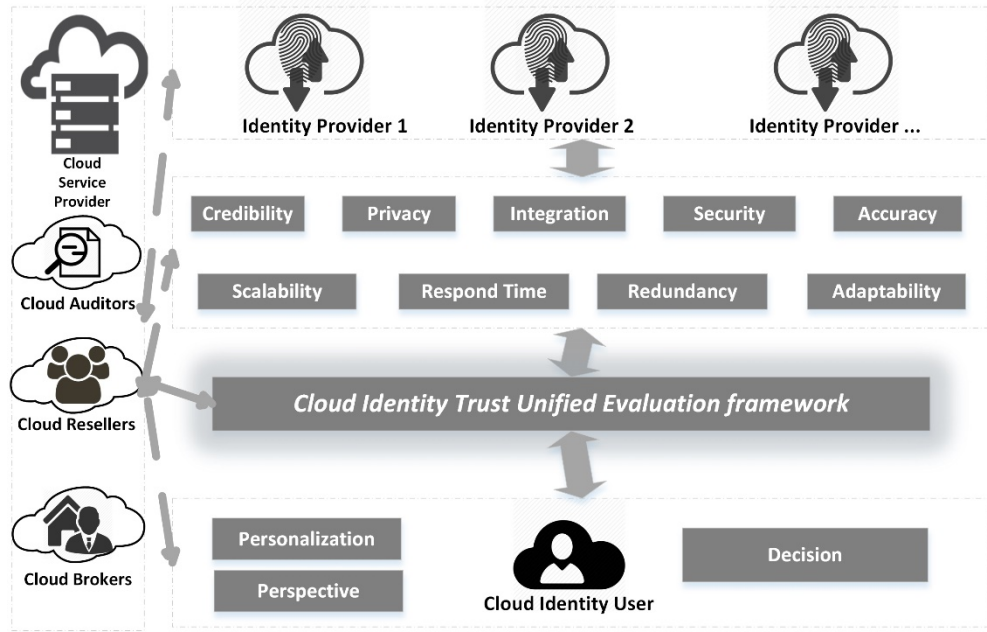


Figure 4.9: Trust unified evaluation framework

Figure 4.9 visualises the trust-aided technical solution (Trust Framework and Past Experience) for supporting the consumers in interacting with the most trustworthy CIdP. It shows the cloud identity consumers' interest and need of reckoning the trust effectors for establishing trust of the identity providers. The mapping shows the usefulness and absolute need of such parameters for selecting trustworthy service providers in an identity environment. Therefore, considering the identity specific parameters for trust models, in turn, support the identity consumers to know the capabilities and competencies of the CIdPs before interacting with them are crucial in this research.

The description of the target (4.2.1) and the criteria (4.2.2) are the basis for developing the yardstick. It contains the specifications, requirements, descriptions, and values for each criterion considered and has been virtualised in figure 4.9. In this section to develop the yardstick, the following steps have been done.

The yardstick is based on the trust framework and experience methods and is explained in the rest of this section. It uses the evaluation method to develop a

criteria tree (figure 4.4 and 4.5) and target. Based on the trust framework and experience, for each criterion, as shown in figure 4.9, the yardstick defines the specifications structured as pairs. Threshold values and the minimum value for each criterion is out of scope for this study, and the Importance Performance Analysis (IAP) method is used to indicate the priority of the criteria.

4.6.2 Data Gathering and Past Experience

The first trust elements (ESA) are developed to identify the essential cloud computing attributes according to cloud security, privacy, and trust attributes. The second trust elements (ESC) is designed to identify the essential CIdPs' characteristics regarding trust, security, and privacy.

This sub-section aims to address the main and crucial trust element for the CIdPs by considering both customers as well as a provider by using evaluation theory. These essential characteristics are considering trust, security and privacy issues of existing CIdPs. However, the method is based on a detail analysis of the current research papers and academic resources and finds the most common and key points regarding trusted computing, the CC, and cloud identity.

Table 4.1: Cloud identity balancing issues

Author (S)	Issues	Main issue	Keyword(S)
(Basney & Gaynor, 2011)	load balancing, fail-over, and replication of the OAuth Service.	Balancing	Elasticity
(Chard et al., 2014)	available, reliable, and scalable collaboration management.		Benchmarking
(Faraji et al., 2014)	scale to billions of transactions for millions of users and applications identity.		Algorithm
Iskandar et al., 2014	lack services that guarantee both data and access control.		Data Storage
(N. Zhang et al., 2014)	performance for data-intensive execution.		Schedule Policy
(Mathew et al., 2015)	malicious nodes.		Energy
			Consumption

Table 4.2: Cloud identity SSO issues

Author (S)	Issues	Main issue	Keyword(S)
(Goode, 2012)	identity issues.	SSO	Usability Identity Management Protocol Architecture Model Adoption Communication Security
(H. Wang et al., 2011)	security of the communication.		
(Shin & Kobara, 2010)	account and service hijacking.		
(Subashini & Kavitha, 2011)	security of the identity management and sign-on process of the SaaS vendor.		
(Saleem et al., 2012)	Surety to providing the secure cloud data management environment.		

Table 4.3: Cloud identity lifecycle issues

Author (S)	Issues	Main issue	Keyword(S)
(Gunter et al., 2011)	IAM less attention.	Lifecycle	Dynamic Management Assessment Measurement Security Requirement
(Iriberri & Leroy, 2009)	type of community.		
(Hu et al., 2014)	deploying an ABAC system across an enterprise.		
(Karuna P Joshi et al., 2014)	automate the usage of cloud services.		
(Jansen, 2011)	policy and procedures.		

Table 4.4: Cloud identity privacy issues

Author (S)	Issues	Main issue	Keyword(S)
(Balamurugan & Krishna, 2015)	mitigate privacy concern of data on cloud.	Privacy	User credential Service transaction Computation Data Policy
(Raykova et al., 2012)	access control policies.		
(Bertino & Takahashi, 2011)	identity management model.		

(Basney & Gaynor, 2011)	risk of plaintext storage of credentials.		
(Dong et al., 2014)	growing number of enterprises and customers.		

Table 4.5: Cloud identity risk issues

Author (S)	Issues	Main issue	Keyword(S)
(Richer & Tschofenig, 2012)	Access control risk.	Risk	Access Control Overbooking of resources Third Party Assessment Business Decision Sharing Data
(Latif et al., 2014)	mitigate theft risk.		
(Theoharidou et al., 2013)	poor access control.		
(Di Vimercati et al., 2012)	data outsourcing.		
(Djemame et al., 2014)	risk assessment.		
(Shirley Crompton, 2011)	security risk in sharing data.		

Therefore, by considering the chapter questions and review the scholarly publications six main categories of trust associated with cloud identity both from a cloud provider and customer perspective has been identified. These categories include balancing, SSO, lifecycle, privacy, risk, and standards. The contribution for this chapter and particularly for this section, is surveying the most relevant privacy, security and trust issues that pose threats in current and existing cloud identity computing environments. Consequently, as a summary for this section tables 4.1, 4.2, 4.3, 4.4, 4.5, and 4.6 analyse the main properties, which help in assessing the CIdPs operational trust.

To recognise and classify ESC, a *document review and guidelines checklists* (Philips et al., 2004) have been reviewed in term of gathering data and identifying criteria. The review result revealed that balancing, SSO, lifecycle, privacy, risk, and standards influence the level of trust in different research contexts. In this step, this research seeks to draw upon key findings from previous researches on the CC, trust computing, trusted computing, identity management, cloud identity, and federated identity management, which aim to extend these ESCs through identifying

characteristics of each CIdP in the cloud context. The result of this step is discussed as follow:

Balancing: load balancing or cloud elasticity is the system that guarantees the scalability and elasticity of the services, during the unpredictable time for the resources' request (peak hours or unusually high demand).

Table 4.6: Cloud identity standard issues

Author (S)	Issues	Main issue	Keyword(S)
(Jyotiyana & Mishra, 2016)	Eliminating Possible Backdoors in Client-Server Endorsement.	Standard	Token Biding Session Revocation
(Alsharnouby et al., 2015)	user strategies for combating phishing attacks.		IoT Shared Intelligence
(W. Li & Mitchell, 2014)	Security issues in OAuth 2.0 SSO implementations.		Phishing Protection Eliminating Password
(Yan et al., 2009)	federal identity management using hierarchical identity-based cryptography.		
(Mahalle et al., 2013)	capability based access control for the internet of things.		
(Leicher et al., 2012)	Card-based identity management.		

SSO: Refers to the user's capability to sign on multiple application or web-based environments. This concept is based on the centralised security point for managing identity and access security for both cloud-based and traditional applications and users.

Lifecycle: Refers to the granular processes from identity provision to revocation. The self-service feature of the cloud and cloud identity assists to implement secure and reliable service in all steps from provisioning to de-provisioning.

Privacy: Outsourcing, resource sharing, multi-tenancy are some examples of the CC new features which bring challenges and privacy issues for the cloud identity environment.

Risk: It is obvious that there are new risks by using new technologies such as cloud and cloud identity. However, these risks are compared with the traditional computing and consider them as essential system characteristics.

Standards: Standardization facilitates collection, verification, and updates to system security configurations. These can work in concert or be implemented separately. It also would allow authentication to be automated. However, the technical specifications that define scalable, open, and interoperable sets of mechanisms are the main goal of any identity and access management. Standard assure industry programs to ensure successful worldwide adoption and interoperability.

4.7 SYNTHESIS TECHNIQUE

Synthesis technique refers to a set of relative activities and stages to synthesize all information and data which are essential for each system criterion and require elaboration in order to evaluate CIdPs (Lopez, 2000). In this thesis, in order to synthesize the information obtained from documents review and guidelines, a novel hybrid evaluation and ranking technique has been developed by integrated critical interpretive (Dixon-Woods et al., 2006) and framework synthesis (Dixon-Woods, 2011). The preliminary concepts of the two evaluation and ranking techniques are addressed in the following sub-sections.

4.7.1 Framework Synthesis

Oliver et al. (2005) have applied a framework synthesis approach in their reviews. Framework synthesis is based on framework analysis. It applies to large amounts of scholarly data in the form of transcripts that need rational analysis to produce valuable data for the researcher. However, it brings a challenge for rigorous analysis, but, framework synthesis as a response to this issue and offers a highly structured approach to organising and analysing data to produce valuable information.

In section 4.2.2 types of trust, frameworks have been categorised. In this section as a part of framework synthesis, these frameworks are explained, and their

weaknesses and strengths are identified. Therefore, this section will cover the common framework adopted in trust models, trust evaluation model categories, and performance assessments. Moreover, during the review, some gaps of different approaches are analysed.

4.7.1.1 User Observation Trust Framework

In regards to user observation framework, numerous Bayesian methods have been proposed to compute the level of providers' trust (Schryen et al., 2011). Mármol et al. (2010) proposed a conceptual trust model of computing nodes. Moreover, a Verity fuzzy metric method was introduced by Omar et al. (2009) to quantify the consistency in compliance levels of a service contract. Messina et al. (2013) presented a model to address the service selection problem, and trust happens to be one of those considered quality criteria. The problem of their model is the lack of malicious detection consideration.

L. Wang et al. (2015) say that trust is complicated in a distributed computing environment. In addition, they construct their framework based on the Bayesian network to evaluate in a distributed computing environment. W. Wang et al. (2012) proposed a trust mechanism-based task scheduling model referring to the trust relationship models of social persons. A Bayesian cognitive method helped them build trust relationship among the CC nodes.

In the method which has been proposed by (Noor & Sheng, 2011), time is considered to measure trust. They named their framework Trust Evaluation Model based on Response Time (TEMRT) where feedback and response time has been considered as trust elements. Another important model is Propositional Logic Terms (PLTs) based trust model, in which feedback from different sources is the key element for the evaluation of trust (Habib et al., 2011a).

Likewise, it does not provide any assurance that all access to the data is under the complete control of the Cloud user. Thus no data ownership is guaranteed. Majority consensus and CC's capability provides dynamic credibility for detecting malicious entities in the Cloud. The trust management layer is deployed at a completely separate infrastructure between the consumer and the Cloud layers that introduces complexity in the applicability of this model. New entities can be inserted into the set of historical records to represent the feedback in a more reliable way that introduces high flexibility in this model.

It is impossible to ask a large number of CSCs to rate a CSPs against a large set of trusted attributes which are complex and fine-grained criteria. Moreover, reputation may be helpful when initially choosing a service, but is inadequate afterwards. CSCs need the experience to rate the trustee, and most of the customer's lack of this kind of experience when this experience is the CSCs' direct basis for cloud attribute assessment. The advantage of using user observation is that the data collected from first-hand and maybe most relevant, but the disadvantage is that the data accumulated are limited to the sample size and the range of the usage of the cloud service. Moreover, it is useful for overall rating because it is limited to rating a small number of attributes and the trustworthiness of a small number of users which is rarely taken into account. Figure 4.14 shows the summary of the framework synthesis for a user observation trust framework.

4.7.1.2 Self-assessment Questionnaires Based Trust Framework

Consensus Assessment Initiative Questionnaire (CAIQ) is the CSA questionnaire which assists to ensure security control transparency of the CSPs (Posey, 2016). This questionnaire assesses different characteristics and elements to provide valuable assessment results.

The design of a trust model should consider some specific criteria. A trust model must be a correct predictor of an identity provider's future behaviour. However, it should be accurate for long-term performance. Then, the trust model should recognise and reflect recent trends in entity performance. A good trust model should allow calculating trust value quickly with acceptable effort. Moreover, it should be able to recalculate a reputation value quickly, for example, old customers. Especially, calculations that can be performed incrementally are critical.

The CSA proposed a Consensus Assessment Initiative Questionnaire (CAIQ) for providing security control transparency. This questionnaire provides a means for assessing the capabilities and competence of cloud providers regarding different attributes (e.g., compliance, information security, governance). However, the metrics working group does not provide any proposals for a metric yet (in contrast to the other working groups of the CSA).

Likewise, the CAIQ, Siegel and Perdue (2012) proposed a method to systematically and critically assess the associated attributes and critical characteristics. They provide a framework Service Measurement Index (SMI) to

measure security, privacy and trust elements to help decision-makers to choose the best cloud service providers (IaaS, PaaS, SaaS, PaaS, and Big Data).

Moreover, a discounting operator is used by the model to assign credibility weights to the opinions collected from different sources depending upon their level of trustworthiness, thus supporting the credibility validation feature. The problem with this model is CSA does not guarantee the accuracy of any entries. As a result, the fact that a provider is listed on the CSA STAR Self-Assessment is an indication that the provider has desired to assert some level of diligence with a registration body but does not provide any assurance that they have adequate security practices or controls in place.

Besides CAIQ and SMI, CloudTrust Protocol (CTP) is another type of request-response mechanism which has been adopted by (DiMaria, 2016). This questionnaire assists to measure trust elements for the customers in the point of configuration, vulnerability, audit log, service management, and service statistics. However, an essential weakness of CTP is that the cloud service provider are only the main resource for the information. Therefore, dishonest CSPs and CIdPs can affect the validity of the data. From a trust judgement, it raises questions of the data's reliability. Figure 4.14 shows the summary of the framework synthesis for self-assessment trust framework.

4.7.1.3 Auditing and Risk Assessment

Cloud providers use different audit standards (SAS 70 II, FISMA, and ISO 27001) to assure users about their offered services and platforms (Gikas, 2010). Amazon Web Service Cloud Compliance (AWSCC) is the good example in for this criteria (AWS, 2016). CSPs use different audit standards (SAS 70 II, FISMA, and ISO 27001) to assure users about their offered services and platforms. The audit SAS 70 II covers only the operational performance and relies on a highly specific set of goals and standards. They are not sufficient to alleviate the CIdUs' security concerns, and most of the CSPs are not willing to share the audit reports, which also leads to a lack of transparency (Jahani & Khanli, 2016).

Moreover, it enables customers to understand robust controls in place at AWS to maintain security and data protection in the cloud. Besides, AWSCC enablers build on traditional programs; helping customers to establish and operate in an AWS security control environment. They are not sufficient to alleviate the

users' security concerns, and most cloud providers are not willing to share the audit reports, which also leads to a lack of transparency (Brooks, 2009).

In both an accreditation and audit provider is assessed by an independent third party; though, they may have different focusing aspects of assessment. Accreditation focuses on the qualification of the accredited provider with respect to conducting a specific type of professional services; while, audit focuses on assessing the performance of the audited provider with respect to the common requirements of the professional standards. However, audit typically takes place annually or once whereas, accreditation takes place over a longer period. In conclusion, in the context of the CC, the assessments by audit and accreditation are objective, but they are not real-time information as real-time benchmarking and monitoring which is explained in the next sub-section. In (Habib et al., 2012) insufficient evidence for security concerns and a lack of willingness to share audit reports has given an audit framework based on the cloud customers. Based on this analysis, Figure 4.14 shows the summary of the framework synthesis for auditing and risk assessment trust framework.

4.7.1.4 Benchmarking and Monitoring

In this section, the concepts of system monitoring, quality of services, and ranking are defined. The concept of ranking is applied to prioritise the elements based on their levels, such as the ranking of web services and universities. Quality of Service is informed by the information of monitoring and benchmarking and to represent the functional level of their attributes (Mohammadkhanli, 2014).

Therefore, in this section, the most common monitoring frameworks are explained. For example, Qu et al. (2013) proposed a trust framework to user feedback for service ranking. Objective assessment and subjective assessment are two types of information from the user to benchmark service provider and put them in, as shown in figure 4.10.

For example, Choudhury et al. (2012) proposed the Service Ranking System (SRS). Static and dynamic states of cloud service ranking are considered in the SRS. Besides SRS, Chan and Chieu (2010) proposed the Service Mapper Approach (MPA) uses Singular Value Decomposition (SVD) technique, which is a statistical technique for cloud service ranking as depicted in figure 4.11.

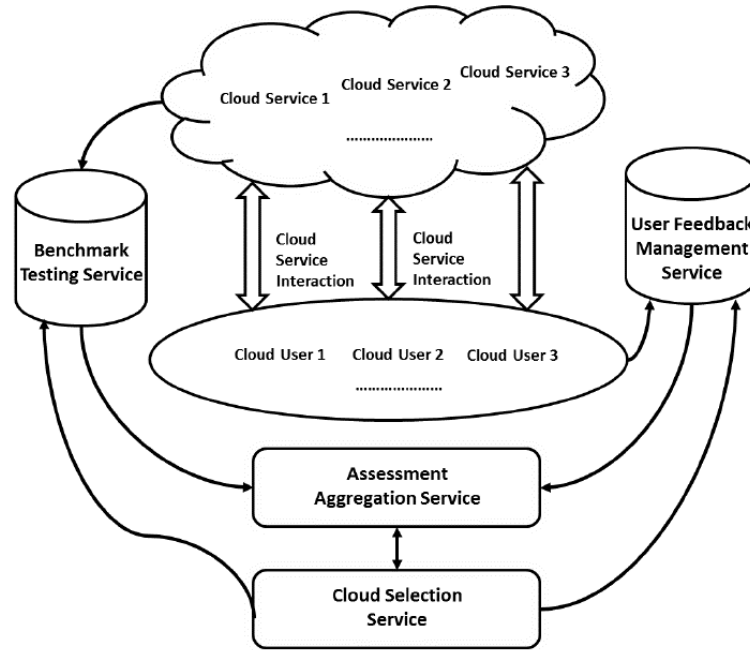


Figure 4.10: Aggregation approach framework for cloud service selection ((Qu et al., 2013, p. 154).

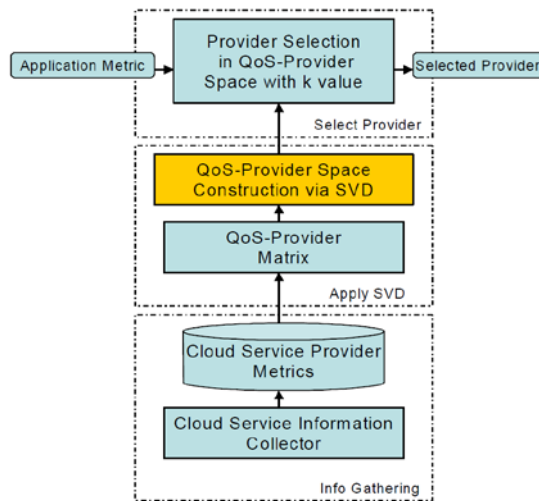


Figure 4.11: Cloud service mapper (Chan & Chieu, 2010, p. 363)

Another example is the prediction of qualitative values in the CloudRank approach (Zheng et al., 2013) which has been considered as a method for the cloud ranking (figure 4.12). Moreover, in conventional approaches based on components, the components were applied for measuring the values. However, it is impossible to apply in a cloud environment, for the reason that this task entails a high time complexity and cost. In addition, calling usually would not achieve a correct answer due to the Internet's unpredictable connections.

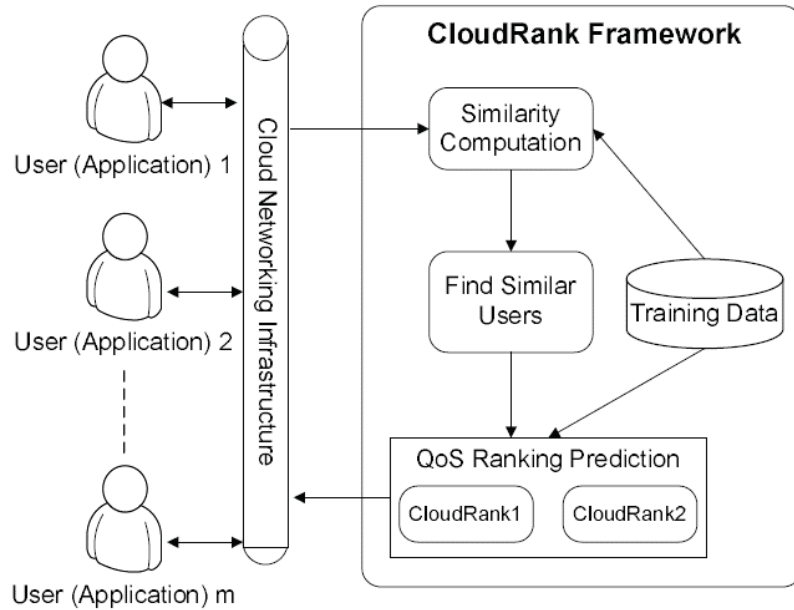


Figure 4.12: CloudRank's system architecture (Zheng et al., 2013, p. 1214).

Cloudstone (Sobel et al., 2008) is a multi-platform, multi-language performance measurement tool for Web 2.0 and internet-based service, so, good example for the cloud monitoring. Cloudstone aims to answer CSCs monitoring questions for the CC services and tested it on Amazon EC2 configuration. Likewise, CloudHarmony (Harmony, 2016) claims that they provided objective, impartial and reliable performance analysis to compare cloud services. CloudHarmony is a resource for evaluating performance. Similarly, CloudCmp (A. Li et al., 2010) is a systematic comparator of the performance and cost of cloud providers. CloudCmp measures elastic computing, persistent storage, and networking services offered by a cloud along with metrics that directly reflect their impact on the performance of customer applications.

In the area of the low level monitoring, CloudSleuth (Dynatrace, 2016) is a good example for cloud performance visualisation tool initially created as an internal resource to help users measure the reliability and consistency of the most popular public IaaS and PaaS providers. Moreover, CloudRank-D (C. Luo et al., 2012) proposes to benchmark and rank the CC systems that are shared for running big data applications. It provides 13 representative applications from different research domains according to their popularity. HiBench (Ivanov et al., 2015) is a benchmark suite targeting the components of the Hadoop framework. The use of many realistic workloads fully exercises Hadoop's parallel computing component (MapReduce) and database component (HDFS).

Furthermore, the ranking tool which has been developed by Yahoo is Yahoo! Cloud Serving Benchmark (YCSB) (Cooper et al., 2008) to benchmark their delivery system. Furthermore, SpotCloud is a new cloud ranking method (spotcloud, 2016) that provides a platform where customers based on the quality, and cost, have the ability to choose the providers.

Table 4.7: Comparison of existing cloud monitoring approaches

Cloud Monitoring	High level	Low level	Computation Based	Network-Based
Cloudstone	✗	✓	✗	✓
CloudHarmony	✓	✗	✓	✓
CloudCmp	✗	✓	✗	✓
CloudSleuth	✓	✗	✗	✓
CloudRank-D	✗	✓	✗	✗
HiBench	✓	✗	✓	✗
YCSB	✓	✗	✓	✗
SpotCloud	✓	✓	✗	✓

This section has defined structures for monitoring and benchmarking and identified their weaknesses and strengths. In figure 4.14, types of approaches are reported, and their pros and cons are systematically presented based on the previous analysis. They are focusing on the infrastructure, and they ignored platform and software as a service. They are challenging the efficient management based on the low level and high-level monitoring. But, by increasing the number of services which must be ranked, the execution process tends to need more time. Consequently, the framework would fail while covering all of the qualitative attributes and may not always respond to the user. Therefore, most of the reviewed approaches did not include interoperability metrics. However, most of the frameworks are customised to monitor and benchmark a particular cloud service. In the other words, focusing on the infrastructure, challenging efficiency and performance are the main strengths of the monitoring and dependent on the existence and usage of previous knowledge weaknesses are: scalability, interoperability, and customizability. So, Figure 4.14 shows the summary of the framework synthesis for monitoring and benchmarking a trust framework.

4.7.1.5 SLA Based Trust Framework

SLA and QoS verification are important sources of evidence to verify the level of trust. The belief in the results of SLA monitoring is dependent on trust attribute extraction with respect to objective and professional monitoring. Numerous

guidelines and researchers have contributed to the standardisation of SLA metrics in the CC. For example, guide to Cloud SLA (Council, 2016), Service Measurement Index (SMI) defined by CSMIC (Siegel & Perdue, 2012), TM Forum (Forum, 2016), NIST Cloud Computing Standards Roadmap (Liu et al., 2011), and Cloud Computing SLAs (Commission, 2016) have worked to identify the SLA metrics. In the CC environments, customers are responsible for monitoring SLA violations and informing providers. The cloud providers write compensation clauses in SLAs in such a way that the customers merely get the advantage of applying for compensation due to SLA violation. The problem of compensation arises for not having standardised SLAs for the consumers in the CC. Resource Description Framework (RDF) format is one of the automatic extraction trust attributes from SLA for the CC (Karuna Pande Joshi & Pearce, 2015; Mittal et al., 2016) use to find SLA parameters. RDF is a World Wide Web Consortium (W3C) standard for describing Web resources. RDF is written in XML, and it is a W3C Recommendation.

Chauhan et al. (2011) conducted the process of identifying compatible cloud provider based on RDF and semantic web for given requirements by matching SLA parameters. Alhamad et al. (2010) proposed an SLA-based model to evaluate the trust of CSP that includes SLA-agent, research module and Cloud services directory. The core of the model is an SLA-agent that is responsible for designing the SLA parameters and negotiating the SLA with the CSP. Another SLA-based model has been proposed by Chakraborty and Roy (2012), in which various QoS parameters have been identified to estimate the trustworthiness of CSPs.

In the cloud environment, customers are responsible for monitoring SLA violations and informing the providers for compensation. Therefore, the critical analysing of the common and contemporary SLA trust framework, the researcher came to this point that cloud users need to verify and re-evaluate SLA trust attributes. However, the QoS, QoP and SLA mechanism can accomplish visible elements of the CSPs; but, it cannot help to accomplish the invisible elements such as privacy protection inside a CSPs. All advantages of the SLA trust framework still leave some issues such as cumbersome task to retrieval, over-committed, and non-standardized elements, and so on, as shown in figure 4.14 (Habib et al., 2012).

4.7.1.6 Computational Based Trust Framework

The CC model has certain unique characteristics and uses techniques that have lead to several new trust frameworks and the need to re-evaluate and redefine many well-defined past trust models. The mechanism of using different attributes, characteristics, assessments, certifications, and evidence like performance, security, and privacy trust judgments are complex, due to a large set of elements to consider and a possibly a long chain of trust relations. Nevertheless, the policy and PKI based, trust judgment can be regarded as a simplified version of the evidence-based, mechanism, in the sense that a widely accepted policy captures a set of key attributes (Huang & Nicol, 2013). However, extensive research (Djemame et al., 2014) effort was focused on defining the CC risks.

Risk assessment has a valuable role in measuring the security and privacy features of the CSPs. Therefore, researchers (Djemame et al., 2014; F. Liu et al., 2015; Z. Liu et al., 2015; Ruiz & Pedraza, 2016) have proposed risk assessment methods in the CC environment to assists delivering the trust result. However, some of these researchers focused on specific security problems such as virtualisation threats, authentication and authorisation issues, and insider attacks. However, some of these researchers (Tanimoto et al., 2011) used the risk breakdown structure method to extract the risk factors in the CC from the users' viewpoint which is an important perspective for this thesis. But, still, these studies overlooked the management of the cloud infrastructure, cloud users, CSCs' privacy, and multifactor integration (Sato et al., 2010).

Noor and Sheng (2011) have proposed "trust as a service" computational trust framework to evaluate the trust of CC on CSP. Their trust framework performs the evaluation and calculation of trust by collecting feedback from various CSPs and CCs. On the other hand, Garg et al. (2013) believe that to choose appropriately between numerous providers there has to be a precise way to identify and measure key performance criteria. In this regard, the trust computational trust framework is proposed by the Cloud Service Measurement Index Consortium (CSMIC) and is a response to this issue.

Wagle et al. (2015) believe that there is no evaluation model, which provides the real status of CSPs for the CSCs. They proposed an evaluation based on the quality of cloud services delivered for each service and provided the service

status of the cloud providers. A. Li et al. (2010) proposed a CloudCmp 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 CPU utilisation and network throughput.

A trust model based on past credentials and present capabilities of a cloud resource provider has been proposed by (Manuel , 2015). Trust value is calculated using four parameters such as availability, reliability, turnaround efficiency, and data integrity. The aim of (Shaikh and Sasikumar , 2015) trust model is measuring the security strength and computing a trust value of the CC. CSA service challenges are used to assess the security of service and validity of the model. Dólera Tormo et al. (2012) described how user-centric techniques and trust and reputation systems can be integrated into identity management systems to achieve some of the presented challenges.

There are ad-hoc approaches to support the consumers in selecting trustworthy CSPs and CIdPs. Based on the figure 4.13 (Habib et al., 2012) these approaches are SLA, Auditing, Measuring and Rating, and Self-Assessment, which are elaborated in the rest of this subsection.

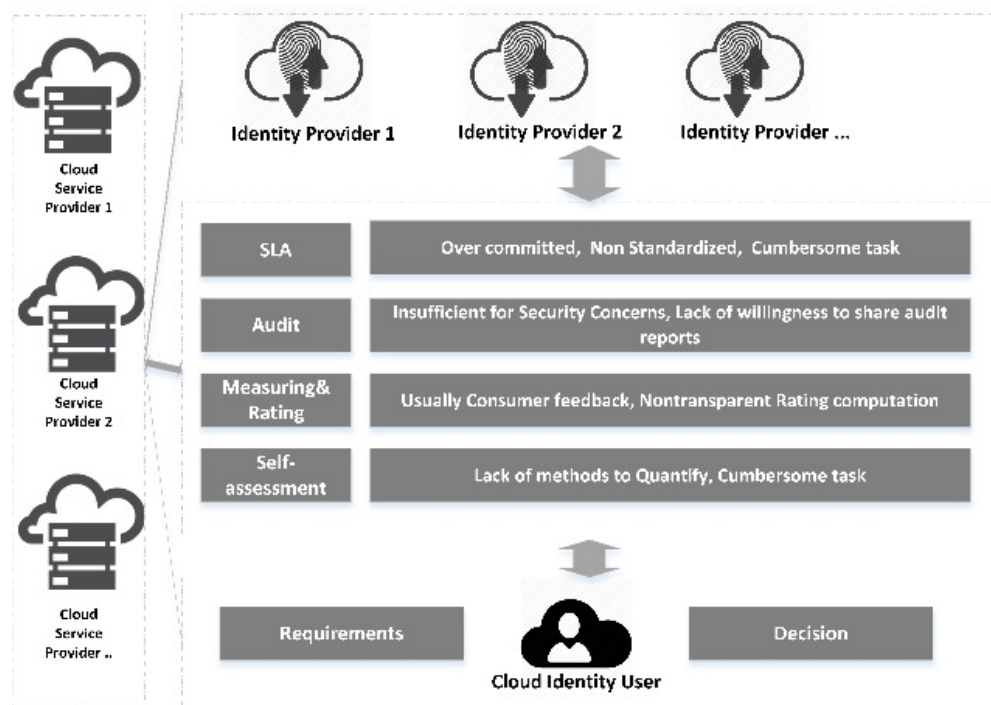


Figure 4.13: Current trends for trust establishment in cloud and cloud identity
(adopted from Habib et al., 2012, p. 9).

Kanwal, Masood, and Shibli (2014) proposed a trust evaluation model that helps the CSPs to evaluate and establish trust, hence making them participate in the trusted and reliable Cloud Federation. The model is based on two essential factors for trust evaluation, feedback and SLAs between CSC and CSP. Chan and Chieu (2010) believed that determining the best service for a specific application is a challenge and often determines the success of the underlying business for the service consumers. They proposed a set of CC specific performance, QoS attributes an information collection mechanism, and the analytic algorithm based on Singular Value Decomposition (SVD) technique to determine the best service provider for a user application with a specific set of requirements.

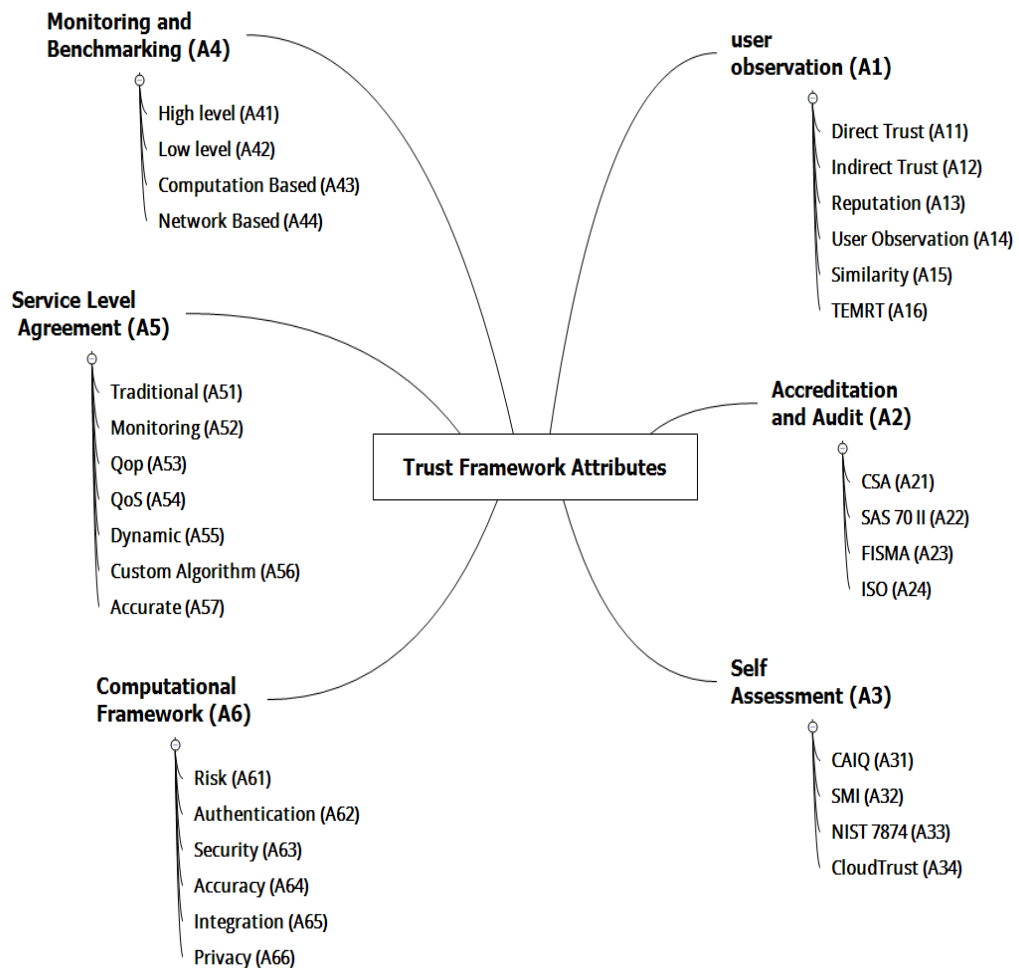


Figure 4.14: ESA for this thesis

(Qu et al., 2013) concluded that trust frameworks focus on objective performance analysis based on cloud monitoring and benchmark testing without considering the viewpoints of cloud users who are consuming cloud services. They proposed a

model of cloud service selection by aggregating the information from both the feedback from Cloud users and objective performance analysis from a trusted third party. So, Figure 4.14 shows the summary of the framework synthesis for computational-based trust framework.

4.7.2 Critical Interpretive Synthesis

Barnett-Page and Thomas (2009) developed their own approach to synthesising multi-disciplinary and multi-method evidence, termed critical interpretive synthesis while researching access to healthcare by vulnerable groups. Critical interpretive synthesis is an adaptation of meta-ethnography, as well as borrowing techniques from grounded theory. The authors stated that they needed to adapt traditional meta-ethnographic methods for synthesis since these had never been applied to quantitative as well as qualitative data, nor had they been applied to a substantial body of data.

(Dixon-Woods et al., 2006) presented critical interpretive synthesis as an approach to the whole process of review, rather than to just the synthesis component. It involves an iterative approach to refining the research question and searching and selecting from the literature (using theoretical sampling) and defining and applying codes and categories. It also has a particular approach to appraising quality, using relevance. The authors also stress, as a defining characteristic, critical interpretive synthesis's approaches to the literature in terms of deconstructing research traditions or theoretical assumptions as a means of contextualising findings. In this section, critical interpretive synthesis is adapted to identify the essential cloud computing trust attributes and essential cloud identity trust characteristics.

4.7.2.1 Essential Cloud Computing Provider Trust Attributes

The analysis of the contemporary trust framework is discussed as a contribution for this section. The researcher came to this point that the feedback from customers does not offer any technique to validate the credibility of the provider. Similarly, the QoS attributes offered by providers does not assure the level of the quality because it is only focused on their supplied services evaluation and selection (Hallappanavar & Birje, 2016).

The CC can have both low and high level of monitoring; however, these two methods are required to have a valuable result. The data related to the virtual

platform is monitored at a high level, but, on the other hand, the data collected by the providers are monitored at the low level.

Likewise, Computation-based and Network-based are two types of monitoring which in the Computation-based the data is related to real or virtualised platforms such as CPU speed, memory page exchanges per second, and server throughput are monitoring to get the trust level while the packet data lost, traffic volume bandwidth are some example for the network-based monitoring (Aceto et al., 2013).

As highlighted above, there is a large number of solutions for monitoring public and private Cloud platforms, having different properties and each focusing on a subset of the features (Table 4.7). The infrastructure of a Cloud is very complex, and this complexity translates into more effort required for management and monitoring. The greater scalability and larger size of Clouds compared to traditional service hosting infrastructures, involve more complex monitoring systems, which have therefore to be more scalable, robust and fast (Fera et al., 2015). Such systems must be able to manage and verify a large number of resources and must do it effectively and efficiently. This has to be achieved through short measurement times and fast warning systems, able to quickly spot and report performance impairments or other issues, to ensure timely interventions such as the allocation of new resources.

In order to solve the complexity and validity of the trust framework, some researchers (Aceto et al., 2013; Fera et al., 2015; Weber et al., 2014) focused on various aspects of trust management including reliability assessment, trust mechanism, trust concept model, and trust evaluation research. However, still service dynamic trust evaluation and valid trust elements for the specific and particular provider remains as an open field of research and available for this research. Marudhadevi et al. (2014) identify trusted cloud services while negotiating an SLA. The knowledge is discovered from a previously monitored dataset, and a trust value is generated.

Habib et al. (2011b) in their research found while SLAs are not consistent among the CSPs with similar functionality, it does not address identifying a trustworthy cloud provider for the customer.

There are numerous SLA trust management systems, but, these methods require a distributed monitoring system for CC and to have several properties that

are not always present. Moreover, they have a problem with defining both QoS and Quality of Protection (QoP) parameters to evaluate the trust score.

Furthermore, custom algorithms and techniques used for filtering and extracting trust parameters in order to achieve accurate trust decision are issues of SLA based trust framework. The combination of functional and non-functional trust models leads to more accurate results. Roughness and the amount of indiscernibility is the result of lack of accuracy. Table 4.8 is an overview of SLA trust models and an analysis of the categories based on previous clarifications. A critically review of SLA shows that it is focusing on visible trust attributes and does not focus on invisible trust attributes like privacy, feedback, and security. Also, extracting visible trust elements needs the capability to do fine-grained QoS and QoP monitoring; and, a professional third party is needed to help CSC to make a good decision.

Table 4.8: Comparison of existing SLA cloud trust approaches

Cloud SLA	Traditional	Monitoring	doQ	QoS	Dynamic	Custom Algorithm	Accurate
(Chauhan et al., 2011)	✓	✓	✓	✗	✗	✓	✓
(Alhamad et al., 2010)	✗	✓	✗	✗	✗	✗	✗
(Chakraborty & Roy, 2012)	✗	✓	✓	✓	✓	✗	✗
(Marudhadevi et al., 2014)	✓	✓	✗	✓	✓	✓	✓
(X. Li & Du, 2013)	✗	✓	✗	✓	✓	✓	✓
(Habib et al., 2011b)	✗	✓	✓	✓	✗	✗	✓

For CC business, selecting the best cloud service from appropriate cloud providers is very complex and challenging for the cloud users. Identifying trustworthy cloud services is difficult because of their diversity and the similar functionalities CSPs provide for the CSCs. Therefore, the following trust characteristics that consumers

should pay attention to when comparing cloud services from various representative providers are defined.

Generally, in the computational framework, there are some criteria to be considered for the researcher to compare contemporary computational frameworks. Therefore, in this research, as a contribution, the risk assessment method is categorised as: Qualitative (QL), Quantitative (QN), and Semi-Quantitative (SQ). However, Authentication (A), is a crucial part of any risk assessment method is considered in the table 4.9 comparisons.

Another element for the computational framework is the security because trusted providers should have an acceptable level of security. Therefore, in this research, as a contribution, the security method is categorised as Access Control (AC) and communication (SC). However, Privacy is another feature for any trust framework which there are two types of privacy for this research based on the systematic and critical analysis of the current scholars: Privacy of the Provider (PP) and Privacy of the Consumers (PC). Moreover, accuracy is another element which the accuracy of trust assessment results depends on both effectiveness of the assessment of functional security and correct identification of trust feedback. Other methods that cause inaccurate trust result are the poor identification of trust Feedback (AF) and failure to prevent Attackers (AA). Besides all of these elements, lacking recommendation make any trust framework inaccurate, therefore, another element for the computational framework is the reputation and recommendation which can increase trust results' accuracy. Last but not least, the last element for this section is integrity (I) can also lead to better trust results by matching appropriate consumers to trustworthy providers.

The elements used to analyse the current literature, and the results are shown in table 4.9. This Table summarises critical interpretive synthesis based on the computational trust framework. These characteristics and criteria have been used to evaluate trust management systems for the CC and cloud identity. Some of the trust management systems (Table 4.9) have been analysed do not have a mechanism to preserve participants' expectation, to protect Cloud users' identity while minimising the impact on system performance.

Table 4.9: Comparison of existing cloud trust framework

Trust Framework	Risk	Authentication	Security	Accuracy	Integration	Privacy
(Tanimoto et al., 2011)	QL	A	SC,AC	N	N	N
(X. Zhang et al., 2010)	QL	N	AC	N	N	PP,PC
(Fitó & Guitart, 2014)	QQ	N	SC	N	N	PC
(Albakri et al., 2014)	QQ	A	SC,AC	N	N	PP,PC
(Theoharidu et al., 2013)	QL	N	AC	N	N	N
(Noor & Sheng, 2011)	QL	Ni	AC,SC	AF,AA	N	PC
(Habib et al., 2011b)	QQ	N	AC,SC	AF,AA	I	PC
(Wagle et al., 2015)	N	N	SC	N	I	PP
(Garg et al., 2013)	QL	N	AC,SC	N	N	PP
(Manuel, 2015)	N	N	AC,SC	N	I	PP
(A. Li et al., 2010)	N	N	SC	N	N	N
(Shaikh & Sasikumar, 2015)	N	A	AC,SC	N	N	PP
(Dólera Tormo et al., 2012)	QL	A	AC	N	N	N
(Kanwal, Masood, & Shibli, 2014)	N	N	SC	AF	I	PP
(Chan & Chieu, 2010)	N	N	SC	AF	I	N
(Qu et al., 2013)	N	N	SC	AF	I	N

Generally, trust is a crucial part of the CC, and it is a critical aspect of whether CSPs or CSCs are used. In this thesis, existing trust frameworks have been categorized, and their evidence has been analysed. This category is based on the user observation, self-assessment, accreditation, SLA, and computational trust framework. Most current research which has focused on aspects of trust has ignored other aspects of trust. Therefore, the literature is insufficient because trust is a complex social phenomenon, and a systematic view of the current literature shows the needs for integrated attributes for trust computing. The summary view of trust establishment mechanisms and their features, attributes, evidence, and weaknesses

have been analysed. As a contribution for this chapter, a computational trust approach to trust evidence has been reviewed by which the trust placed between CSCs and CSPs is visible.

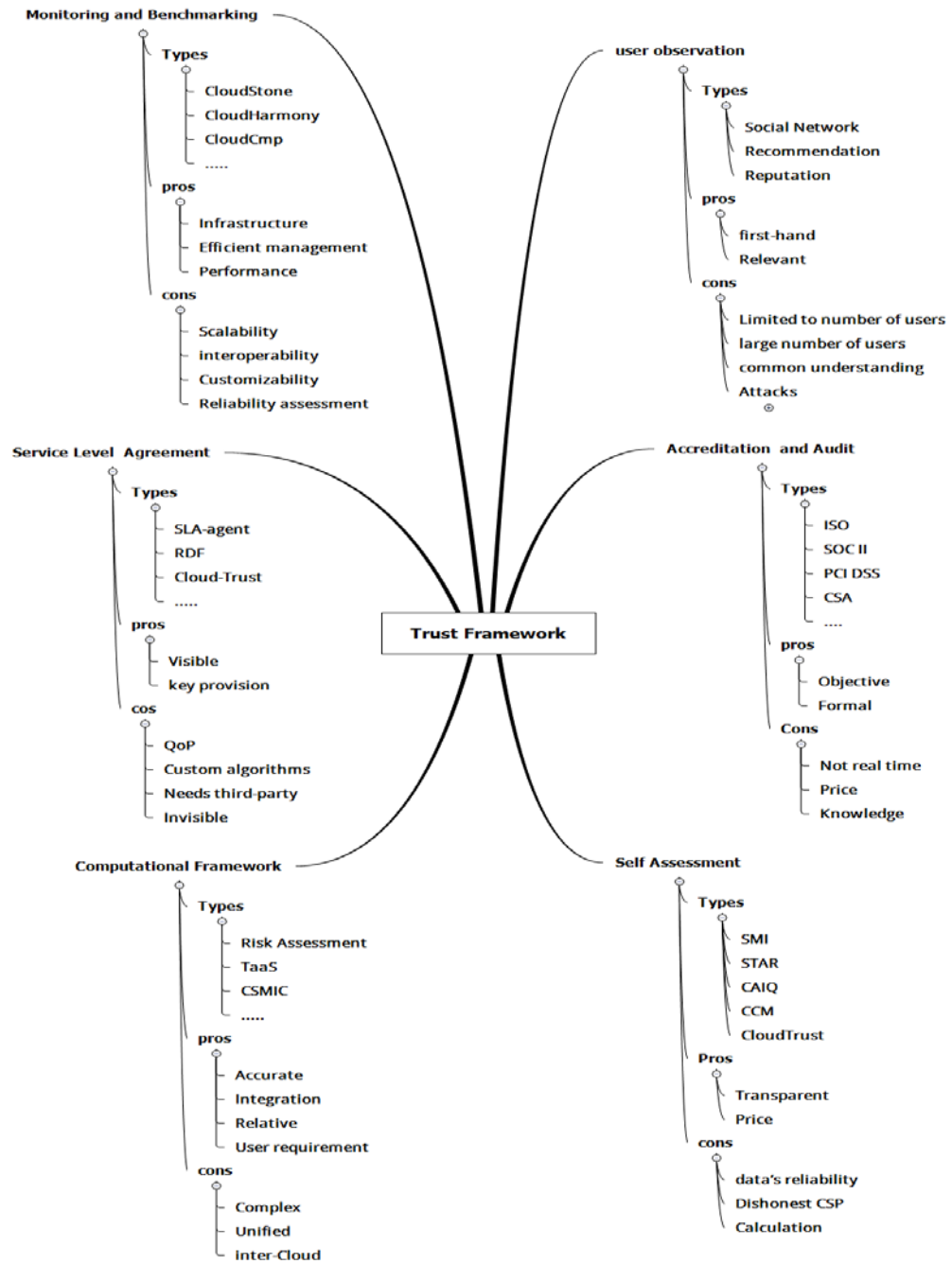


Figure 4.15: Cloud computing framework synthesis

Moreover, a general structure of the computational framework has been proposed to do trust judgments based on the semantics of trust. In chapter four, based on the methodology of chapter three, has focused on mathematically formal frameworks for reasoning about trust, including modelling trust, prioritise the evidence, formulation and languages, and calculation for computing trust level.

Systematically and critically most of the trust management frameworks (Table 4.7, 4.8, and 4.9) have been examined do not support the integration and utilisation of trust feedback while this is a challenge for providers and issue for customers. Therefore, a trust framework that has the ability to integrate numerous types of feedback is needed to improve trust results. Also, some of the trust management systems (section 4.6) do not provide proper security and privacy protection for their customers.

Furthermore, some of the works (Table 4.7, 4.8, and 4.9), only compare network throughput or CPU utilisation and do not cover the performance measurements, security, and privacy of service providers. The granular analysis of considerable literature exists on trust models (Table 4.7, 4.8, and 4.9) reveals that most of the trust frameworks are mainly evaluate the trust between two providers. However, after analysing these trust models (Table 4.7, 4.8, and 4.9, and previous methods), the main finding is revealed that trust evaluation should not be based on a single factor (feedback, SLA or recommendation) rather trust value should be the aggregation of these different trust elements.

The level of trust in the cloud environment is dependent on several sources of evidence and trust elements; however, it is not necessary to use all of these attributes and characteristics; because, a cloud user may use one or more sources of evidence for trust decision making, dependent on the user's trust requirements. For example, to decide whether to CSP' trust level, a CSC simply checks whether the user observation, accreditation, monitoring, SLA, and computational sources of evidence, are present. As a finding for the literature, there are only a few theses (Table 4.7, 4.8, and 4.9) articles that focus on the evaluation of CIdPs or on finding appropriate solutions to establish confidence and trust between the consumers and the CIdP. The particular issue in this research is focused as shown in the figure 4.15. In addition, a model that incorporates all aspects of security quantification measure for cloud identity is still needed. Moreover, many research-works (Table 4.7, 4.8, and 4.9) have been conducted on various aspects of trust management including trust concept models, reliability assessment, trust mechanisms and trust evaluation. Service dynamic trust evaluation in the CC environment remains as an open field for research from diverse perspectives.

At present, according to the cloud ESA and essential CIdP characteristics, there is no longer a unified standard and rank framework for CIdP trust evaluation.

Therefore, to evaluate trust of identity services, a new framework and evaluation method is required to determine the weight of different indexes, and fully reflect the objectivity and accuracy in the cloud authentication environment. However, the factor scope is usually limited, which neglects the other important contributions, which have a huge effect on trust. Additionally, a whole evaluation framework for trust, can help users choose and monitor the CIdP state. Regarding trust behaviour, trust models paid attention to different trust effective measures like uncertainty, trust aggregation and trust customisation. No framework can allow CIdUs to evaluate CIdPs offerings and rank them based on their ability to meet the CIdUs' requirements.

In conclusion, Cloud trust framework is a highly promising technique, but despite many efforts to address cloud trust issues, several issues such security, privacy, access control, and integration, continue to be major weaknesses for cloud user decision making.

4.7.2.2 Essential Cloud Identity Provider Trust Characteristics

While there are numerous CIdPs with similar functionalities (Habiba et al., 2014), CIdUs are interested in selecting CIdP not only based on the functional characteristics but also based on non-functional characteristics. The main motivation for this selection is the capabilities the providers possess regarding functional and non-functional attributes. SLA is a common practice that identity providers consider building a contractual relationship with potential consumers. In the context of SLA, identity users trust an identity provider to provide compensation in the case of violation of specific clauses in the agreement. Therefore, this section of research will attempt to identify the ESC of the cloud identity systems.

These characteristics would help both CIdUs and CIdPs understand the importance of these features that are worth considering when selecting or implementing the Cloud IAM. Moreover, PKI is a widely used mature technology that employs trust mechanisms to support, key certification and validation, digital signature, attribute certification and validation. But the question is, can the researcher apply trust ideas used in PKI to establish trust mechanisms to the cloud? Huang and Nicol (2013) identified and answered this question and say that this raises questions that ask about the foundation of trust, and how the trust is inferred or calculated.

ESC of Cloud Identity aims to highlight the major security, privacy and trust issues in existing cloud identity computing environments. The contributions can be summarised as surveying the most relevant privacy, security and trust issues that pose threats in current cloud identity computing environments; and analysing the ways that may be addressed to eliminate the potential threats. To sum up, this section has reviewed the main properties, which help in assessing the CIdPs operational trust. The following key points are summative of the issues arising:

Balancing: As the data in the CC increases quickly based on the customers' request, load balancing and scalability are one of the main challenges in the CC and crucial feature for the cloud customers. However, this feature aims to improve the cloud performance and user's satisfaction by providing automated, extensible, and flexible area. Therefore, it vital for the long-term success of a cloud balancing strategy by integrating high availability with security (Gopinath & Vasudevan, 2015).

Single Sign-on: Authentication across multiple vendors is one of the first issues to be solved in the Cloud area. The different barriers can limit SSO technology, regarding data protection, confidentiality, and privacy issues. SSO streamlines secure access into all applications and resources with one set of credentials, regardless cloud, mobile, web, and VPN resources. The result is an improved user experience and trust without tedious login procedures and high friction authentication workflows and user-friendly. SSO is a simple solution to user identity issues because since they are already authenticated, no password is required and because no password is required, there is no password for anyone to steal. It increases application adoption, employee productivity, and decreases helpdesk costs (Moreno-Vozmediano et al., 2013).

Lifecycle: The goal of cloud lifecycle management is to manage the dynamic nature of the cloud environment, accelerating provisioning, facilitating flexibility, and rapidly meeting the needs of the business. With the cloud lifecycle management solution, organisations can deliver flexible, customizable cloud services while maintaining a structured, controlled, and dynamic IT environment. Moreover, Iriberri and Leroy (2009) indicated the features that should be selected and gradually added depending on the type of community under development and the purpose of the community as shown in figure 4.16.

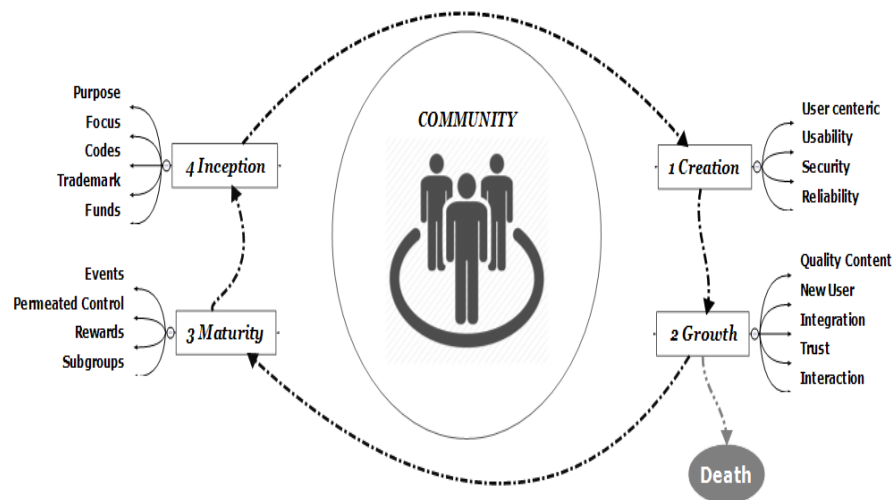


Figure 4.16: Online community life-cycle perspective (Iriberri & Leroy, 2009, p. 9).

Privacy: Identity management systems have existing services offering privacy and anonymity in a cloud environment for CIdUs (Khalid et al., 2013). Trust management, as well as efficient Cloud IAM and user keys, are required to achieve privacy. It is therefore difficult to design a system, which provides privacy and security to the sensitive CIdUs' data. As a result, there is a significant gap between CIDPs' claims and CIdUs' views of the cloud's privacy and security (Kshetri, 2013).

Risk: Among all the privacy and security issues, this section treats the challenges posed by identity management in the cloud, focusing on risk assessment. Federation as a vital feature of cloud and cloud identity needs strong integration, cooperation and collaboration among different clouds. Consequently, it introduces complex tasks in risk assessment to quantify CIdPs and investigate new metrics in the Cloud IAM (Arias-Cabarcos et al., 2012). Djemame et al. (2014) designed a risk assessment model and focused on a specific aspect of risk assessment applied in the CC, and they described the various stages in the service lifecycle whereas

risk assessment takes place. Theoharidou et al. (2013) examined privacy risk assessment for cloud and identify threats, vulnerabilities and countermeasures that clients and providers should implement to achieve privacy compliance and accountability.

Standards: Securing information and the systems that store, process, and transmit users' identity information is a challenging task for organisations. Standardized facilitates to collect, verify, and update system security configurations and they can work in concert or be implemented separately. It also would allow authentication automation.

There are six methods and standards that industry collaborates to make major progress in terms of mitigating identity theft and improving strong authentication. The first has Fast IDentity Online (FIDO) (Loutfi & Jøsang, 2015) to eliminate the password by strong authentication that is tight with the hardware. There is a need to keep working with fishing protection like Internet Engineering Task Force (IETF) (Zhu & Tung, 2015) and the Organization for the Advancement of Structured Information Standards (OASIS). Work for share intelligence and IP practically OpenID Connect Reduced Instruction Set Computing (OIDC-RISC) is important for the strong authentication. There are two new methods, token binding and session revocation. Token binding aims to mitigate impersonate a user identity by binding a token with hardware against man in the middle attack. CIdUs want to revoke all sessions and access tokens that have been handed out.

Eliminating Password: The FIDO and W3C (WebAuthn) could eliminate, or at least significantly mitigate the risk of passwords. The main goal of these standards is to define a client-side API that provides strong authentication functionality to Web Applications, therefore, it improves and simplifies the security of authentication. In this regards, the W3C is uniquely positioned to focus the attention of Web infrastructure providers and developers on the shortcomings of passwords While FIDO protocol employs public key cryptography (Jyotiyana & Mishra, 2016).

Phishing Protection: Phishing is a technique that involves users to steal confidential information and passwords by using email. Security Automation and Continuous Monitoring (SACM) that reuse existing protocols, mechanisms, information and data models. Also, IETF standards that could support automation

of asset, change, configuration, and vulnerability management. Three foundational cybersecurity specifications, Structured Threat Information Expression (STIX), Trusted Automated Exchange of Indicator Information (TAXII), and Cyber Observable Expression (CybOX), are now being advanced through the OASIS and they will support automated information analysis and share for cyber security situational awareness, real-time network defence, and sophisticated threat characterization and response. Security professionals are overwhelmed and simply do not have time for analysing data in disparate formats. STIX, TAXII, and CybOX streamline the process, putting the focus of cyber intelligence where it belongs. STIX is a language for describing cyber threat information so that it can be analysed and exchanged. TAXII defines services and message exchanges that enable organisations to share the information they choose with the partners they choose. CybOX is a language for specifying, capturing, and communicating events that are observable in the system and network operations (Alsharnouby et al., 2015).

Shared Intelligence and IP: The ability to react quickly to identity theft attacks will effectively stop the access of hackers before they take provider's and user's information. However, shared security and threat intelligence require a trusted community between providers. In this regard, the aim of the Risk and Incident Sharing and Coordination (RISC) is to provide privacy recommendations, protocols to Share information, and data sharing schemas to thwart attackers from leveraging compromised accounts from one CSP to another CSP (OpenID, 2016). Therefore, Shared intelligence and IP brings identity theft information to be represented in a standardised format (Leicher et al., 2012).

Token Binding: CIdPs generate various security tokens such as OAuth tokens for CIdUs to access cloud service providers. Attackers export bearer tokens from CIdU machines or compromised network connections, present these bearer tokens to Cloud Service Providers and impersonate authenticated users. Token Binding enables defence against such attacks by cryptographically binding security tokens to a secret held by the CIdU (W. Li & Mitchell, 2014).

Session Revocation: In terms of any CIdUs' system compromising, they want a way to revoke all sessions and access tokens that are handed out. It is important that any outstanding access tokens are not revoked by clicking Logout all, so, they have to expire naturally. Based on the OIDC standard, Revoke refresh token, SSO Session Idle, SSO Session Max, Offline Session Idle, Access Token

Lifespan, and client login timeout are matters of concern in cloud federated identity management systems (Yan et al., 2009).

Internet of Things: There are seemingly competing, complex security requirements to be deployed on the IoT platforms with potentially limited resources like authentication to multiple networks securely and provide strong authentication and data protection. Thus, IoT must be secure for its value to be realised. If we do not have the confidence of the IoT entity, then we cannot protect the potentially sensitive sensor data being shared or the transactions being conducted (Mahalle et al., 2013).

The CSA has established the IoT Working Group (WG) (Russell, 2016) to focus on providing relevant guidance to cloud users who are implementing IoT solutions. They aim to provide understandable recommendations to information technology staff charged with securely implementing and deploying IoT solutions considering IoT Identity and Access Management (IAM). Moreover, the ISO 27000 series of International Standards has standards for the protection of information and ICT. They include generic methods, techniques and guidelines to address both security and privacy aspects such as security in identity management, biometrics and privacy (Disterer, 2013).

4.7.3 Analysis

Based on the previous analysis, it is obvious that there are numerous benefits with using and adopting cloud such as but not limited to assure application availability, improve application performance, and implementing a strategic disaster recovery plan (Ruiz & Pedraza, 2016).

Aside from all advantages for the cloud, still there are numerous challenges associated with the implementation of such a strategy, some of which might take years to address for a strong, flexible foundation to enable customers to meet current technical and business goals (Lonea et al., 2013; Tormo et al., 2014). According to the critical analysis by (Gopinath & Vasudevan, 2015; Mathew et al., 2015) the main trust elements are techniques, dynamic management, algorithms, amount of data, energy consumption, , benchmark, scheduling, metrics to capture bottlenecks, response times, centralise, and decentralised system which has been shown in figure 4.17.

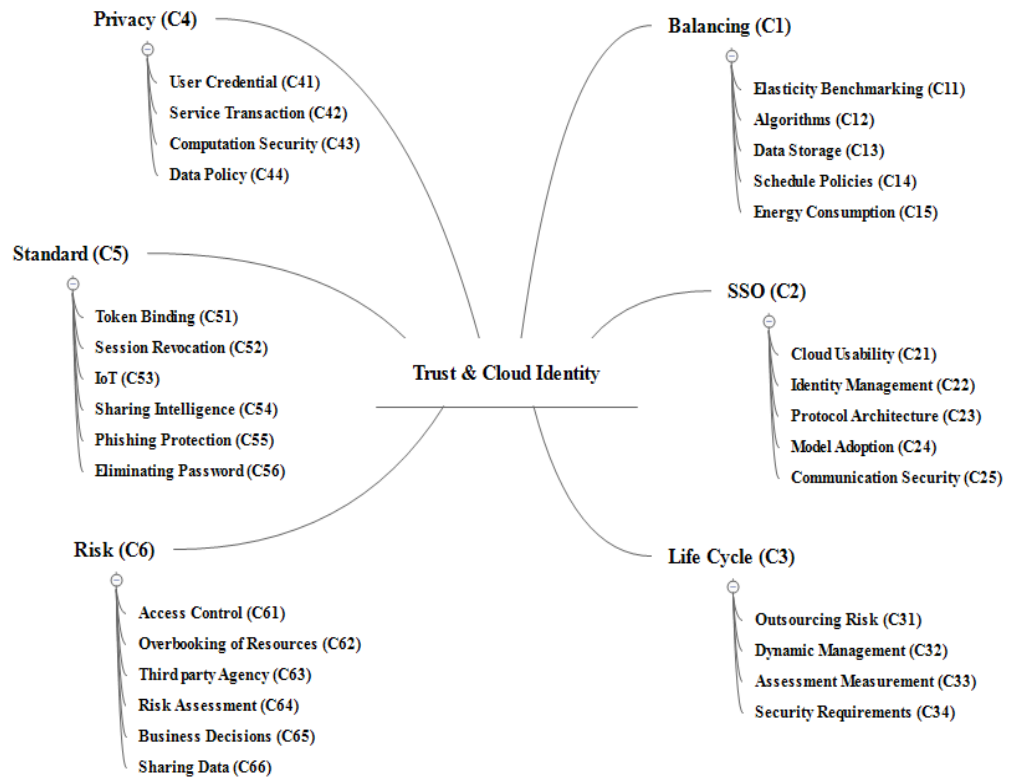


Figure 4.17: Cloud identity's ESC.

The research shows that cloud load balancing is in early stages. Moreover, having a standardised application delivery framework mitigates issues arising from operational differences across solutions and the CC environments.

Many SSO solutions also deliver a wide-ranging solution (one-time password, challenges for adopting, service hijacking, usability, global security network, mobile phone security, identity management, new architecture, security and privacy, challenges related log out, and identity theft) that covers both on-premises and cloud-based applications to eliminate the need for different credentials across multiple providers (Ghazizadeh, Manan, et al., 2012; Méndez et al., 2016).

The way the different systems exchange credentials and information is often based on one or more of the standards like SAML, OAuth and OpenID. Therefore, it is important to look at the portfolio of cloud-based solutions in use to determine the standard most commonly supported. There is risk from manually managing identities across the growing number of cloud-based applications which has is addressed in figure 4.17. Any cloud strategy today needs to include a strategy for SSO and identity management outside the corporate network and into the growing

landscape of cloud-based providers. With today's sensitivity around data, the wise decision is to leverage a cloud-based SSO and secure identity management solution.

IT organisations have relied on standards and guidelines from some organisations, including the Organization for the Advancement of Structured Information Standards (OASIS), NIST, Open Web Applications Security Project (OWASP), European Telecommunications Standards Institute (ETSI) and International Organization for Standardization (ISO). The main reason for these standards is addressing life cycle issues, including requirements, implementation, security, architectures, and deployment. According to the reviewed publication, we have identified main trust issues of life cycle associated with the CC both from a cloud provider and customer perspective. These categories include: dynamic nature, flexible, self-service, assessment on each phase, automated the usage, control and manage, migration to cloud, portable cloud, reusable management, traditional framework, privacy policy, deviation in coverage, revoke or changed, high level enterprises, and types of community (Breiter & Behrendt, 2009; Chou & Chou, 2009; Conway & Curry, 2012).

4.8 EVALUATION PROCESS

Lopez (2000) identified that the preparation process, examination process, and decision-making process are three essential processes for evaluation theory. However, the main aim of these activates, and tasks are solved the specific decision problem and identify the most relevant element to the target of the theory (ESC and ESA).

4.8.1 Preparation Process

It is the initial process that describes the basic parts of trust identity framework. In this step one, the evaluation target, evaluation criteria, and decision makers is identified:

- A set of A (ESA) called: $A = (A_1, A_2, \dots, A_i)$;
- A set of C (ESC) called: $C = (C_1, C_2, \dots, C_j)$;
- A set of Trust elements called: $T = (t_1, t_2, \dots, t_n)$;
- A set of U (CIdU) decision makers called: $U = (U_1, U_2, \dots, U_m)$;

4.8.2 Examination Process

The examination process of evaluating target based on evaluation criteria framework to identify and rank the ESA and ECA associated with cloud and cloud identity. Initially, this process started by gathering data regards each ECA and ESA using document review and guidelines which mentioned in 3.2.5. After checking the completeness of evaluation data and synthesis technique (3.2.6), the decision-making process is applied to achieve the evaluation goal.

4.8.3 Decision Making Process

The IPA as a multi-attribute model has been introduced by (Martilla & James, 1977). It helps this thesis to identify which evaluation criteria (ESA and ESC) associated with service providers that either CIdPs and CIdUs should focus on to make a best trust level and trust decision. Typically, IPA provides a graphical representation that shows evaluation criteria on importance and performance dimensions' matrix. IPA has been used in different studies (Alabool & Mahmood, 2015; Azzopardi & Nash, 2013; Lai & To, 2010; Lewis, 2004) for the purpose to provide analysis to allocate unimproved gaps between different services. The aim behind using IPA map in this thesis is to describe the providers' trust criteria that is associated with CIdUs in detail. IPA map is very helpful in deciding how best to make decisions between providers depending on evaluation criteria by determining the gap. In fact, IPA is a useful technique for evaluating the trust attributes, characteristics, and elements of CSPs and CIdPs for this research.

Table 4.10: IPA map ((Martilla & James, 1977), p. 2).

Weight	Quadrant 1 High Importance Low Performance	Quadrant 2 High Importance High Performance	Quadrant 1 Major weakness
	Quadrant 4 Low Importance Low Performance	Quadrant 3 Low Importance High Performance	Quadrant 2 Major Strength
			Quadrant 3 Minor strength
			Quadrant 4 Minor weakness
	Performance (Trust)		

Table 4.10 as a main part of IPA, demonstrates the relationship between performance (Trust) and the importance level of the attributes, characteristics, and elements. It also describes the level of concentration for these trust elements and they are prioritised based on analysis. These four quadrants describe different

interactions and achievements for determining and prioritising the ESAs and ESCs. According to the four quadrants are defined as follows:

Quadrant 1: This section (concentrate here) has the elements that rated as having high importance and low performance. On the other word, it represents elements that should be considered as top priority.

Quadrant 2: This section (keep up with good work) has the elements that rated as having high importance and high performance. It represents elements that should be considered with important priority for CIdPs.

Quadrant 3: This section (possible overkill) has the elements that rated as having low importance and high performance. On the other word, it represents elements that could be ignored for CIdPs.

Quadrant 4: This section (low priority) has the elements that rated as having low importance and low performance. On the other word, it represents elements that might be ignored for CIdPs trust evaluation. Therefore, ordering and prioritising the elements should emphasise elements in other quadrants.

The linguistic variable has been used in some research to define elements not defined by numbers (Tzeng & Huang, 2011). Therefore, linguistic variables with powerful characterisations motivated the researcher to utilise it much closer to human thinking, moreover, its ability to model the fuzziness or vagueness inherently in the human decision making (Alabool & Mahmood, 2015). Table 4.11 shows the linguistic variables for the important weight of criteria rates of alternatives against criteria.

Table 4.11: Linguistic variable for trust elements and their weighting

Elements Rating	Elements Weighting	Triangular Fuzzy Number
Very Essential (VE)	Very High (VH)	(0.9,1.0,1.0)
Essential (E)	High (H)	(0.7,0.9,1.0)
Fairly Essential (FE)	Fairly High (FH)	(0.5,0.7,0.9)
Fair (F)	Fair (F)	(0.3,0.5,0.7)
Fairly Inessential (FI)	Fairly Low (FL)	(0.1,0.3,0.5)
Inessential (I)	Low (L)	(0.0,0.1,0.3)
Very Inessential (VI)	Very Low (VL)	(0.0,0.0,0.1)

To determine the priority of ESA and ESC within CIdPs, IPA map, linguistic, table 4.12, and table 4.13 is used.

Table 4.12: ESC and trust elements

Characteristics Trust Elements		Balancing C_1	SSO C_2	Lifecycle C_3	Privacy C_4	Standard C_5	Risk C_6
Entities	Credibility		$C_{21}, C_{22},$	C_{31}, C_{34}	C_{41}	$C_{51},$	
	Privacy	C_{12}, C_{14}	$C_{22},$		C_{42}	C_{52}, C_{54}, C_{56}	$C_{61}, C_{63}, C_{65}, C_{66}$
	Personalization	C_{12}, C_{14}	C_{21}, C_{23}			C_{53}	C_{64}
	Integration	C_{13}	C_{22}	C_{32}, C_{33}		C_{51}, C_{53}	
	Security	C_{13}, C_{14}	C_{22}, C_{25}	C_{31}, C_{33}, C_3	C_{41}, C_{42}, C_{44}	C_{51}, C_{55}	$C_{61}, C_{62}, C_{63}, C_{66}$
Monitoring	Perspective	C_{11}, C_{15}	C_{21}, C_{23}				
	Technique	C_{11}	C_{22}, C_{23}	C_{33}	C_{42}, C_{43}	C_{51}, C_{56}	C_{64}
	Adaptability	C_{14}, C_{15}	$C_{21}, C_{22}, C_{23}, C_{23}$	C_{31}, C_{32}	C_{44}	C_{53}, C_{54}	C_{63}, C_{65}
	Security	C_{12}, C_{13}, C_{14}	C_{21}, C_{22}, C_{25}		C_{41}	C_{52}, C_{55}	C_{61}, C_{62}, C_{66}
	Scalability	C_{13}, C_{15}	$C_{21},$	C_{31}, C_{32}			
Computing	Response Time	C_{12}		C_{34}		C_{51}	C_{62}, C_{64}
	Redundancy	C_{11}, C_{13}	C_{22}, C_{24}	C_{32}		C_{52}	C_{66}
	Accuracy	C_{12}	C_{21}, C_{23}, C_{25}	C_{31}, C_{33}	C_{41}, C_{42}, C_{43}	C_{51}, C_{54}	C_{64}

These tables (Table 4.12 and 4.13) show the analysis techniques of this research to find the connectivity between trust elements, ESAs, and ESCs. This connectivity is used as a weight and performance parameters in the IPA model rather than checklists and interviews. In order to represent the relationship, ESAs and ESCs have been mapped to trust elements which have been found in the previous sections.

Performance and weight data have been gathered regarding either ESA (A) and ESC (C) with trust elements (T). Table 4.14 and 4.15 are used to investigate the importance of ESAs, ESCs, and trust elements for identifying the weight of the IPA. On the other hand, table 4.16 and 4.17 are used to investigate the performance of each ESAs and ESCs elements. All the connections which have been shown in the tables, are based on analysis and defining the relation between trust elements with respect to both content and context.

Table 4.13: ESA and trust elements

Frameworks Trust Elements		User observation A_1	Accreditation and Audit A_2	Self Assessment A_3	Monitoring and Benchmarking A_4	SLA A_5	Computational A_6
Entities	Credibility	A_{12}, A_{13}	$A_{21}, A_{22}, A_{23}, A_{24}$				A_{61}
	Privacy		$A_{21}, A_{22}, A_{32}, A_{24}$	$A_{31}, A_{32}, A_{33}, A_{34}$	A_{41}, A_{43}	A_{51}	$A_{61}, A_{62}, A_{64}, A_{66}$
	Personalization	A_{11}		A_{32}	A_{42}		
	Integration	A_{12}	A_{21}, A_{22}, A_{23}	A_{31}, A_{32}	A_{41}, A_{43}	A_{57}	A_{62}, A_{64}, A_{65}
	Security	A_{11}, A_{12}	$A_{21}, A_{22}, A_{23}, A_{24}$	$A_{31}, A_{32}, A_{33}, A_{34}$	A_{41}	A_{51}	$A_{61}, A_{62}, A_{63}, A_{64}$
Monitoring	Perspective	A_{14}			A_{44}	A_{52}, A_{54}	
	Technique	A_{13}		A_{31}, A_{34}	A_{41}	A_{51}, A_{52}	A_{61}, A_{64}
	Adaptability			A_{33}, A_{34}		A_{52}, A_{55}	A_{65}
	Security	A_{11}	A_{21}, A_{22}, A_{24}	$A_{31}, A_{32}, A_{33}, A_{34}$	A_{41}	A_{51}, A_{53}	A_{63}
	Scalability	A_{14}	A_{21}	A_{31}, A_{32}	A_{41}, A_{44}		
Computing	Response Time	A_{16}				A_{55}	
	Redundancy	A_{11}				A_{55}	
	Accuracy	A_{15}				$A_{53}, A_{54}, A_{56}, A_{57}$	A_{61}, A_{63}, A_{64}

Table 4.14: Importance of ESC and performance of ESC elements

Importance (Weight) (WC)	$C_1(21)$	$C_2(25)$	$C_3(16)$	$C_4(12)$	$C_5(18)$	$C_6(19)$
Performance (Connectivity)	$C_{11}(3), C_{12}(5), C_{13}(5), C_{14}(5), C_{15}(3)$	$C_{21}(7), C_{22}(8), C_{23}(5), C_{24}(2), C_{25}(3)$	$C_{31}(5), C_{32}(4), C_{33}(4), C_{34}(3)$	$C_{41}(4), C_{42}(4), C_{43}(2), C_{44}(2)$	$C_{51}(6), C_{52}(3), C_{53}(3), C_{54}(3), C_{55}(2), C_{56}(2)$	$C_{61}(3), C_{62}(3), C_{63}(3), C_{64}(4), C_{65}(2), C_{66}(4)$

Table 4.15: Importance of ESA and performance of ESA elements

Importance (Weight) (WA)	$A_1(6)$	$A_2(19)$	$A_3(21)$	$A_4(11)$	$A_5(17)$	$A_6(18)$
Performance (connectivity)	$A_{11}(4), A_{12}(3), A_{13}(2), A_{14}(3), A_{15}(1), A_{16}(1)$	$A_{21}(6), A_{22}(5), A_{23}(4), A_{24}(4)$	$A_{31}(6), A_{32}(6), A_{33}(4), A_{34}(5)$	$A_{41}(5), A_{42}(1), A_{43}(2), A_{44}(2)$	$A_{51}(4), A_{52}(3), A_{53}(2), A_{54}(2), A_{55}(3), A_{56}(1), A_{57}(2)$	$A_{61}(5), A_{62}(3), A_{63}(3), A_{64}(5), A_{65}(2), A_{66}(1)$

The weight of the ESC connection (WC) and Weight of the ESA connection (WA) show the number connectivity of ESA and ESC elements with trust elements and is used as a weight parameter in the IPA model. The second parameter which is performed is based on the rate of characteristics and attributes within trust elements.

Next step is using the linguistic terms as shown in the table 4.11 for assessing both important fuzzy weight of ESC and ESA, and also for assessing the performance ratings of ESC's elements and ESA's elements. Table 4.16 and table 4.17 are the summaries of the analysis elements based on the linguistic terms.

Table 4.16: Fuzzy linguistic of ESC.

Importance (Weight) (WC)	$C_1(0.7,0.9,1.0)$	$C_2(0.9,1.0,1.0)$	$C_3(0.1,0.3,0.5)$	$C_4(0.0,0.1,0.3)$	$C_5(0.3,0.5,0.7)$	$C_6(0.5,0.7,0.9)$
Performance Connectivity	$C_{11}(0.0,0.1,0.3)$ $C_{12}(0.9,1.0,1.0)$ $C_{13}(0.7,0.9,1.0)$ $C_{14}(0.5,0.7,0.9)$ $C_{15}(0.1,0.3,0.5)$	$C_{21}(0.7,0.9,1.0)$ $C_{22}(0.9,1.0,1.0)$ $C_{23}(0.3,0.5,0.7)$ $C_{24}(0.0,0.0,0.1)$ $C_{25}(0.0,0.1,0.3)$	$C_{31}(0.9,1.0,1.0)$ $C_{32}(0.5,0.7,0.9)$ $C_{33}(0.3,0.5,0.7)$ $C_{34}(0.0,0.1,0.3)$	$C_{41}(0.9,1.0,1.0)$ $C_{42}(0.5,0.7,0.9)$ $C_{43}(0.1,0.3,0.5)$ $C_{44}(0.0,0.0,0.3)$	$C_{51}(0.9,1.0,1.0)$ $C_{52}(0.7,0.9,1.0)$ $C_{53}(0.3,0.5,0.7)$ $C_{54}(0.5,0.7,0.9)$ $C_{55}(0.1,0.3,0.5)$ $C_{56}(0.0,0.1,0.3)$	$C_{61}(0.5,0.7,0.9)$ $C_{62}(0.1,0.3,0.5)$ $C_{63}(0.3,0.5,0.7)$ $C_{64}(0.9,1.0,1.0)$ $C_{65}(0.0,0.0,0.1)$ $C_{66}(0.7,0.9,1.0)$

Defuzzification (Zimmermann, 2012) is the process that converts the fuzzy numbers (Table 4.16, Table 4.17) which represent the linguistic terms, to crisp value (Table 4.18, Table 4.19). Centre of Area (CoA) (Samuel et al., 2013) method is the used method in this section because it does not suffer from ambiguity and can work in any situation (Alabool & Mahmood, 2015). Therefore, this study aims to adopt the type of a CoA method in order to de-fuzzified (Table 4.16 and 4.17) triangular fuzzy number to find best Non-Fuzzy Connectivity Value (NCV) of the table 4.16 and table 4.17 fuzzy value. Based on these two tables, fuzzy triangular numbers parametrised by $(F_1^{Low}, F_2^{Medium}, F_3^{High})$.

$$NCV = [(F_3^{High} - F_1^{Low}) + (F_2^{Medium} - F_1^{Low})]/3 + F_1^{Low} \quad (4.1)$$

Table 4.17: Fuzzy linguistic of ESA.

Importance (Weight) (WA)	$A_1(0.0,0.1,0.3)$	$A_2(0.7,0.9,1.0)$	$A_3(0.9,1.0,1.0)$	$A_4(0.1,0.3,0.5)$	$A_5(0.3,0.5,0.7)$	$A_6(0.5,0.7,0.9)$
Performance Connectivity	$A_{11}(0.9,1.0,1.0)$ $A_{12}(0.7,0.9,1.0)$ $A_{13}(0.3,0.5,0.7)$ $A_{14}(0.5,0.7,0.9)$ $A_{15}(0.0,0.1,0.3)$ $A_{16}(0.0,0.0,0.1)$	$A_{21}(0.9,1.0,1.0)$ $A_{22}(0.7,0.9,1.0)$ $A_{23}(0.3,0.5,0.7)$ $A_{24}(0.5,0.7,0.9)$	$A_{31}(0.9,1.0,1.0)$ $A_{32}(0.7,0.9,1.0)$ $A_{33}(0.1,0.3,0.5)$ $A_{34}(0.5,0.7,0.9)$	$A_{41}(0.9,1.0,1.0)$ $A_{42}(0.1,0.3,0.5)$ $A_{43}(0.5,0.7,0.9)$ $A_{44}(0.7,0.9,1.0)$	$A_{51}(0.9,1.0,1.0)$ $A_{52}(0.5,0.7,0.9)$ $A_{53}(0.1,0.3,0.5)$ $A_{54}(0.0,0.1,0.3)$ $A_{55}(0.7,0.9,1.0)$ $A_{56}(0.0,0.0,0.1)$ $A_{57}(0.3,0.5,0.7)$	$A_{61}(0.7,0.9,1.0)$ $A_{62}(0.5,0.7,0.9)$ $A_{63}(0.3,0.5,0.7)$ $A_{64}(0.9,1.0,1.0)$ $A_{65}(0.1,0.3,0.5)$ $A_{66}(0.0,0.1,0.3)$

Table 4.18: Defuzzification of ESC.

Importance (Weight) (WC)	$C_1(0.86)$	$C_2(0.96)$	$C_3(0.3)$	$C_4(0.13)$	$C_5(0.5)$	$C_6(0.7)$
Performance Connectivity (C)	$C_{11}(0.13)$ $C_{12}(0.96)$ $C_{13}(0.86)$ $C_{14}(0.7)$ $C_{15}(0.3)$	$C_{21}(0.86)$ $C_{22}(0.96)$ $C_{23}(0.5)$ $C_{24}(0.03)$ $C_{25}(0.13)$	$C_{31}(0.96)$ $C_{32}(0.7)$ $C_{33}(0.5)$ $C_{34}(0.13)$	$C_{41}(0.96)$ $C_{42}(0.7)$ $C_{43}(0.3)$ $C_{44}(0.13)$	$C_{51}(0.96)$ $C_{52}(0.86)$ $C_{53}(0.5)$ $C_{54}(0.7)$ $C_{55}(0.3)$ $C_{56}(0.13)$	$C_{61}(0.7)$ $C_{62}(0.3)$ $C_{63}(0.5)$ $C_{64}(0.96)$ $C_{65}(0.03)$ $C_{66}(0.86)$

Table 4.19: Defuzzification of ESA.

Importance (Weight) (WA)	$A_1(0.13)$	$A_2(0.86)$	$A_3(0.96)$	$A_4(0.3)$	$A_5(0.5)$	$A_6(0.7)$
Performance Connectivity (C)	$A_{11}(0.96)$ $A_{12}(0.86)$ $A_{13}(0.5)$ $A_{14}(0.7)$ $A_{15}(0.13)$ $A_{16}(0.03)$	$A_{21}(0.96)$ $A_{22}(0.86)$ $A_{23}(0.5)$ $A_{24}(0.7)$	$A_{31}(0.96)$ $A_{32}(0.86)$ $A_{33}(0.3)$ $A_{34}(0.7)$	$A_{41}(0.96)$ $A_{42}(0.3)$ $A_{43}(0.7)$ $A_{44}(0.86)$	$A_{51}(0.96)$ $A_{52}(0.7)$ $A_{53}(0.3)$ $A_{54}(0.13)$ $A_{55}(0.86)$ $A_{56}(0.03)$ $A_{57}(0.5)$	$A_{61}(0.86)$ $A_{62}(0.7)$ $A_{63}(0.5)$ $A_{64}(0.96)$ $A_{65}(0.3)$ $A_{66}(0.13)$

Equation 4.1 is used to convert the linguistic terms into fuzzy triangular numbers and aggregating fuzzy weight of ESAs and ESCs. Moreover, Equation 4.1 is used aggregating fuzzy connectivity ratings of ESA's elements and ESC's elements.

The next step is using Simple Additive Weight (Churchman & Ackoff, 1954) to handle the problem of trust element selection. This method as an MCDM method is the best, widely, and most popular method because of its uncomplicatedness and capability to prioritise attributes, characteristics, and elements (Tzeng & Huang, 2011). The fundamental principle of the SAW is to compute a weighted sum of the connectivity (Performance) ratings of each group of criteria under a specific category, which can be derived from equation 2 and 3.

According to table 4.18 and table 4.19, in order to rank the trust elements of ESC and ESA; the Connectivity Rate (CR) has been obtained by applying SAW method. Equations 4 and 5 are suitable for more than two tables and is used later when the number (chapter five and six).

$$\text{Number of ESC} = m;$$

$$\text{Number of ESA} = n;$$

$$CR = w_{A_j} * C_{A_j} \quad j=1,2,\dots, n \quad (4.2)$$

$$CR = w_{C_i} * C_{C_i} \quad i=1,2,\dots,m \quad (4.3)$$

$$\text{Average CR} = \frac{\sum_{k=1}^i w_{A_k}}{n} \quad (4.4)$$

$$\text{Average CR} = \frac{\sum_{k=1}^j w_{c_k}}{m} \quad (4.5)$$

Table 4.20: Weight and connectivity rate for elements of ESA and ESC.

ESA			ESC		
Elements	Weight	CR	Elements	Weight	CR
A_{11}	0.13	0.1248	C_{11}	0.86	0.1118
A_{12}	0.13	0.1118	C_{12}	0.86	0.8256
A_{13}	0.13	0.065	C_{13}	0.86	0.7396
A_{14}	0.13	0.091	C_{14}	0.86	0.602
A_{15}	0.13	0.0169	C_{15}	0.86	0.258
A_{16}	0.13	0.0039	C_{21}	0.96	0.8256
A_{21}	0.86	0.8256	C_{22}	0.96	0.9216
A_{22}	0.86	0.7396	C_{23}	0.96	0.48
A_{23}	0.86	0.43	C_{24}	0.96	0.0288
A_{24}	0.86	0.602	C_{25}	0.96	0.1248
A_{31}	0.96	0.9216	C_{31}	0.3	0.288
A_{32}	0.96	0.8256	C_{32}	0.3	0.21
A_{33}	0.96	0.288	C_{33}	0.3	0.15
A_{34}	0.96	0.672	C_{34}	0.3	0.039
A_{41}	0.3	0.288	C_{41}	0.13	0.1248
A_{42}	0.3	0.09	C_{42}	0.13	0.091
A_{43}	0.3	0.21	C_{43}	0.13	0.39
A_{44}	0.3	0.258	C_{44}	0.13	0.0169
A_{51}	0.5	0.48	C_{51}	0.5	0.48
A_{52}	0.5	0.35	C_{52}	0.5	0.43
A_{53}	0.5	0.15	C_{53}	0.5	0.25
A_{54}	0.5	0.065	C_{54}	0.5	0.35
A_{55}	0.5	0.43	C_{55}	0.5	0.15
A_{56}	0.5	0.015	C_{56}	0.5	0.065
A_{57}	0.5	0.25	C_{61}	0.7	0.49
A_{61}	0.7	0.602	C_{62}	0.7	0.21
A_{62}	0.7	0.49	C_{63}	0.7	0.35
A_{63}	0.7	0.35	C_{64}	0.7	0.672
A_{64}	0.7	0.672	C_{65}	0.7	0.021
A_{65}	0.7	0.21	C_{65}	0.7	0.602
A_{66}	0.7	0.091			

According to the results which have been shown in table 4.20, based on equation 4.4 and equation 4.5, the dataset of CR and weight is used to build an IPA map for prioritising the elements of ESC and ESA. To specify the analysis, SPSS Statistics application has been used. Figure 4.18 and figure 4.19 show the modified and revised IPA map which categorises the elements into four quadrants as shown in these figures (4.18 and 4.19).

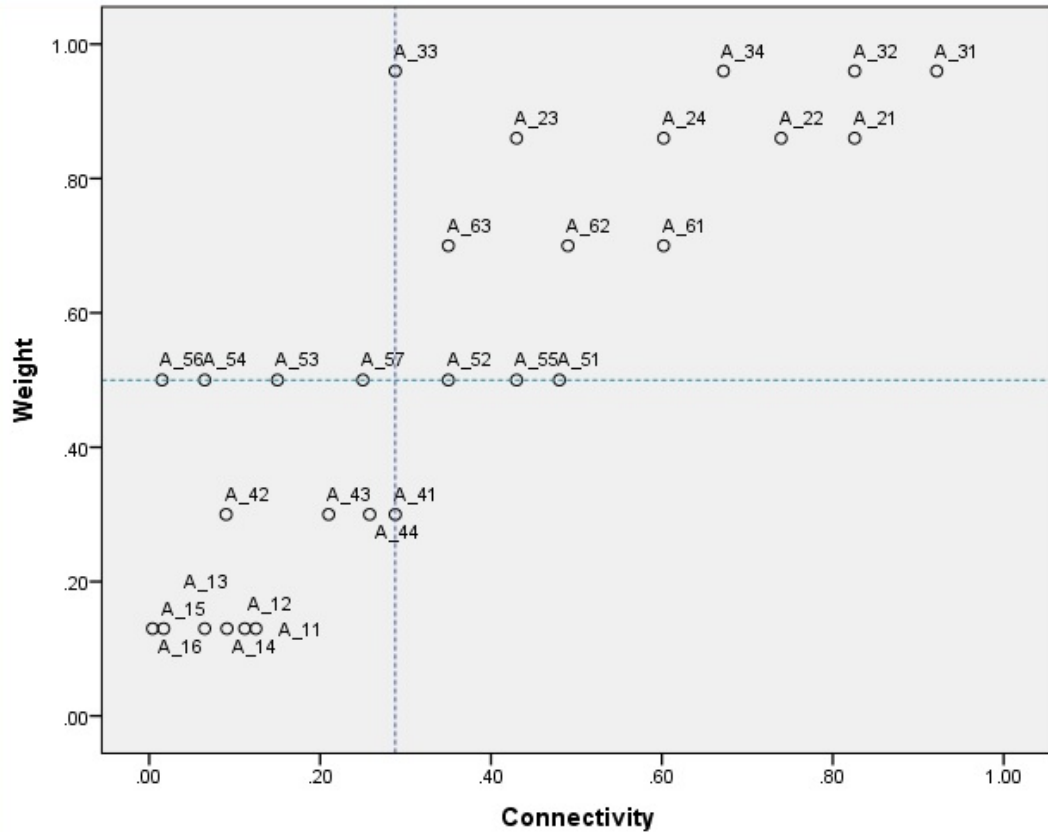


Figure 4.18: Modified IPA map for ESA.

4.8.4 Discussion and Analysis of The Result

On the basis of results shown in Table 4.20, the CR of ESC and ESA and the ideal (set to Median) point (ESA (0.288,0.5) and ESC (0.288,0.7) in each of them have been presented in figures 4.18 and 4.19. It can be observed that majority of elements are in the quadrant two (High Performance (Connectivity) and High Importance (Weight)), also, the poor area is quadrant four (Low Performance (Connectivity) and Low Importance (Weight)). Therefore, this research should give more attention to quadrant two and less attention to quadrant four regarding the selection of trust elements.

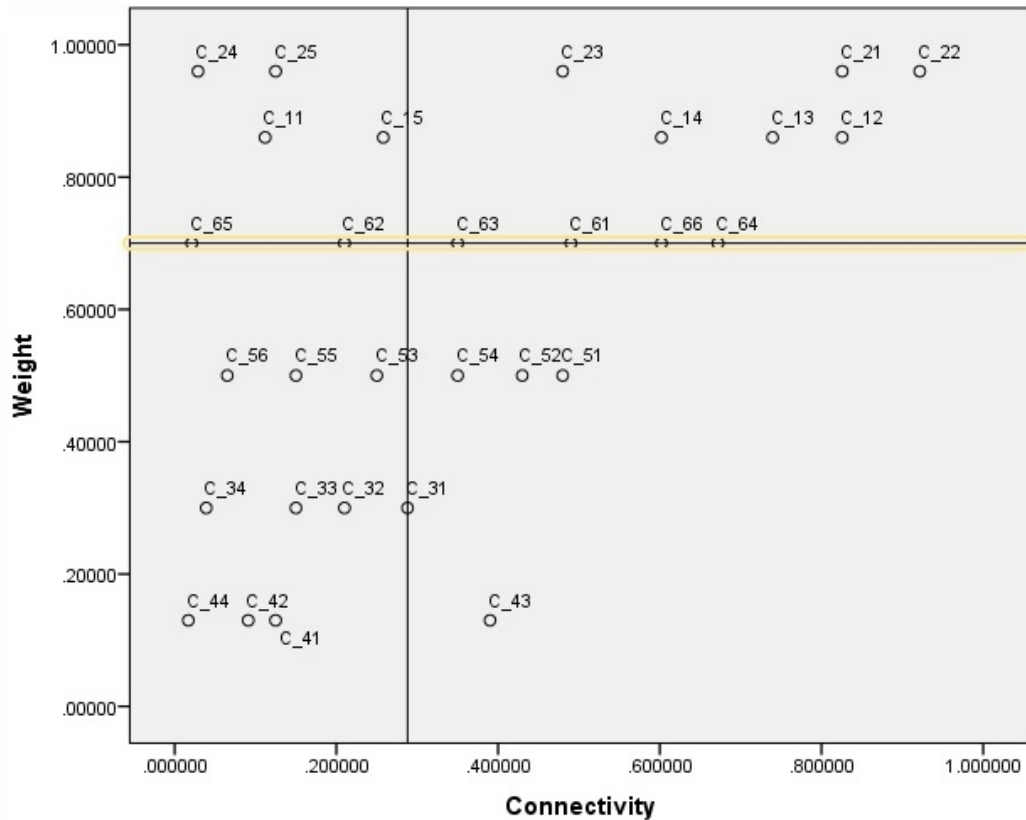


Figure 4.19: Modified IPA Map for ESC.

Quadrant one (Major Weakness) (ESA): Custom Algorithm (A (56)), Quality of Service (A (54)), Quality of Protection (A (53)), and Accurate SLA (A (57)) are the elements which are located in quadrant one. Elements that fell into this quadrant have high importance (weight) and low connectivity (CR) which make it the second priority that needs to be considered as a trust element in term of benchmarking the trust level of any CIdPs. However, the majority of SLA elements have fallen in this area.

Quadrant one (Major Weakness) (ESC): SSO Model Adoption (C (24)), SSO Communication Security (C (25)), Balancing Elasticity Benchmarking (C (11)), Balancing Energy Consumption (C (15)), Risk Business Decision (C (65)), Risk Overbooking of Resources (C (62)) are the elements which are located in quadrant one. Elements that fell into this quadrant have high importance (weight) and low connectivity (CR) which make it the second priority that needs to be considered as a trust element in term of benchmarking the trust level of any CIdPs. However, the majority of SSO, Balancing, and Risk elements have fallen in this area.

Quadrant two (Major Strength) (ESA): NIST 7874 (A (33)), Cloud Trust (A (34)), SMI (A (32)), CAIQ (A (31)), FISMA (A (23)), ISO (A (24)), SAS 70 II (A (22)), CSA (A (21)), Security (A (63)), Authentication (A (62)), Risk (A (61)), Monitoring SLA (A (52)), Dynamic SLA (A (55)), and Traditional SLA (A (51)) are the elements which are located in quadrant two. Elements that fell into this quadrant have high importance (weight) and high connectivity (CR) which make it the top priority that need to be considered as a trust element in term of benchmarking the trust level of any CIdPs. Identity cloud provider should put more attention to improve their service with respect to these elements. Similarly, more improvement is necessary for these elements. However, CIdP needs a great improvement to bring all other criteria into this quadrant.

Quadrant two (Major Strength) (ESC): Protocol Architecture (C (23)), Cloud Usability (C (21)), Identity Management (C (22)), Schedule Policy (C (14)), Data Storage (C (13)), Algorithm (C (12)), Third Party Agency (C (63)), Access Control (C (61)), Risk Sharing Data (C (66)), and Risk Assessment (C (64)) are the elements which are located in quadrant one. Elements that fell into this quadrant have high importance (weight) and high connectivity (CR) which make it the top priority that need to be considered as a trust element in term of benchmarking the trust level of any CIdPs. Identity cloud provider should put more attention to improve their service with respect to these elements. Similarly, more improvement is necessary for these elements. However, CIdP needs a great improvement to bring all other criteria into this quadrant.

Quadrant three (Minor Strength) (ESA): Monitoring and Benchmarking High Level (A (41)) is the only one element which is located in this quadrant. Elements that fell into this quadrant have low importance (weight) and high connectivity (CR) which make it the third priority that needs to be considered as a trust element in term of benchmarking the trust level of any CIdPs. Moreover, Monitoring and Benchmarking are in this area.

Quadrant three (Minor Strength) (ESC): Standard Sharing Intelligence (C (54)) Token Binding (C (51)), Session Revocation (C (52)), Outsourcing Risk (C (31)), Computation Security (C (43)) are the elements which are located in this quadrant. Elements that fell into this quadrant have low importance (weight) and high connectivity (CR) which make it the third priority that needs to be considered

as a trust element in term of benchmarking the trust level of any CIdPs. Moreover, the majority of Standard and Privacy have been fallen in this area.

Quadrant four (Minor Weakness) (ESA): Monitoring Low Level (A (42)), Computational Based (A (43)), Network-Based (A (44)), Direct Trust (A (11)), Indirect Trust (A (12)), Reputation (A (13)), User Observation (A (14)), Similarity (A (15)), and TEMRT (A (16)) are the elements which are located in this quadrant. Elements that fell into this quadrant have low importance (weight) and low connectivity (CR) which make it the lowest priority that needs to be considered as a trust element in term of benchmarking the trust level of any CIdPs. Moreover, the majority of Monitoring and User Observation elements have fallen in this area.

Quadrant four (Minor Weakness) (ESC): Standard Eliminating password (C (56)), Phishing Protection (C (55)), Internet of Things (C (53)), Life Cycle Security Requirement (C (34)), Assessment Measurement (C (33)), Dynamic Management (C (32)), Privacy Data Policy (C (44)), Service Transaction (C 942)), and User Credential (C (41)) are the elements which are located in this quadrant. Elements that fell into this quadrant have low importance (weight) and low connectivity (CR) which make it make it the lowest priority that needs to be considered as a trust element in term of benchmarking the trust level of any CIdPs. Moreover, the majority of Standard, Lifecycle, and Privacy have been fallen in this area.

These results could lead to some key points; firstly, although CIdPs should show the capability to offer the capability of the trust characteristics. Moreover, they have to ensure subjective trust elements such as Self Assessments, Accreditation, SSO, Balancing, Risk, and Computational Framework, which are very important to overcome trust concern of CIdUs. ESA, ESC, and their elements proved (based on the literature) their ability to provide a sufficient set of trust evaluation criteria that cover many different valuable identity assets. This framework, however, has some limitations for use because usually the IPA model is based on the gathering information from different resources. Therefore, in the use requires involving as much as possible participants (Questionnaires, Interview, Usability, and guidelines).

In this chapter, the researcher came to this point that trust has to be made measurable, in order to represent it in decision-making contexts on both commercial and technical trust elements. In the self-assessment section, the researcher identified that transparency is the main feature for the cloud and is to be one of the main

factors for trust. Therefore, it is been proposed the unified trust evaluation framework to address the difficulties of the analysed trust framework as well as integrating some parts of their features.

4.9 CONCLUSION

In conclusion, this chapter has provided a justification for the selection of the literature for this thesis based on the evaluation theory to identify the most relevant trust elements. Figure 4.3 is the chapter pathway, so, as the figure shows there are steps from problem identification to solution design (figure 4.1).

- **Target:** A target which means the element under evaluation provides information about what the element is and presents a general description of the objective domains and functions. Therefore, in this chapter trust elements for CIdPs has been selected to be the object under evaluation.
- **Criteria:** There are two main questions for this section (how to find most relevant ESA and ESC) which identify the criteria for this chapter. Therefore, trust elements of the CIdP and CSPs that are to be evaluated are the criteria. Figure 4.5 depicted the proposed trust framework architecture and its element (trust elements). However, entities, monitoring, and computing are three main elements for the trust elements (figure 4.6).
- **Yardstick or standard:** It is important to define the ideal target. However, in this chapter the trust framework for the cloud identity area is the main target. Therefore, the yardstick is defined as the trust identity management framework.
- **Data-gathering techniques:** Trust framework and past experience are two critical or systematic literature reviews used to obtain data to analyse each criterion for this chapter.
- **Synthesis techniques:** Framework synthesis and critical interpretive synthesis are referring to a set of relative activities and stages to synthesize all information and data which are essential for trust elements and elaboration in order to evaluate CIdP against these elements.
- **Evaluation process:** preparation process, examination process, and decision making process are three unique methods to solve the specific decision problem and identify the most relevant element to the target of the theory.

In addition, these processes show that there is a need to consider questions of trust level of any CIdPs. First, which attributes and characteristics should be selected for

trust level measurement (figure 4.14 and 4.17 the attributes and characteristics)?

Moreover, the following questions require answer:

- How is the value of each attribute determined?
- Which algorithm should be applied for determining trust level?
- How to get the received result?
- How to disseminate to the CIdUs and CSCs?

To answer these questions, an evaluation theory finds a set of trust criteria under fuzzy and complex environments for effectively evaluating and prioritising trust elements. The relevant weight of ESA, ESC, and their elements and the rating have been identified in section 4.7.

Therefore, based on the result in this chapter, in chapter five, the researcher will start with implementing the trust artefact to measure the most relevant trust elements by using a computational trust framework (you cannot control while you cannot measure). Therefore, it is obvious that after identifying the elements, measuring these elements are the challenge. Therefore, in chapter five, based on the figure 4.1, formulation, aggregation of the current measurement methods, and usability checking are the main criteria which will be presented in the chapter five.

Chapter Five

Implementation and Usability Study

5.0 INTRODUCTION

The objective of this chapter is to ensure applicability in practice as well as to improve the method's quality by including solutions to problems encountered in trust and reputation. The implemented of the trust management system is developed to assess the assertions of the framework and to evaluate CIdPs based on the ESA and ESC. Therefore, chapter five is devoted to the implementation and usability study of the proposed artefact trust management system in the distributed and highly dynamic environments of cloud identity.

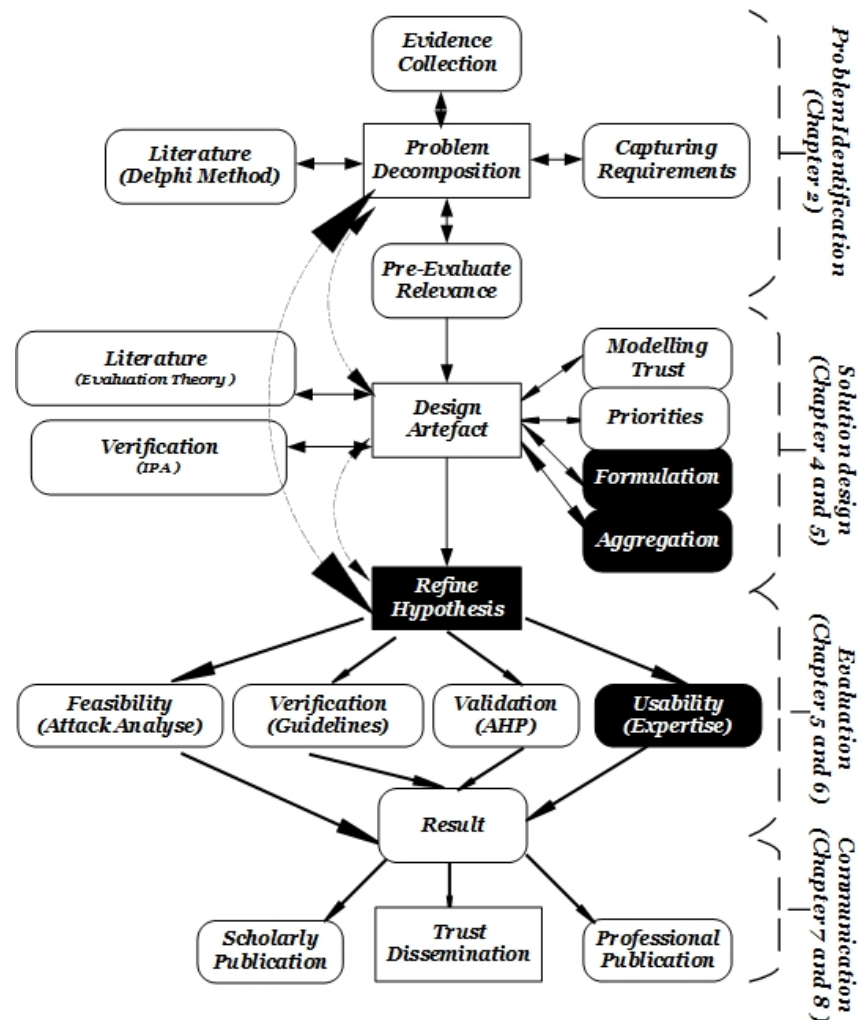


Figure 5.1: Chapter five Pathway

Figure 5.1 is the summary of the thesis based on the proposed methodology which has been presented in chapter three, so, the highlighted are is the main scope for

this chapter to step forward to solution design and evaluation. The approach is to clarify the pathway and roadmap of the thesis by highlighting (black areas) the particular steps and sub steps to reach the main objective (mitigate identity theft). Therefore, in the solution design step, this chapter is analysing the method to measure the trust elements of the previous chapter. Formulation and aggregation of the current methods are two main methods for measuring the trust elements. However, identifying the usability of the artefact is another concern addressed. Therefore, these techniques are implemented inside the Trust Cloud Identity Provider Framework (TCIdPF). The TCIdPF aims to provide a comprehensive platform for the trust-based recommendation of cloud identity services and knowledge-based decision-making support. To validate the usability and benefit of the approach, extensive experimental and performance studies of the proposed techniques using a collection of real-world trust frameworks in the cloud ((ESA) and (ESC)) are conducted.

First, based on the existing trust frameworks, a set of formula to present the level of trust for any CIdPs is analysed. The trust level results offer an overall view of the current trust status of CIdPs. Second, by studying the effectiveness in distinguishing feedback from expert people (Real CIdUs and cloud identity customers), the usability of the application has been evaluated.

This chapter is structured as follows: in section 5.1 the application architecture has been elaborated followed by section 5.2 which demonstrates the application workflow. In section 5.3 the overview of the implemented application has been explained followed by section 5.4 formulation for the trust evaluation. The first evaluation method based on the thesis methodology is conducting in the section 5.5, expert usability evaluation. This section has two main sub-sections, ethics and privacy which explain the ethical approval process for this thesis, and critical reflection on the expert's evaluation results. This chapter is concluded by summarising the key points achieved and the linkages to other chapters.

5.1 APPLICATION ARCHITECTURE

In this section, the application architecture of Trust Evaluation Model and its objects is presented. The trust evaluation model acts as a trusted third party that evaluates the trust of CSPs and provides the required trust credentials on receiving the trust requests from CSPs participating in the federation. Previous trust

frameworks are defined vaguely because they cannot commit to a certain type of technology, protocols, and services (Habib et al., 2012; Noor et al., 2016; Shaikh & Sasikumar, 2015). However, cloud users need to see a transparent trust level of CIdPs by TCIdPF to prevent or mitigate identity theft. TCIdPF provides a technical environment where consumers (Providers and Customers) can customise the level of trust and request trust assessment for a particular CIdPs.

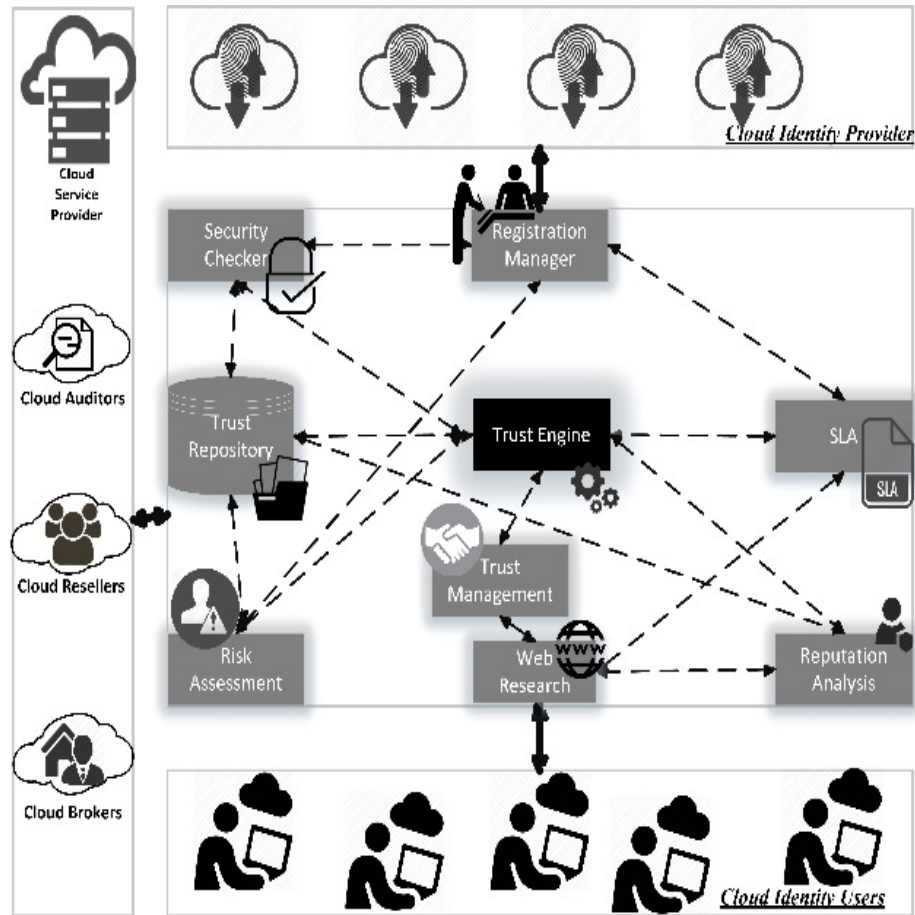


Figure 5.2: Architecture of the CIdP's Trust Framework

This framework is based on clearly defined and simple measurement assumptions. In addition, this high-level architecture is based on object-oriented architecture to deliver trust as a service to CIdUs because it must be able to manage and verify a large number of resources and do so effectively and efficiently. This has to be achieved through short measurement times and fast warning systems, able to quickly spot and report performance. It ensures an integrated view for building and evaluating trust based on the provider and user's information. The main aim of any trust management is to bring the capabilities for trustors to make evaluation and decisions regarding the dependability of the trustees with the trust elements.

Figure 5.2 shows the conceptual structure of the novel trust model with the individual parameters elaborated and their relation to other CIdPs and consumers. It also shows the design overview of a trust system and shows the location of each of the fundamental dimensions. The overarching goal of this framework is to produce a metric encapsulating trust for better decision making for each identity user within the cloud identity system.

The trust framework receives input from various types of sources. Based on these inputs, a system produces a metric by using a calculation algorithm. Once calculated, metric values are then disseminated throughout the system in advance or on demand as the metric values are requested by the service provider. Finally, higher-level systems or users can then utilize these metric trust values in their decision-making processes to achieve the goals of the assessment risk of using an identity provider. The framework consists of nine components, namely the security checker, Trust repository, Registration manager, Trust engine, SLA, Trust management, Risk assessment, Web research, and Reputation analysis.

5.2 APPLICATION WORKFLOW AND MODELLING TRUST

As with large-scale cloud identity environment, it is necessary to come up with an overview of trust relationships among providers and users. Statistical results of the trust level, such as average trust level and the structure of trust, to some extent, indicate the quality of services. In this section, a general workflow of trust evaluation application is presented for large-scale cloud identity, which not only obtains the overall trust level of the CIdPs but also builds a trust framework from the user's feedback using the proposed algorithm. The overall workflow for the application is depicted in figure 5.3. Based on this figure, the first step starts with CIdP registration. CIdP and their primary customers register with the Registration Manager module and submit the required data, which includes Risk assessment, Consensus Assessment, Identity Access Management Standard, Security Protocols, and SLAs of CIdPs. Next, the collected SLAs are submitted to the SLA module. A list of protocols sent to Security Checker module and a risk assessment form is sent to Risk Assessment module.

CIdUs submit their weight for attributes and will submit their feedback for CIdPs regarding the usability of the providers. Next, User feedback is sent to the Reputation Analysis module to calculate the CIdP's reputation. In step five, Reputation Analysis module checks the previous CIdP's data that they have in Trust Repository module. After processing data in all modules, the results will send to Trust Engine to make a knowledgeable data. Because of cloud identity consumers' requirements, Trust Engine checks the requirement (Weight) of the users in step seven. Next, in step eight, the Trust Engine evaluates and combines all trust values and calculates the final aggregated trust value regarding cloud identify users' decision making. The Trust Repository forwards the particular data to the Trust Engine module whenever it receives a request from this module. Finally, the trust score and trust level are presented to CIdU to make knowledgeable trust decision making.

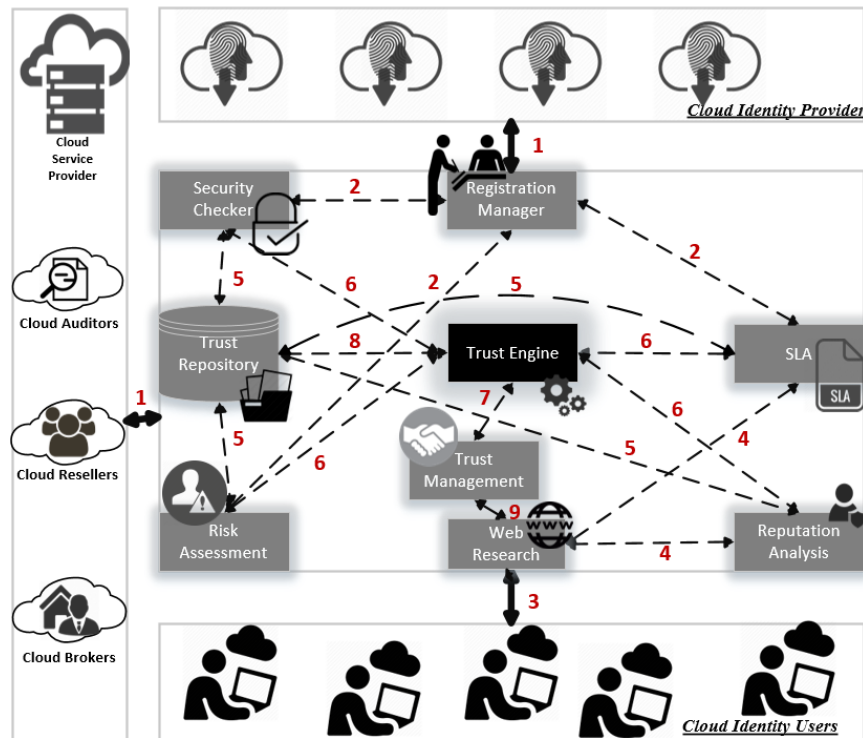


Figure 5.3: Cloud Identity Trust Decision-Making Workflow

5.3 TCIDPF APPLICATION OVERVIEW

The application is responsible for collecting providers and users trust information. The research application is developed based on the Amazon Web Services (AWS) and free open-source content management system (CMS) (WordPress), Windows 2012 r2, Hypertext Pre-processors (PHP) and open-source Relational Database

Management System (MySQL) and Internet Information Server (IIS). AWS is a secure cloud services platform, offering computing power, database storage, content delivery and other functionality to help businesses scale and grow. Nowadays, millions of customers are currently leveraging AWS cloud products and solutions to build sophisticated applications with increased flexibility, scalability and reliability (Kim et al., 2016). In this regard, WordPress, PHP, Database and IIS are installed on the AWS windows 2012 r2 instance. WordPress is reportedly the most popular website management or blogging system in use on the Web, supporting more than 60 million websites in the world (West, 2016). Furthermore, PHP is a widely used open source general-purpose scripting language that is especially suited for web development and can be embedded into Hypertext Markup Language (HTML) (Bashir et al., 2016). In addition, MySQL is a central component of the (Linux Apache) open-source web application software Stack (Donepudi et al., 2016). A set of functionalities were implemented by using these technologies as described in table 5.1 to simplify the process of trust and make the trust data more comprehensive. In addition, the TCIDPF was developed to collect trust data either from CIdPs or CIdUs.

Table 5.1: Enabling technology in the TCIdPF

Product	Usage Description
AWS	Platform and Content Delivery
WordPress	Content Management System
IIS	Web server
MySQL	Application databases
PHP	Web Development

The main objective of this application is to quantify the assessment into a trustworthiness score with complementary numerical and graphical opinion representations. Trust value is measured by giving inputs for various parameters and sub-parameters. AWS service manager holds a repository that includes the database (MySQL) for all the CIdPs and can be used by the CIdUs to select one amongst the available options with respect to their requirement and demand for security. The result is evaluated according to the ESAs and ESCs quality criteria. As a proof of concept, a demonstration scenario is used to show the noticeable features of the TCIdPF.

Home

Cloud identity with Simplifying Identity and Access Management to bring More Secure Enterprise is the vital key to adopt and use the cloud services. However, with the single sign-on portal users only have to enter one set of credentials to access to their web apps in the cloud and behind the firewall either via desktops or smartphones. Likewise, this greatly increases productivity while keeping data secure. Moreover, it allows us to synchronize users with any number of directories, such as Active Directory, LDAP, Workday, or Google Apps. However, with a recent focus on the large-scale proliferation of Cloud computing, identity management in Cloud-based systems is a critical issue for the sustainability of any Cloud-based service. Numerous Cloud Identity Management Systems have been proposed so far; however, most of those systems are neither widely accepted nor considered highly reliable due to their constraints in terms of scope, applicability and security.

Therefore, in order to achieve reliability and effectiveness, building trust in the cloud identity environment is key to facilitate and social development. On the other hand, lack of trust, in particular, because of a perceived lack of legal certainty, makes consumers, businesses and public authorities hesitate to carry out transactions electronically and to adopt new services. This framework is set out in order to give consistency in the cloud identity environment regarding researches and guidelines and, thereby improving trust.

SEARCH

ABOUT THIS SITE

Building trust in the cloud identity environment is a key to facilitate and social development. Lack of trust, in particular because of a perceived lack of legal certainty, makes consumers, businesses and public authorities hesitate to carry out transactions electronically and to adopt new services.

FIND US



Address
WT305, 55 Wellesley St E, Auckland, 1010, New

Figure 5.4: Trust Cloud Identity Provider Framework

Figure 5.4 shows the main user interface of the application, which is available on the researcher website <http://www.cidptrust.com> and has four main panels and a menu. The first menu is for the public user, and they can see the overview of the website and they cannot contribute in the research. As figure 5.4 indicates they have access to Home, About, Blog, Contact, CIDP Trust Level, and user panel (Login and Register).

CIIdU is the real owner of the data assets and is the only one who knows the real value of the data and the realistic consequences of data security breaches. However, one of the valuable metrics for trust decision making is CIIdP's feedback, which might appear in quantitative or qualitative forms. Thus, ignoring the client's feedback and objectives will result in an inaccurate evaluation of security risk level and consequently trust measurement. Moreover, the Trust Manager allows cloud identity consumers to specify their requirements before assessing the trustworthiness of CIIdPs. It provides a front end by using the Web Research gate for the users for specifying their requirements. This application attempts to use clear and helpful language when it comes to explaining the trust levels. However, users can have their own (customise) trust level, which is based on their priority for the trust characteristics. Therefore, the second panel is for the identity users, which

allow them to give their feedback and trust weight, which is to be considered in the provider trust evaluation. Consequently, they have access to previous menus as well as Feedback and Weight as shown in figure 5.5.

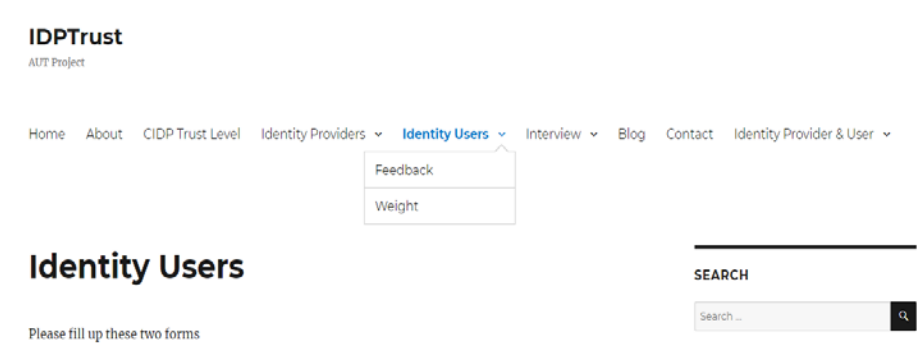


Figure 5.5: CIdU Dashboard

The third panel is for the identity providers who allow them to enter their trust information such as Consensus Assessment, Risk Assessment, Identity Management Standards, Service Level Agreement, and current industry benchmarking (Standards). Figure 5.6 shows the identity provider’s dashboard.

The fourth kind of the user is a contributor who has access to the interview dashboard. Contributor users are the identity expert user, and it helps this research to improve and validate the usability based on the questions (section 3.7) which are analysed in the next chapter. Figure 5.7 shows the interviewee’s dashboard.

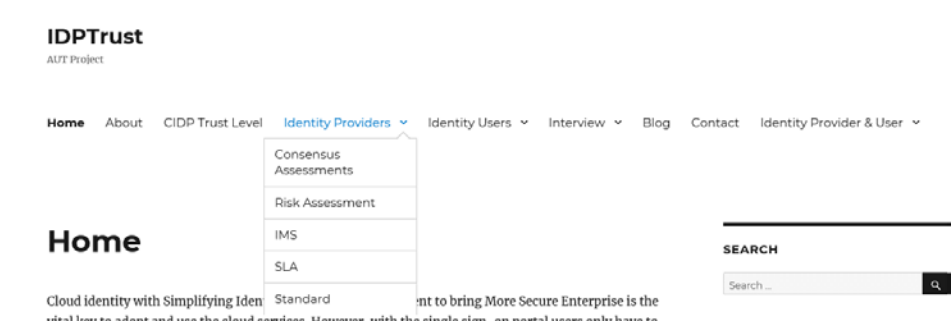


Figure 5.6: CIdP Dashboard

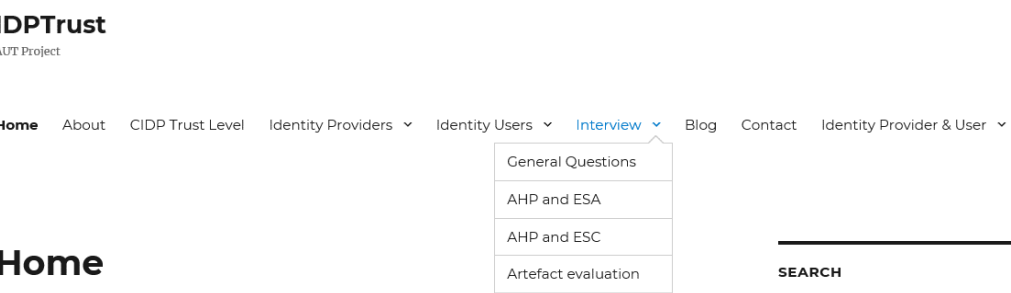


Figure 5.7: Interviewee Dashboard

5.4 FORMULATION FOR TRUST EVALUATION

The formulation is the part of methodology and is one of the crucial steps in the trust evaluation. The model for trust formation and evolution is based on cloud identity's quality of service. In case, the mathematical specification assists to transfer the information from trust modules to Trust Engine and with the usable metric and explicit equation. The formulation determines the theoretical properties of the providers, consequently, the upper bound on its resilience to attacks. So, the formulation is a crucial component because any weakness and issues in the design of the formulation allow malicious manipulation of the metric values. Therefore, in this section, three important components of the formulation are identified and discussed which are: the source of information, the type of information, and the trust metric.

Home About CIDP Trust Level **Identity Providers** Identity Users Interview Blog Contact Identity Provider & User

Protected: Consensus Assessments

Consensus Assessments


1. Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)? *
☒ YES ☐ NO ☐ N/A
2. Do you monitor and log privileged access (e.g., administrator level) to information security management systems? *
☒ YES ☐ NO ☐ N/A
3. Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes? *
User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant)
☒ YES ☐ NO ☐ N/A
4. Do you provide metrics to track the speed with which you are able to remove systems access that is no longer required for business purposes? *
☒ YES ☐ NO ☐ N/A
5. Do you use dedicated secure networks to provide management access to your cloud service infrastructure? *
☒ YES ☐ NO ☐ N/A
6. Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access? *
☒ YES ☐ NO ☐ N/A
7. Do you manage and store the user identity of all personnel who have network access, including their level of access? *
☒ YES ☐ NO ☐ N/A

SEARCH

ABOUT THIS SITE

Building trust in the cloud identity environment is a key to facilitate and social development. Lack of trust, in particular because of a perceived lack of legal certainty, makes consumers, businesses and public authorities hesitate to carry out transactions electronically and to adopt new services.

FIND US



Address
WT305, 55 Wellesley St E, Auckland, 1010, New Zealand

Figure 5.8: Consensus Assessments Form (CIMI)

The Cloud Identity Measurement Index (CIMI), questions are designed based on International Organization for Standardization (ISO) standards, National Institute of Standards and Technology Interagency Report (NISTIR) 7874, European Network and Information Security Agency (ENISA) Critical Cloud Computing, and Cloud Service Measurement Index Consortium (CSMIC) which has been derived from Cloud Security Alliance (CSA) Consensus Assessments Initiative Questionnaire (CAIQ). The CIMI includes 40 questions (in this step and it is dynamic based on the nature of cloud) and aims to cover Management, Configuration, Privileges, Delegation, Non-Repudiation, Scalability, Access

Control, and Auditing of any CIdPs. Each of these questions has three answers: Yes, No, and Not Applicable. A Provider-based on services can choose only one of the answers between these three options. Figure 5.8 shows the application consensus assessments form.

The CIMI allows CIdPs to fill in the questionnaire by providing an intuitive graphical interface through the CIMI menu. The questionnaire helps CIdPs to represent their competencies to the potential users with respect to different attributes. These questions consist of a set of most related and critical questions about identity providers that provide a standardised method for measuring and comparing an identity provider.

Therefore, after gathering the provider information for the assessment answers, the model is able to represent trust under uncertain probabilities. For evaluating the CIdP's trust, the associated opinion ($t, T_{Certain}$) for each of the propositions (CIMI questions (Appendix B)) is required (Ries, 2007; Ries et al., 2011). The opinions need to be extracted from each of the questions, where the cloud providers answer the underlying questions. The answers are in the form of 'YES', 'NO', or 'Not Applicable (N/A)', which upon analysis can be classified to negative (n) and positive (p) parts of evidence. These part units correspond to the existence of each of the CIMI questions, which demonstrate the level of trust. The mapping between the evidence space and the CIMI opinion space is as follows:

$$t = \begin{cases} 0 & \text{if } p + n = 0 \\ \text{else } \frac{p}{p+s} \end{cases} \quad (5.1)$$

$$T_{Certain} = \frac{N*(p+n)}{((2*(N-(p+s))) + (N*(p+s)))} \quad (5.2)$$

Average rating, t is calculated based on the number of positive assertions and the number of negative assertions under each domain. If there are no questions answered with 'yes' or 'no', t is 0. Otherwise, t is the relative frequency of positive and negative assertions.

Consequently, $T_{Certain}$, is calculated based on the total number of questions (in this part N is 40) and the number of negative and positive assertions. Though, the definition of N is adjusted according to the context of CIMI assessment. However, it is clear that the $T_{Certain}$ is 1 when all questions are answered with negative or positive assertions and 0 if none are answered.

Risk Assessment: For the portion of likelihood and risk assessment, Semi-quantitative risk analysis and standard risk level matrix based on control specification in the CSA CAIQ is used, in order to bring out level estimations of trust for the provider. These questions have been driven from the control specification of CAIQ, and it is easy for the providers to answer risk assessment questions. A 5x5 matrix is used because five possibilities are considered for cloud identity impacts. In the impact analysis and likelihood determination based on table 5.2, determines the likelihood of the existing questions and relative answers. Likelihood rating and Impact rating is the result of this step. Likelihood, the magnitude of trust level, and adequacy of planned or current control based on the questionnaire form is the input for trust determination step, and the result are trust scale and trust level matrix of the CIdPs.

IDPTrust

AUT Project

Home About CDP Trust Level **Identity Providers** Identity Users Interview Blog Contact Identity Provider & User

Protected: Risk Assessment

Risk Assessment

- How **LIKELY** would be compromised and misused the log data? *

☐ RAR
 ☐ UNLIKELY
 ☒ POSSIBLE
 ☐ LIKELY
 ☐ FREQUENT
- How **LIKELY** would be compromised and misused least privilege based on job function? *

☐ RARE
 ☐ UNIKLEY
 ☒ POSSIBLE
 ☐ LIKELY
 ☐ FREQUENT
- How **LIKELY** would be compromised access segmentation to sessions and data in multi-tenant architectures by any third party? *

☐ RARE
 ☐ UNLIKELY
 ☒ POSSIBLE
 ☐ LIKELY
 ☐ FREQUENT
- How **LIKELY** would be compromised and misused account credential life-cycle management from instantiation through revocation? *

☐ RARE
 ☐ UNLIKELY
 ☒ POSSIBLE
 ☐ LIKELY
 ☐ FREQUENT
- How **LIKELY** would be compromised and reuse account credential? *

☐ RARE
 ☐ UNLIKLEY
 ☒ POSSIBLE
 ☐ LIKELY
 ☐ FREQUENT
- How **LIKELY** would be compromised and misused non-shared authentication secrets? *

☐ RARE
 ☐ UNLIKELY
 ☒ POSSIBLE
 ☐ LIKELY
 ☐ FREQUENT

SEARCH

Search ...

ABOUT THIS SITE

Building trust in the cloud identity environment is a key to facilitate and social development. Lack of trust, in particular because of a perceived lack of legal certainty, makes consumers, businesses and public authorities hesitate to carry out transactions electronically and to adopt new services.

FIND US



Address
WT305, 55 Wellesley St E, Auckland, 1010, New

Figure 5.9: Risk assessments form

Figure 5.9 shows the web page of risk assessment which is contain 29 questions. Also, appendix C lists all 29 risk assessment questions for this study. The probability of occurrence of risk (P_i), expressed by means of: Rare 0.1, unlikely 0.25, possible 0.5, likely 0.75, and frequent 1.0. The semi-quantified impact of risk (I_i) is between very high (10), high (7.5), medium (5), low (2.5) and very low (1). The impact table is managed by administrator based on the impact of the relative

question to the industry but in this research with assume all medium which open future research for researcher to work on the impact of these question criteria. Cloud identity vendor affected by risk (B_i); and the Risk Level Estimation (RLE), which is proportional to the probability of a given risk and its impact on the CIdP in question, resulting in the following equation:

$$Trust_i = Imcat_i * Likelihood_i, R_i = P_i * I_i \quad (5.3)$$

That reflects that Trust (T) is proportional to both the probability of an undesirable event occurring (P) and the impact of this event (I). Total trust is calculated by the equation 5.4, where k refers to the number of the questions in the application as shown in figure 5.8.

$$T_{Trust} = \frac{\sum_{j=1}^k (T_j)}{k} \quad (5.4)$$

Finally, the result of the documentation assists CIdU to make a good decision-making based on the policy, procedural, and system operational. The result is stored in the trust repository and is sent to the Trust Engine to be used in the main formula. The five levels of RLE are as follow:

Catastrophic: if $7.4 < RLE_i < 10$

Major: if $3.7 < RLE_i < 7.4$

Moderate: if $1.75 < RLE_i < 3.7$

Minor: if $0.74 < RLE_i < 1.75$

Negligible: if $0 < RLE_i < 0.74$

Table 5.2 and Figure 5.10 illustrate all the possibilities concerning risk level estimations for a given CIdP regarding ranges and numeric values, respectively.

Table 5.2: Trust level estimation

Likelihood \ Impact	Rare (0.1)	Unlikely (0.25)	Possible (0.5)	Likely (0.75)	Frequent (1.0)
Very low (1)	Negligible	Negligible	Negligible	Minor	Minor
Low (2.5)	Negligible	Negligible	Minor	Moderate	Moderate
Medium (5)	Negligible	Minor	Moderate	Major	Major
High (7.5)	Minor	Moderate	Major	Major	Catastrophic
Very high (10)	Minor	Moderate	Major	Catastrophic	Catastrophic

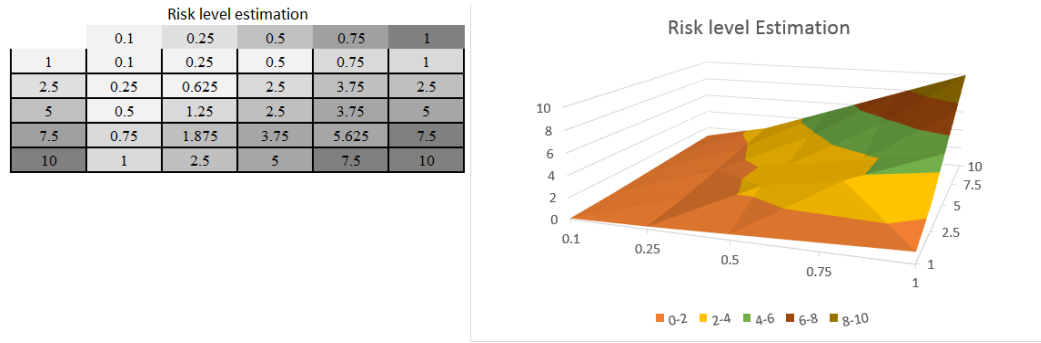


Figure 5.10: Risk level estimation

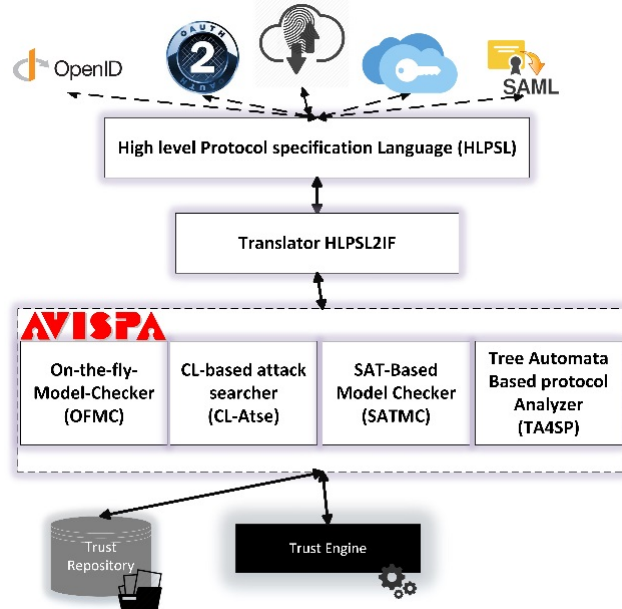


Figure 5.11: AVISPA's architecture in the proposed framework

IMS Security Checker: Model checkers have been remarkably successful in finding flaws in security protocols. The use of cloud identity protocols is rapidly on rising to minimise associated risks of identity theft. Security protocols are required to be

verified thoroughly before being used to secure authentication. There are several automatic security protocol verification tools based on formal approach. In the formal approach, protocol description, security properties and intruder capabilities are defined formally.

There are many open source security model checkers which choose AVISPA (figure 5.11) and in this thesis as per (Patel et al., 2010). AVISPA is a suitable tool for model checking. The result of security checking indicates that the protocol (standard) can be effectively used to automatically test implementations against supposed attack traces found by the model checker (Viganò, 2006).

By using this approach, it is easy to automatically detect and reproduce an attack witnessing an authentication flaw in the IAM systems. As shown in figure 5.11 IAM is translated to High-Level Protocol Specification Language (HLPSL). In the next step, HLPSL2IF converts it into rewrite IF format. OFMC, CL-Atse, SATMC, and TA4Sp are four back-end tools of AVISPA which has been integrated and will identify the weaknesses (level of security for this research) of the protocols. Next, IF specifications are given as input to all back-end tools. Finally, by running the back-ends of the AVISPA Tool against the provider's protocols, it will obtain the results (out of scope for this research and just the result of the tool explored in this section) summarised in table 5.3. The template table (No content in this section) gives the number of security problems (“#P”), the number of problems for which no attacks are detected (“S”), the number of problems for which attacks are detected (“A”), and the (average) time in seconds (“Time (T)”) spent by the back-end to find the attacks or to report that no attack exists.

Table 5.3: Effective template table of AVISPA tool

Problems		CL-AtSe (α)			OFMC (β)			SATMC (γ)			TA4SP(δ)		
Protocol	#P	T	S	A	T	S	A	T	S	A	T	S	A
OpenID													
SAML													
.....													

In the context of security checker, evidence units are based on the attack detected, average time detection, and some security problems that CIdPs possess regarding the services they offer. The mapping between the evidence space and the security checker space is as follows:

$$T_{Scheck} = \sum_{i=1}^{Number\ of\ protocols} \frac{A_{\alpha i} P_{\alpha i} + A_{\beta i} P_{\beta i} + A_{\gamma i} P_{\gamma i} + A_{\delta i} P_{\delta i}}{T_{\alpha i} S_{\alpha i} + T_{\beta i} S_{\beta i} + T_{\gamma i} S_{\gamma i} + T_{\delta i} S_{\delta i}} \quad (5.5)$$

Figure 5.12: IAM form

Trust evaluation average rating (T_{Scheck}), is calculated based on the number of protocols that CIdP use them in each domain. $A_{\alpha i}$, is the number of attack/attacks which has been detected based on the α (CL-AtSe) method. Besides, $P_{\alpha i}$ is the number of security problem/problems which check the security of the CIdP based on the α (CL-AtSe) method. In addition, $T_{\alpha i}$ is the time spent by the α (CL-AtSe) method and $S_{\alpha i}$ is the number of attack/attacks which has not been detected based on the α (CL-AtSe) method. Moreover, table 5.4 comparison between IAM systems is summarised in table 2.1 is used as a second method for the identifying the trust level for them. Therefore, the overall level is:

$$T_{IAM} = (T_{Scheck} + T_{Fulfill\ Requirement})/2 \quad (5.6)$$

Table 5.4: Trust Level of Current IAM solutions

$T_{Fulfill\ Requirement}$	OpenID	SAML	OAuth	CardSpace	Higgins	UProve	Idemix
Overall	29	25	29	31	33	26	26
Average	2.23	1.92	2.23	2.38	2.54	2	2

Finally, the result of the T_{IAM} is stored in Trust Repository and is sent to the Trust Engine to be used in the main formula. Moreover, figure 5.12 shows the web page of IAM system which providers have two choices for any IAM systems: Yes or NO.

Service Level Agreement: This module is based on strong SLAs containing various security attributes along with the QoS parameters specified by the consumers (Kanwal, Masood, Shibli, et al., 2014; Marudhadevi et al., 2014). Similarly, this module is responsible for formulating trust opinion based on SLA's Key Performance Indicator (KPI). SLA module is responsible for sending trust score to the trust manager to update the trust value. As per figure 5.13, the first process is extracting the parameters. In this research, the parameter is extracted and weighted manually (Symantec web method is out of scope for this research for extracting the parameters). The process of trust evaluation is performed in three steps: First, at initial stages, the users weight their required functional features based on template table 5.5. Next, site administrator fills up the table 5.6 based on the uploaded SLA's provider.

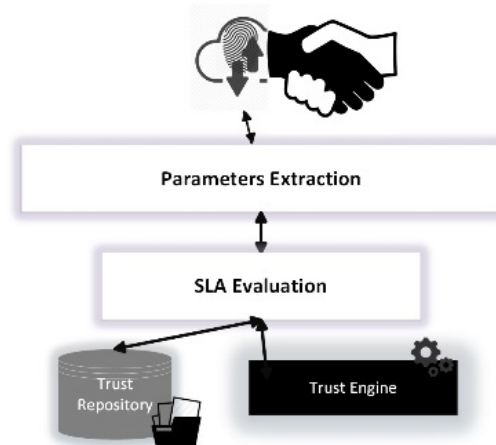


Figure 5.13: SLA evaluation process

Table 5.5: User weight template table for the SLA parameters

Criteria/Parameters	User 1	User 2	User K	AV
Load Balancing					
Life cycle					
SSO					
Privacy					
Risk					
Standards					

T_{SLA} is a term to indicate calculated SLA direct trust for each defined SLA between CIdP and cloud identity consumers. The extracted parameters from previous step module (template table 5.6) are forwarded to the SLA based Trust Evaluation module for evaluation of a SLA based trust score. KPI is defined for each specified measure in SLA. These KPIs are compared against defined set of security features that include Balancing (B), lifecycle (L), SSO (S), Privacy (P), and Risk (R) of data which are represented by the set $T = B, L, S, P, R$. We define Wi as the weight for each KPI based on cloud identity's requirements (Table 5.5, average Column).

Table 5.6: Extracted parameters template table for the providers

Criteria/Parameters	Provider 1	Provider 2	Provider n
Load Balancing				
Lifecycle				
SSO				
Privacy				
Risk				
Standards				

IDPTrust Home About Blog Contact CIdP Trust Level Identity Providers Identity Users Identity Provider & User

AUT Project

Protected: Weight

What is your weight for the below criteria?

Load Balancing *
3

Single Sign on *
3

Standards *
3

Life cycle *
3

Privacy *
3

Risk *
1

Please provide your User Name: *
User ID:

SEARCH

Search

ABOUT THIS SITE

Building trust in the cloud identity environment is key to facilitate and social development. Lack of trust, in particular because of a perceived lack of legal certainty, makes consumers, businesses and public authorities hesitate to carry out transactions electronically and to adopt new services.

FIND US


 Address
WT 305, 55 Wellesley St E, Auckland, 1010, New Zealand

Figure 5.14: User Interface for weighting the SLA parameters

Dynamic Weights (from users) are assigned to these features according to the desired security level of the CIdUs from Trust Management Module. SLA evaluation assigns weights to each of the five KPI in order to evaluate the customised trust score for users given by the set $W = wB, wL, wP, wR$. Extracted parameters are returned to the SLA evaluation module in the form of a

set represented by the t which is the subset of the power set of T ($t \in T$). Next, in order to calculate SLA based trust score T_{SLA} for each CIdPs the following equation is used.

$$T_{SLA} = \sum_{i=1}^{n=Number\ of\ the\ parameters} \frac{W_i * t_i}{|S|} \quad (5.6)$$

Finally, the result is stored in Trust Repository and is send to the Trust Engine to be used in the main formula. In addition, figure 5.14 shows the web application interface for the user to update the weight dynamically and figure 5.15 shows the CIdPs interface which they can upload their SLA pdf file.

Figure 5.15: Web interface for uploading the SLA

Global Compliance: Finding an identity provider that complies with all global and modern standards is important for the identity customers, both reputation and financially. Nowadays, CIdUs are looking for providers that have a good reputation for privacy and security standards compliance. Therefore, based on the importance of the user data, they are looking for a provider with a solid level of security and privacy compliance regarding this information while they are moving their identity and information to the cloud. On the other hand, the provider, which maintains compliance with applicable privacy and security standards, is preferred, and essential for any cloud migration.

Therefore, based on the compliance standards for choosing the providers and to help the CIdUs to have knowledge-based decision-making, compliance is used as trust elements. First, the provider answers the questions regarding these standards in the standard menu as shown in figure 5.16. Next, the administrator will update the template table 5.7 which is the weight for any standard (weighting the

standard is out of scope for this research, and in this thesis, all standard has same weight and value, but it could be future research for this thesis).

Table 5.7: Compliance weight template table

No	Accreditation	Weight
1	SOCIII	
2	ISO	
	PCI-DSS	
	CSA	
	HIPPA	
	FISMA	
N	SOCII	

Figure 5.16: Web interface for standards

Based on the provider's compliance and compliance weight, the following equation is used in order to calculate the level of trust based on standards. In this section, if the provider chooses yes, S_i is 1 and for No consider 0. In addition, N is using for normalisation

$$T_{Compliance} = \sum_{i=1}^{n=Number\ of\ the\ standards} \frac{W_i * S_i}{|N|} \quad (5.7)$$

Finally, the $T_{Compliance}$ result is stored in the Trust Repository and is sent to the Trust Engine to be used in the main formula.

Reputation analysis: CIdU is the real owner of the data assets and is the only one who knows the true value of the data and the realistic consequences of data security breaches. However, one of the valuable metrics for trust decision making is CIdP's feedback, which might appear in quantitative or qualitative forms. Thus, ignoring the client's feedbacks and objectives will result in an inaccurate evaluation

of security risk level and consequently trust measurement. Therefore, in this research, besides the involving CIdU to weight the low and high-level trust elements, they also give and share their level of trust base on their understanding. This module aims to combine CIdP's consumer feedback with technical measurements regarding the main aim, which is assessing and comparing the trustworthiness of CIdPs. It assists to complement the trustworthiness attributes of the framework and to allow identity users to control trust evaluation of the CIdPs.

The user's feedback as a manual source of information in the form of user ratings is the feedback resource. It is based on the user's unique identity as a result of their transaction with identity providers. The source information includes POSITIVE, NEGATIVE, or N/A. Figure 5.17 shows the web interface for user's feedback.

Figure 5.17: Web Interface for user feedback

The Reputation Analysis module receives the information from Web Research (figure 5.17) module and evaluates the trust of CIdP based on the received feedback. Next, it retrieves the feedback from the Trust Repository (other user's feedback) and evaluates the trust score. Subjective logic (Kanwal, Masood, Shibli, et al., 2014) is the main method for the evaluating of the feedback because the subjective logic is based on subjective opinions about the truth of propositions. An opinion about the CIdP proposition given by the CIdU is represented by W_{CidP}^{User} , Whereas, for N number of registered users submitting the feedback about CIdP, the opinions about an identity provider are represented by equation 5.8.

$$W_{CidP}^{User1}, W_{CidP}^{User2}, \dots, W_{CidP}^{UserN}, W_{CidP}^{User1} = (p, g, u, a)$$

$$p = \frac{\text{Positive feedback}}{\text{collected feedback} + n}, g = \frac{\text{Negative feedback}}{\text{collected feedback} + n}, u = \frac{n}{\text{collected feedback} + n}, a = \frac{1}{n} \quad (5.8)$$

Here p is the value for belief about the truth of the proposition CIdP which is derived from the positive feedback collected from the user. Similarly, g is the disbelief about the truth of the proposition that is derived from the negative feedback submitted by the user about CIdP. Whereas u and a, are the uncertainty and base probability respectively. After calculating the individual opinions for all the users, fusion operator is used to aggregate all the opinions about the CIdP proposition. The opinions are combined as follows:

Start

$$W_{CidP}^{User1}, W_{CidP}^{User2}, \dots, W_{CidP}^{UserN}$$

for i=2 to n do

$$p_i = \frac{(p_{CidP}^{user\ i} * u_{CidP}^{user\ i-1}) + (p_{CidP}^{user\ i-1} * u_{CidP}^{user\ i})}{(u_{CidP}^{user\ i} + u_{CidP}^{user\ i-1}) - (u_{CidP}^{user\ i-1} * u_{CidP}^{user\ i})}; \quad (5.9)$$

$$g_i = \frac{(g_{CidP}^{user\ i} * u_{CidP}^{user\ i-1}) + (g_{CidP}^{user\ i-1} * u_{CidP}^{user\ i})}{(u_{CidP}^{user\ i} + u_{CidP}^{user\ i-1}) - (u_{CidP}^{user\ i-1} * u_{CidP}^{user\ i})}; \quad (5.10)$$

$$u_i = \frac{(u_{CidP}^{user\ i} * u_{CidP}^{user\ i-1})}{(u_{CidP}^{user\ i} + u_{CidP}^{user\ i-1}) - (u_{CidP}^{user\ i-1} * u_{CidP}^{user\ i})}; \quad (5.11)$$

End;

$$T_{Feedback} = g_n + (a * u_n); \quad (5.12)$$

End;

By using the Subjective logic equation, all opinions are aggregated. This operator is executed iteratively for N number of times to aggregate all the N opinions. After the aggregation of opinions, an expected value $T_{Feedback}$ is calculated that represents the trust value of CIdP given. This module collects the submitted feedback from user feedback interface (figure 5.17) and manages the storage of the feedback at backend database. Feedback about each CIdP is stored in separate tables of database along with other trust elements. Finally, the output of a deterministic reputation calculation is used in the Trust Engine module. The calculated reputation values are stored in the trust repository for retrieval later.

Trust Engine: The Engine is able to model which configuration of propositional logic is required by the consumers in order to evaluate the trustworthiness of a CIdP based on the collected trust results. Trust Engine as a

main engine and aggregator, contains the definitions of operators in order to aggregate trust result from all trust results. The outcome of the evaluation is a numerical score.

In order to generate the trust responsibility, the Trust Engine collects the evaluated trust scores of the $T_{Feedback}$, T_{IAM} , $T_{Compliance}$, T_{SLA} , $T_{Certain}$, and T_{Risk} respectively. It combines both the trust values and calculates an aggregated trust value T_{Final} for particular CIdUs as follows:

$$T_{Final} = \frac{T_{Feedback} + T_{Compliance} + T_{Certain} + T_{SLA} + T_{Risk} + T_{IAM}}{6} \quad (5.13)$$

This scientific and very detailed trust measurement allows the identity customers to inspect and discover trust level of these extremely important trust elements (ESA and ESC) in depth that is not possible for the cloud users as shown in figure 5.18. However, the six categories of the trust along with the overall trust level is disseminated to the users.

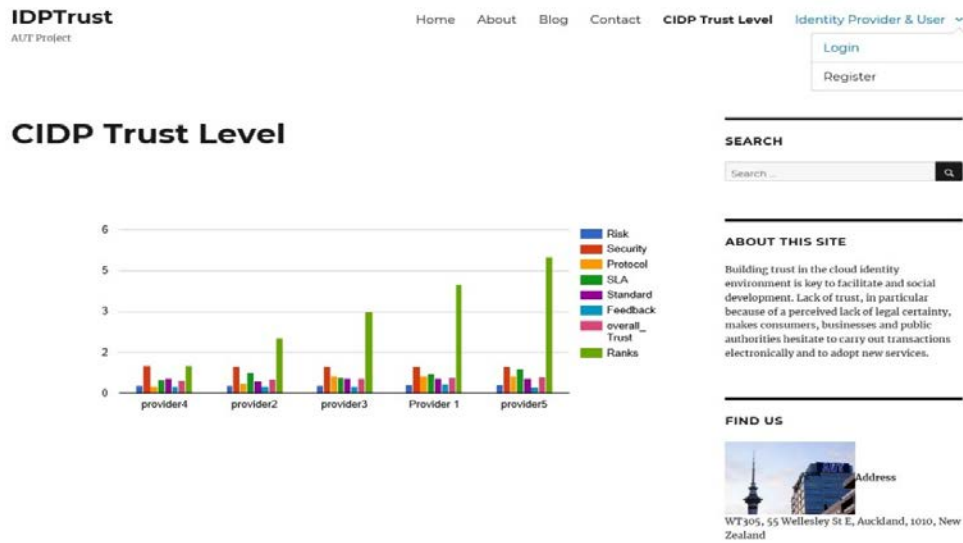


Figure 5.18: Web Interface of CIDP trust level

5.5 EXPERT USABILITY EVALUATION

In this section, based on the Design Science methodology, which has been presented in chapter three, usability testing is an effective, powerful and enlightening method that can bring validity to the application with an extensive range of questions which can be crucial to how the application is performing. The main reason is that this method provides compelling insights and genuine evidence of the real users (Expert people).

As (Charmaz, 2014) suggested, this research has considered the credibility, originality, resonance, and usefulness as the criteria for the validity of the research. Therefore, it incorporates qualitative usability testing by interviewing with usability related questionnaire to generate data about application attitudes and behaviour based on direct expert observing. The questions have been designed to help this thesis to find the issues, mitigate them, and consequently validate the usability of the application (Artefact).

IDPTrust
AUT Project

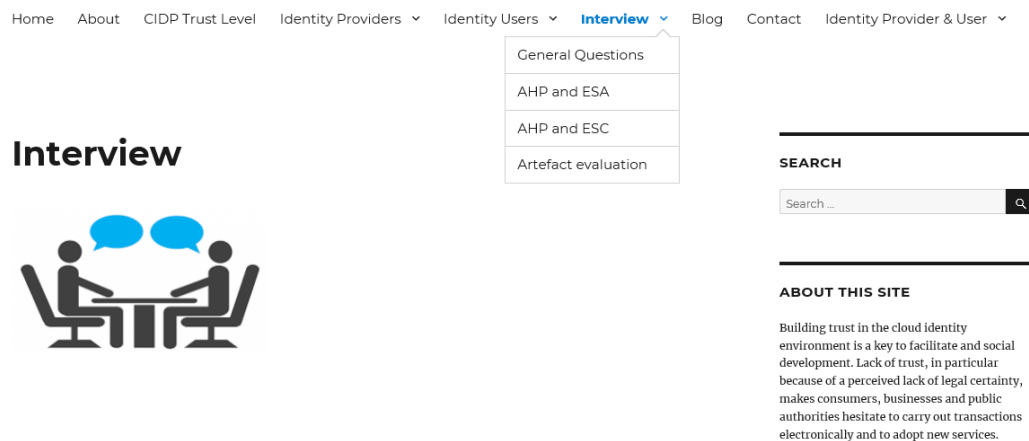


Figure 5.19: Interview page and its components

Therefore, based on (Robinson, 2014) the purposive sampling method was chosen for this study because in the method participants are selected according to predetermined criteria relevant to a particular research objective. The interviewees (research subjects) are selected because of their particular roles and skills in the company such as but not limited to IT managers and IT technicians which are directly involved with the cloud, cloud identity, and cloud adoption and have insights to the processes and issues faced by the organisation for cloud providers selection. This kind of sampling method suits the purpose of this research. In this regard, LinkedIn as the main place for professional and expert people has been chosen. Next, a brief explanation about the project and interview sent to defined people in different areas and perspectives of cloud and cloud identity (Network level, Software, Azure and DevOps, Security and governance, Academic and researcher). Finally, one member from each organisation and different areas of cloud were chosen for this research as shown in table 5.8. However, the small sample size with different perspectives, as well as the fact that the interviewees represent different positions in various types of cloud, provide the accuracy

required for analysis. Then, an initial meeting was arranged with each expert, interface, and questions link page as shown in figure 5.19. As shown in this figure and explained in section 3.7, there are two types of questions (general and artefact evaluation). Moreover, as discussed in section 4.7, in the IPA method, expert weight and rate are important to prioritise the trust elements (Attribute and Characteristics). Therefore, in the meeting, the capability and functionality of the artefact were demonstrated and explained.

Furthermore, the steps to prepare the trust level (CIDP Trust Level menu), instructions on how to fill up the Identity Providers and identity users form have been discussed and explained (demonstrated in chapter five), to ensure the expert's understanding of the implementation and evaluation procedures. Following that the experts respond based on the real experience in the cloud, working with cloud and CIdPs for some years, and their expectation with the application, and finishing with answering the evaluation questions.

Table 5.8: Interview participants

ID	Role	Expert area	Years in Market
I1	Cybersecurity Research and Development Expert	Cloud and cloud identity, security assessments and assurance	8
I2	Project Technical Lead/Senior Software Engineer	DevOps and cloud migration	More than 10 years
I3	Network Operations Team Lead	SDN, Cloud, NaaS and MaaS	12 Years
I4	Digital Transformation	Azure and cloud identity	6 Years
I5	Cloud Researcher	Open Source Cloud	5 Years

The experts were given 1-2 weeks to check the application and another week to have their feedback. The main question during that time was about ESC and ESA, and these questions helped the researcher to enhance the accuracy and applicability of the application by the real-world feedback. It has been raised, that gathering more information about the different providers in different ranges will help users and customers to make a better decision. Also, they said that ESC and ESA need more clarity. Moreover, they mentioned that Stakeholders should be involved to validate the application which in this stage is impossible but as future work will involve

them in the application. Their contribution will boost the credibility of research findings and will give proper context, business processes, and brand perception.

5.5.1 Ethics and Privacy

Ethics approval (Appendix A) was granted before the study commenced. Prior to conducting this thesis, it was made clear to all research participants that any personal information supplied by them such as their name, company name and addresses would not be made public. Their personal values were respected while conducting the research. An assurance of confidentiality was given through a signed consent forms which has been approved by AUT Ethics Committee (Appendix A). It was made clear that any data or information analysed through interviews would be published only if agreed upon and permitted by the participant. Participants were made fully aware of the fact that they were volunteers, taking part in this study without having been coerced or deceived.

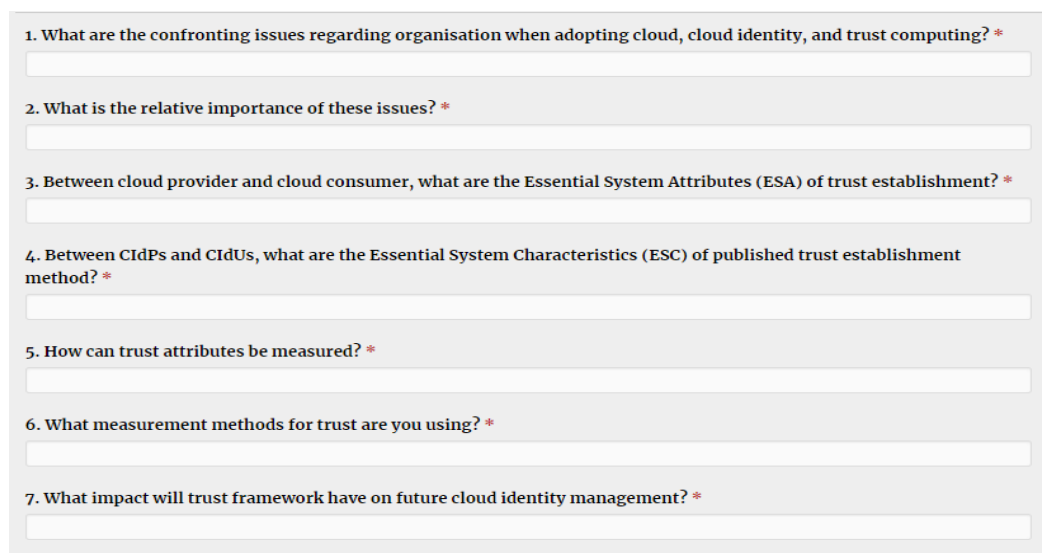
The image shows a screenshot of a web-based interview questionnaire. It contains seven numbered questions, each followed by a text input field. The questions are: 1. What are the confronting issues regarding organisation when adopting cloud, cloud identity, and trust computing? *, 2. What is the relative importance of these issues? *, 3. Between cloud provider and cloud consumer, what are the Essential System Attributes (ESA) of trust establishment? *, 4. Between CIdPs and CIdUs, what are the Essential System Characteristics (ESC) of published trust establishment method? *, 5. How can trust attributes be measured? *, 6. What measurement methods for trust are you using? *, and 7. What impact will trust framework have on future cloud identity management? *. The asterisk indicates that these are mandatory questions.

Figure 5.20: Interview questions dashboard from trust elements

It was important for this research that their viewpoints were conveyed openly. They were also reminded throughout the interview process that they could stop the interview at any stage. A degree of mutual respect was maintained throughout the interview process by giving due deference to participants' judgments and ensuring that they were free to respond without interference. The focus of the research design was to encourage participants to feel comfortable and relaxed while answering questions and the study aimed to profit from responses derived from the participants. This research was not judgemental or critical of the participants' answers during the interview, instead placing the facts as they were presented by

the participants. Protection was ensured by keeping both the participants' and organisations' identities private. The main ethical issue presented by this research relates to the privacy of all the participants involved. In order to maintain discretion at all times, so no names or personal details of any participant were revealed in this research. Instead pseudonyms were applied.

The image shows a screenshot of a web-based questionnaire titled 'Question dashboard of artefact evaluation'. It contains 10 numbered questions, each followed by a text input field. The questions are:

1. How effective is the application in managing trust in the cloud? *
2. How reliable is the trust level? *
3. Is this application adequate? *
4. How easily this application is used? *
5. Is this application capable of including all required trust elements? *
6. Can this application use the output of the other application (Monitoring, Benchmarking, SLA, Reputation, and computational)? *
7. Will this application meet the customer expectations? *
8. Do you find any usability issues with the application? *
9. Is there any area for improvement? *
10. Does this application provide enough detail and instruction for use? *

Figure 5.21: Question dashboard of artefact evaluation

5.5.2 Critical Reflection on Experts' Evaluation Results

Experts' artefacts evaluation is an essential stage in a DS-based research an artefact, as well as its theory, are put to the challenge. This essential part is beneficial by its outcome which is the real and up to date comments about the artefact. Moreover, it helps the researcher to get more feedback and knowledge during the evaluation with the expert, by challenging and testing both artefact and researcher.

As depicted in figure 5.20 and 5.21, there are two types of questions, General and artefact evaluation. Table 5.9 lists the set of questions to which all five experts' reply. As mentioned before, a different point of view and perspective helps the accuracy of the artefact validation. Using the web environment helped the efficiency of this section and interviewees were comfortable in the web environment instead of an oral interview. The next step was based on the thesis methodology (chapter three), the extracting and tabulating of the data from the experts' feedback as shown in table 5.9.

Table 5.9: Analysis the interviewees question (General Questions)

Question	Interviewee 1	Interviewee 2	Interviewee 3	Interviewee 4	Interviewee 5
Q1	Secure way to migrant data from local hosted server, Finding Cloud provider who has NZ local Data-centre, trust	Organisation existing identity model, compatibility with cloud identity, migration and applications integrations.	All main cloud providers are in overseas and it causes a lot of limitation in the decisions. Control, Security, Ownership and Prevention are other important problem factors.	compliance, cost, data protection laws.	Data security issue is the main concern when organisation makes decision.
Q2	these issues may cause delay in migration or cause bad experience of using cloud.	Business impact	Very high	high	Identity theft and data security and privacy.
Q3	Rapid elasticity	Compatibility with other apps.	Control, Security, Ownership and Prevention.	cost, integration with other platforms, security.	Data security, Availability of services, SLA optimization, Clarity in charging methods (Cost).
Q4	Identity Standard	B2B trust	user similarity, security, ownership and control.	adequate protection of user's data, transparent	Support latest IAM protocols.

				policy and communication, reliable service, security.	
Q5	Cloud provide need to have occasional test report done by independent third party companies and they could publish out to make sure they are trustable.	SLAs	It has used face-to-face communication with other customers and their experience along with available international benchmarks.	SLA, application	Using online benchmarking standards.
Q6	Datacentre visit 2- company done penetration test annual bases 3- be in list to TaaS (TaaS Supplier Directory). 4- 27/4 access to all data centre.	B2B, B2C trust	Reputation of the company, Recovery mechanisms, Confidential computations and storage, Direct and Relative trust.	security assessment, accreditation of certification bodies.	Indirect

Q7	Reputation of the business.	organizations/apps collaboration using same identity.	Capacity and computational power of computers and network speed, Future of companies and their road map for providing different technologies.	It can reduce risk and facilitate decision making process for board members.	It is important to have a framework to help decision making.
----	-----------------------------	---	---	--	--

Table 5.10 shows interviewees mentioned different points and answers for each question as they have a different background in the cloud area. Question 1 has: Secure way, local Data-centre, trust, existing identity model, compatibility, migration, applications integrations, control, security, ownership and prevention, compliance, cost, data protection laws, data security are the confronting issues regarding organisation when adopting cloud, cloud identity, and trust computing. However, most of these key points are considered to be measured in this thesis.

In question 2, the interviewees give the relative importance of these issues as a delay in migration, business impact, very high, high, and identity theft as the motivation for this thesis. Moreover, in question 3, Rapid elasticity, compatibility, control, security, ownership, cost, integration, availability, SLA optimisation, clarity in charging methods (cost) are stated as an ESA for trust establishment between cloud providers and customers. However, in question 4, identity standard, Business to Business (B2B) trust, user similarity, security, ownership and control, adequate protection of user's data, transparent policy, reliable service, security, support latest IAM protocols, are stated as an ESC between CIdPs and CIdUs.

Trust measurement is one of the most challenging questions, and even during the interview, the interviewee did check the trust measurement of their company by talking and asking their colleagues. In the question 5, they mentioned that a test report was done by an independent third party, checking the SLAs, face-to-face communication, available international benchmarks, and using online benchmarking standards, are the most common method based on their experience. However, in their company they are using datacentre visit (direct trust), penetration test annual bases, list of the TaaS (TaaS Supplier Directory), access to all data centre B2B, B2C trust Reputation, Recovery mechanisms, confidential computations, direct and Relative trust, security assessment, accreditation of certification bodies, and indirect assessment. In chapter five the thesis artefact covered these methods. In the question 7, the researcher is looking for the impact on the future cloud identity management (research motivation). The interviewee identified that trust management is important for the reputation of the business, application, organisations, computational, future of companies and their roadmap for providing different technologies. Also, they mentioned that trust management could reduce risk and facilitate decision-making processes for board members. Moreover, they

encouraged the researcher by stating the importance of this research in the future of cloud and cloud identity.

At the end the interviewees suggested the below comments to consider in the final version of the artefact.

1. Trust is a fragile element and the artefact is better to be more dynamic.
2. Trust depends on the provider location, and one example is Trustable Telecommunication Supplier Directory (<https://www.ict.govt.nz/services/showSuppliers/TaaS>); therefore, the trust is related to the geographic location.
3. Service providers are flexible to take advantage of the latest and innovative technology; therefore, the artefact should consider the latest technology and protocols to be measured

The next step is application (which is based on the artefact) evaluation by expert questionnaire. As mentioned in chapter three, usability checking, and evaluation are of the most valuable methods for artefact assessment. Therefore, the researcher asked the interviewees to answer the corresponding artefact questions as outlined in Figure 5.21. In this section, the evaluators (expert) were asked to register in the application (website). Next, the researcher (application admin) changed their role as a contributor to privileges on their access to the website. They had two weeks to work with the application and check it, and consequently, the researcher asked them to fill up the questionnaire form as depicted in table 5.10.

Table 5.10: Analysis of the interviewee's question (Application Questions)

Question	Interviewee 1	Interviewee 2	Interviewee 3	Interviewee 4	Interviewee 5
Q1	Very effective and demanding.	Based on my overview, this application is thoughtful and has the real-world trust perspective.	to a great extent	very effective	Very effective
Q2	Very much	As a prototype is a reliable application.	as it includes several factors to calculate trust level, I think it could be adequately reliable.	very much	Good
Q3	It is but needs to be improved by writing more technical information and not using abbreviation.	Yes, the application is adequate to use as a trust benchmark application in the future.	yes, it is	yes	Yes
Q4	It is quite simple	this application is easy to use, however, needs more polish by getting user's feedback.	A bit confusing and hard to get your hands on.	descent easy	Easy to use

Q5	Yes, it is but required more information about the definitions of different terms.	Yes, consider both sides provider and user.	It might require including certifications to the calculation. for example, PCI-DSS.	yes	Most of them
Q6	Yes, it is very helpful for decision making.	As here I can see, yes, this application using the output of other methods.	of course, it is recommended.	yes	Yes
Q7	Yes, if they provide more information.	for this stage, yes.	yes	yes	Yes, most of them
Q8	Easy to use	No, but after adding the explanation.	It should provide users with more drill-down like the dashboard.	no	No
Q9	More information required in most questions. It would be better to have a short tip for every question to clarify them.	Clarity of trust methods is beneficial for this application.	user experience	Remove complexity	None so far

Q10	It is ok but needs to have more details on each question.	Overall application is fine at this stage but, add more detail is essential in the future.	not really	yes	Yes enough
-----	---	--	------------	-----	------------

Table 5.11 shows that the interviewees give different points and answers for each question as they have a different backgrounds in the cloud area. In Question 1, most of the interviewees agree with the effectiveness of the application in managing trust in the cloud (*Very effective and demanding, thoughtful and has the real-world trust perspective, to a great extent very effective, and very effective*). They answer to this question very positively, and it is an achievement for this thesis.

In the question 2, regarding the reliability of the trust level, after explaining the formula, source of information, and chosen provider and users, the interviewees have figured out that this artefact is reliable as it includes several factors to calculate trust level (*Very much, as a prototype is reliable, adequately reliable, very much, and good*). However, in question 3, the researcher asks them to criticise the application adequately. Therefore, after working with the application, they all agree with the application adequately but with writing more technical information and removing the abbreviations (*It is but need to be improved by writing more technical information and not using abbreviation, Yes, the application is adequate to use as a trust benchmark application in the future, yes, it is, yes, and Yes*).

During the designing, planning, and implementation, user-friendly was one of the main criteria which the researcher tried to be aligned with. Therefore, in the question 4 (*“How easily the application is used”*), four interviewees were agreed with the easy to use (*It is quite simple, this application is easy to use, however, needs more polish by getting user's feedback, descent easy, and Easy to use*), but one interviewee believed that (a bit confusing and hard to get your hands on) needs more clarity to remove the complexity of the application.

The capability of including most of the required trust elements is the role of question 5. In this question, the first interviewees identified their required trust elements, and after that, they compared their requirements and application trust elements. They said that this application is capable of covering most of the trust elements, but one of the interviewees mentioned considering Payment Card Industry Data Security Standard (PCI-DSS) standard which is added to this application.

One of the main features for any trust framework is using the output of another framework. In the question 6, the researcher asked the interviewees about this feature, and they all agree with this idea, which prohibits parallel trust processing. Their comments were positive as shown in table 5.10 (*yes, it is very*

helpful for decision making.as here I can see, yes, this application using the output of other methods, of course, it is recommended, yes, and yes). Customers are the real owner of the applications, so, their expectation is so important and should consider as one of the main criteria for this thesis. Therefore, in question 7 the researcher asked the interviewees “Will this application meet the customer expectations?”. As they are working in the cloud area with more than five years and they were both cloud providers and cloud customers, and they approved that this application meets the customer expectation (yes, if they provide more information, for this stage, yes, yes, yes, yes, most of them). In the question 8, the interviewees have been asked about any usability issues with the application, which is the main question for this section. Similar to the previous question, after a while, to work with the application and the researcher explanation, they all are agreed with that there are no major issues with usability of the artefact (*easy to use, no, but after adding the explanation, it should provide users with more drill-down like the dashboard, no, no*). Therefore, as a response to this concern, the trust level (Dashboard) is modified and will add some more information.

In the question 9, interviewees have been asked to find any issues in the application to be improved by the researcher. They mentioned that clarity of the trust elements, short tips for each section are the main issues which are added in the second round of the design science methodology. However, about the user experience, the researcher mentioned that direct and indirect trust had been used in this artefact to cover the user experience. The question is about the application detail and instruction for the user. One of the interviewees mentioned, “that it is ok but need to have more details on each question”. In response to this concern, the researcher added one main instruction menu. The second interviewee stated that the overall application is fine in this stage but, add more detail is essential in the future. As a response to this concern, the researcher has added one main instruction as well. Interview 3 said “not really” for the same concern which obviously the instruction menu will remove this concern. The other two interviewees are agreed that this application provides enough detail and instruction for use.

5.6 CONCLUSION

This chapter has demonstrated and provided the design, architecture, and workflow of the proposed artefact. In the application architecture, the application architecture of Trust Evaluation Model and its objects are presented. Figure 5.2 shows the proposed architecture along all the components. In the application workflow and modelling trust, first, the workflow of the proposed method is depicted, next, the connection between them has been identified as depicted in figure 5.3. The application utilised the contemporary technologies such as but not limited to AWS, MYSQL, and IIS. Section 5.4 has formulation as the crucial part for this chapter. Analysing different methods to gain the main objective of the thesis is the aim of this section. Equation 5.13 is the result of the analysing the measurement methods as well as a tool to disseminate the trust level. However, this chapter is based on the previous trust framework that has verification from the current literature, but expert usability evaluation is the essential part for evaluating any artefact based on the methodology. The main reason is that this method provides compelling insights and genuine evidence from the real users.

However, in chapter six, the finding of the project is evaluated. Therefore, first the researcher has developed the trust evaluation hierarchy to evaluate the artefact. The MCDM approach delivers the inputs to an analytic hierarchy process (AHP) to complete the trust assessment. The next method is based on figure 5.1, and is evaluation based on the guidelines. Therefore, three main cloud identity standards are analysed in term of their main criteria. The standard's comparison and discussion of the result are two parts which illustrate the relevance between the proposed method and these guidelines. The feasibility of the framework is another concern which the researcher discusses in the section 6.3 by using the validity of the STRIDE threat modelling.

Chapter Six

Findings

6.0 INTRODUCTION

In chapter five, the design, workflow, architecture of the proposed application along with formula have been presented. In addition, the application component and the functionality of the application to measure the trust level have been demonstrated.

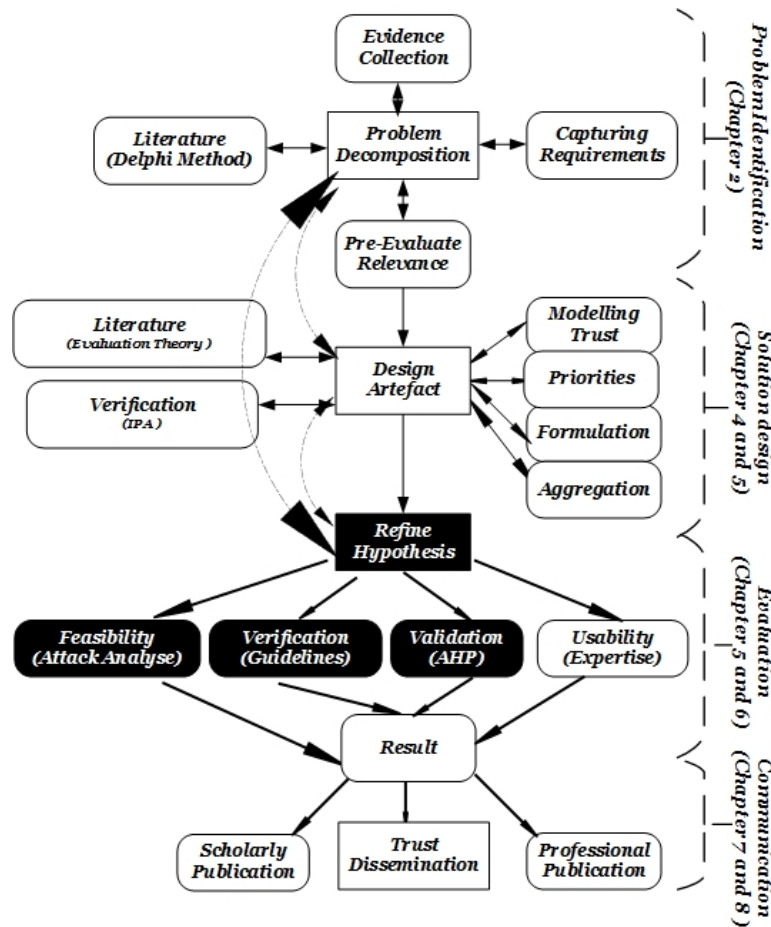


Figure 6.1: Chapter six Pathway

Figure 6.1 is depicted the summary of the thesis based on the proposed methodology, also the main topic of the chapter six which is proposed framework evaluation. As mentioned in the section 1.2, the approach is to clarify the pathway and roadmap of the thesis by highlighting (black areas) the particular steps and sub steps to achieve the main objective of the thesis (mitigating identity theft). Therefore, in this part there are three main topics; validation from AHP, verification from guidelines, and feasibility checking from STRIDE threat modelling. However, based on the mixed methodology, there are six approaches to evaluate the artefact.

In chapter four, the trust method was defined as well as related trust elements. Moreover, in chapter five, the usability checking has been done; therefore, in this chapter, the following steps are completed: Evaluating the artefact elements by using AHP (section 6.1), verification from the standards (section 6.2), and feasibility validation by using STRIDE Threat Modelling (section 6.3) is conducted to identify the findings of the research.

6.1 EVALUATION THE ARTEFACT

The trust assessment is a key function that should be performed in advance of any cloud customers' decision making. As part of thesis methodology (figure 6.1), the key elements of the artefact are prioritised after modelling the trust. In this part Multiple Criteria Decision-Making (MCDM) is introduced to prioritise the attributes for a cloud identity trust framework. The overall trust assessment is decomposed into two parts: the trust analysis of the federated identity management systems, and the quantification of trust. The MCDM approach delivers the inputs to an analytic hierarchy process (AHP) to complete the trust assessment. This part innovates a theoretical solution to the trust gap (section 3.1) between CIdPs and the cloud identity customers.

Prioritizing characteristics and attributes affecting CIdUs decision making can be viewed as a complex Multi-Criteria Decision Making (MCDM) problem and a suitable method to answer the identity customer question. The Analytical Hierarchy Process (AHP), a prevalent MCDM method, facilitates understanding of the decision-making process and thus assists CIdU decision makers in finding trustable providers. The focus of the chapter is on prioritising for such characteristics of trust service in the cloud identity environment. Therefore, this thesis encourages the use of the analytic hierarchy process (AHP) in dealing with the challenge (Ghazizadeh & Cusack, 2017b).

The AHP approach (Saaty, 1989) is one of the more extensively used MCDM methods. The AHP has been applied to a wide variety of decisions and the human judgment process (Chen, 2006; Goepel, 2013). The approach is used to construct an evaluation model and has criterion weights. It integrates different measures into a single overall score for ranking decision alternatives. Applying it usually results in simplifying multiple criterion problems by decomposing it into a multilevel hierarchical structure. Obtaining solutions in the AHP is not a statistical

procedure because it can help either a single decision maker or a decision group to solve an MCDM problem. Applying the AHP procedure involves three basic steps:

- Decomposition, or the hierarchy construction.
- Comparative judgments or defining and executing data collection to obtain pairwise comparison data on elements of the hierarchical structure.
- Synthesis of priorities or constructing an overall priority rating.

Also, it is important that all essential elements relevant to the problem are covered within the hierarchy structure. In its most typical form, a hierarchy is very often structured from the top (objectives from the managerial standpoint) through the immediate level (criteria and sub-criteria that subsequent levels depend on), and onto the lowest level (which is usually a list of alternatives). Next, the decision makers (interviewees) begin the prioritisation procedure to determine the relative importance of the elements in each level.

- Two elements being compared at a given time greatly reduces the conceptual complexity of analysis. Given a pairwise comparison, the analysis involves three tasks: Developing a comparison matrix involves three tasks: Developing a comparison matrix at each level of the hierarchy starting from the second level and working down
- Computing the relative weights for each element of the hierarchy
- Estimating the consistency ratio to check the consistency of the judgment

Elements in each level are compared in pairs concerning their importance to an element in the next higher level. Starting at the top of the hierarchy and working down, the pairwise comparisons at a given level can be reduced to some square matrices $A = [a_{ij}]_{n \times n}$ as in the following:

$$\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix}$$

The matrix has reciprocal properties, which are

$$a_{ji} = \frac{1}{a_{ij}} \quad (6.1)$$

In AHP, Satty (1980) recommended a scale of relative importance from 1 to 9 for making subjective pairwise comparisons as shown in table 6.1. Pairwise comparison matrices are formed, the vector of weights, $W = [w_1, w_{21}, \dots, w_n]$, is computed on the basis of Satty's eigenvector procedure. The computation of the

weights involves two steps. First, the pairwise comparison matrix, $A = [a_{ij}]_{n \times n}$, is normalized by equation (1), and then the weights are computed by equation (6.3).

Normalisation

$$a^*_{ij} = \frac{a_{ij}}{\sum_{i=1}^n a_{ij}} \quad (6.2)$$

Weight Calculation

$$w_i = \frac{\sum_{j=1}^n a^*_{ij}}{n} \quad (6.3)$$

Satty (1980) showed that there is a relationship between the vector weights, w , and the pairwise comparison matrix, A , as shown in equation (6.4).

$$Aw = \lambda_{\max} w \quad (6.4)$$

The λ_{\max} value is an important validating parameter in AHP and is used as a reference index to screen information by calculating the consistency ratio (CR) of the estimated vector. To calculate the CR, the consistency index (CI) for each matrix of order n can be obtained from equation (6.5).

$$CI = \frac{\lambda_{\max} - n}{n - 1} \quad (6.5)$$

Then, CR can be calculated using equation (6.6):

$$CR = \frac{CI}{RI} \quad (6.6)$$

Where RI is the random consistency index obtained from a randomly generated pairwise comparison matrix. The usual values are tabulated and have an RI value calculated from matrices of order 1 to 10 as suggested by. If $CR < 0.1$, then the comparisons are acceptable. If, however, $CR > 0.1$, then the values of the ratio are indicative of inconsistent judgments. In such cases, one should reconsider and revise the original values in the pairwise comparison matrix A .

Table 6.1: Scale of relative importance (Saaty & Kearns, 2014)

Importance	Definition
1	Equal importance
3	Moderate importance
5	Essential
7	Demonstrated importance
9	Extreme importance
2,4,6,8	Intermediate values between the two adjacent judgments

To obtain an aggregate measure of the pairwise comparisons of all individuals involved in a decision problem, the geometric mean of the individual assessments using equation (6.7) can be used (Saaty, 1989).

$$a_{ij}^{hp} = \sqrt[Q]{\prod_{q=1}^Q a_{ij}^q} \quad (6.7)$$

where a_{ij}^q is an element of matrix A of an individual q between 1 and Q, and a_{ij}^{hp} is the geometric mean of all individuals a_{ij}^q . The group CR is calculated according to equations (6.5) and (6.6).

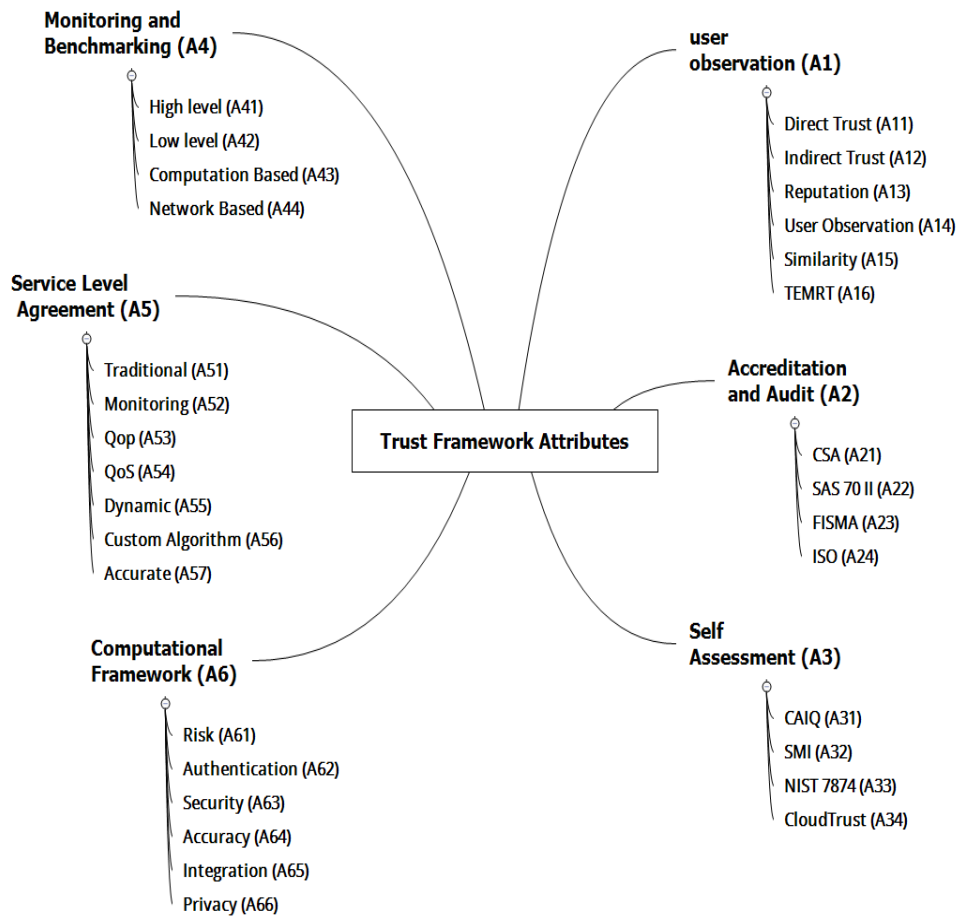


Figure 6.2: The Hierarchy of trust framework attributes

6.1.1 Developing the Trust Evaluation Hierarchy

In this section, cloud identity service selection is the application case. The case aims to evaluate how cloud identity customers prioritise trust elements affecting CIdPs selection. In figure 6.2 and 6.3 the ESA of trust framework and ESC of CIdP decision making are itemised according to chapter four. As figures 6.2 and 6.3, a

simple three-level hierarchical structure are first constructed. Initially, the number of levels is determined, and the variables identified.

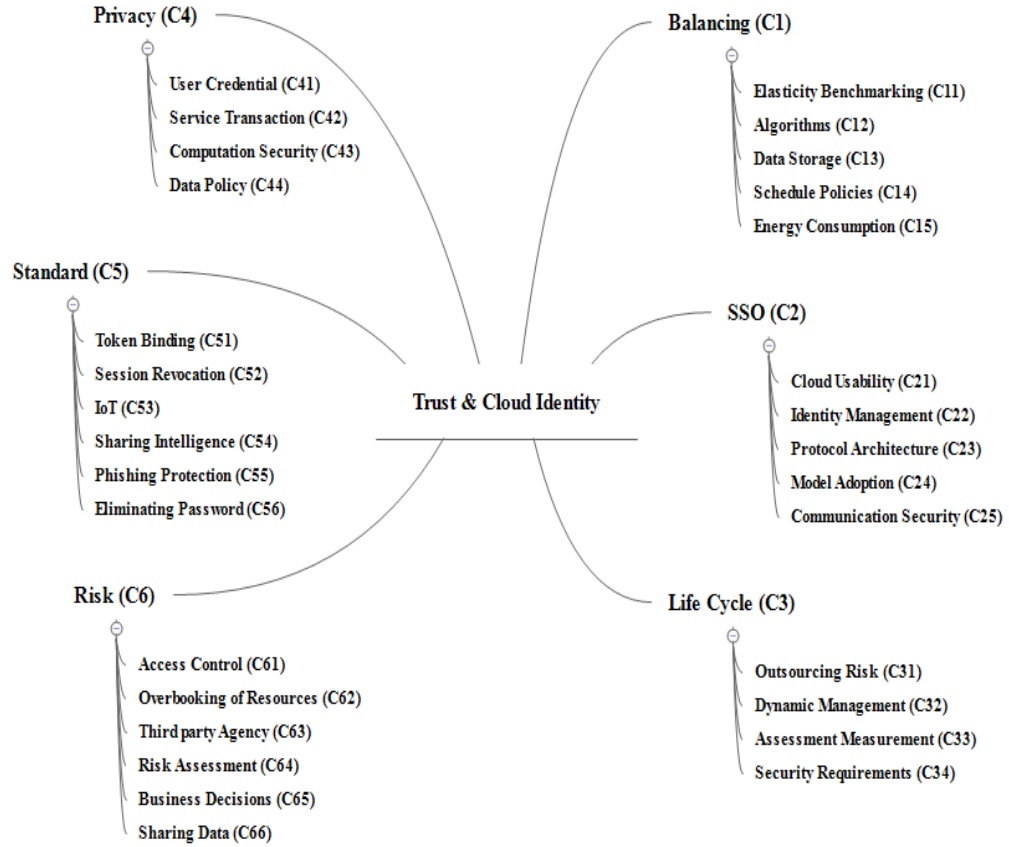


Figure 6.3: The hierarchy of CIdP decision making

In the next step, this thesis adopts AHP to work with the trust framework and trust elements. Data collection is essential to develop a hierarchical decision model for the decision problem as illustrated in figures 6.3 and 6.4. The data collection is broken into three major levels including goal level, objectives, and level and design criteria level. The goal level is the top most level which describes the decision problem. This section attempts to work out the most sustainable trust framework elements and most suitable CIdP characteristics, and therefore, the topmost levels are to “design the best trust framework” and “identify the best CIdP trust Characteristics”. The second level is the objectives level comprised of six trust framework models and six main trust criteria, while the third level consists of various method and criteria. In order to identify the priorities of objectives in the second level, and the relative importance of different criteria in the third level, a series of the questionnaire have to be performed by the experts along with the

application evaluation. The elements in both levels are then weighted, and the final score for each part is based on the composite view of the five experts engaging in the judgment process.

AHP Analytic Hierarchy Process (EVM multiple inputs)

Only input data in the light green fields and worksheets!

n= Number of criteria (2 to 10) Scale: AHP 1-9

N= Number of Participants (1 to 20) α : Consensus:

p= selected Participant (0=consol.) 2 7

Objective

Author

Date

Thresh: Iterations: EVM check:

Table	Criterion	Comment	Weights	Rk
1	A1	USER OBSERVATION	12.2%	4
2	A2	ACCREDITATION AND AUDIT	22.7%	2
3	A3	SELF ASSESSMENT	14.8%	3
4	A4	MONITORING AND BENCHMARKING	4.9%	6
5	A5	SERVICE LEVEL AGREEMENT	6.5%	5
6	A6	COMPUTATIONAL FRAMEWORK	39.0%	1
7			0.0%	
8			0.0%	
9			0.0%	
10		for 9&10 unprotect the input sheets and expand the question section ("+" in row 66)	0.0%	

Result

Eigenvalue lambda:

Consistency Ratio 0.37 GCI: CR:

Matrix											normalized principal Eigenvector	
	A1	A2	A3	A4	A5	A6	0	0	0	0		
A1	1	-	1/2	3/5	3 8/9	2	1/4	-	-	-	-	12.16%
A2	2	1 8/9	-	2 1/3	4 1/8	4	2/5	-	-	-	-	22.69%
A3	3	1 2/3	3/7	-	3 3/4	2 5/7	1/3	-	-	-	-	14.78%
A4	4	1/4	1/4	1/4	-	1/2	1/4	-	-	-	-	4.86%
A5	5	1/2	1/4	3/8	1 8/9	-	1/5	-	-	-	-	6.53%
A6	6	3 3/4	2 5/9	3 1/4	4 1/8	5	-	-	-	-	-	38.97%
0	7	-	-	-	-	-	-	-	-	-	-	0.00%
0	8	-	-	-	-	-	-	-	-	-	-	0.00%
0	9	-	-	-	-	-	-	-	-	-	-	0.00%
0	10	-	-	-	-	-	-	-	-	-	-	0.00%

Figure 6.4: The ESA weighting interface

In order to have a representative result, as mentioned section 6.1, five experts were invited to participate in the judgment process as they have enough experience and knowledge to prioritise these elements. Therefore, while conducting AHP, all interviewees are required to make judgments on the relative standings of different criteria in the matrices with reference 0 to 9-point scale as shown in figure 6.4.

Consequently, during the expert interview, each expert is requested to take part in the AHP judgment process with the assistance of the AHP template which is available in (<https://bpmsg.com/new-ahp-excel-template-with-multiple-inputs/>). This free template consists of 20 sheets for 20 interviewees for pairwise comparison. It also includes a sheet for solving the eigenvalue problem when using the eigenvector method (EVM), consolidation of all judgments, a sheet with reference tables, and a summary sheet to display the result. By using this application, the relative weights of the objectives and corresponding criteria, and the consistency ratios of the matrices can be gathered and calculated.

Table 6.2: Consistency Test for CIdP trust characteristics

Level		Consistency Ratio	Consistency Test
Goal		0.046	Accepted
Characteristics			
	Balancing C1	0.018	Accepted
	SSO C2	0.05	Accepted
	Life Cycle C3	0.038	Accepted
	Privacy C4	0.036	Accepted
	Standard C5	0.08	Accepted
	Risk C6	0.047	Accepted

Table 6.3: Consistency test for trust framework attributes

Level		Consistency Ratio	Consistency Test
Goal		0.038	Accepted
Characteristics			
	User Observation A1	0.078	Accepted
	Accreditation and Audit A2	0.05	Accepted
	SELF ASSESSMENT A3	0.049	Accepted
	Monitoring and Benchmarking A4	0.059	Accepted
	SLA A5	0.049	Accepted
	Computational Framework A6	0.059	Accepted

In order to improve the quality of the artefact, the experts explained the concept of each method, elements, and characteristics. The respondents are asked to make

judgments about the relative importance of the element with respect to the overall goal of selecting the elements (Methods and characteristics). For example, when the researcher asked, “Observational - TEMRT A16” the verbal explanation helped the interviewee to know the exact meaning of the TEMRT. After doing all trust framework pairwise comparisons at level 2 and 3, the pairwise comparison matrix is constructed. Similarly, the CIdP characteristics pairwise comparison procedure is then applied to all factors with respect to all levels.

Tables 6.2 and 6.3 summarise the consistency test, and both ESC and ESA global weights, respectively. All CR values in table 6.2 and 6.3 are lower than 0.1, and therefore bring the validity for this research. Also, it shows the consistency between the judgments (interviewees) and accuracy of the elements.

According to (Saaty and Kearns , 2014), the global weights for the ESA and ESC are synthesized from the second level (objectives) by multiplying the local weight. Therefore, table 6.4 and 6.5 show the local and global weight which has been driven from the interviewees with respect to a single criterion.

In table 6.4, the result of local weights in terms of attributes reveals that Computational framework (0.39) and Accreditation and audit (0.227) are the most important trust frameworks for checking the trust level of the cloud providers, followed by Self-assessment (0.148), user observation (0.122), SLA (0.06), and Monitoring and benchmarking (0.049) appears to be the factor with the lowest importance. However, A62 (0.13), A22 (0.112), A63 (0.09), A31 (0.074), and A21 (0.06) are most ranked global attributes.

Moreover, in table 6.5, the result of the ESC local and global weight has been shown. It reveals that align with Standard (36.2) and SSO protocols (24.0) are the most important trust characteristics for the CIdPs with respect to other characteristics. However, by looking at the global weights in table 6.5, the C55 (1.12), C56 (0.83), C22 (0.72), C52 (0.64), C23 (0.61) are the top five rankings. In contrast, the elements of C13 (0.08), C15 (0.074), and C12 (0.05) are the bottom three rankings.

Table 6.4: ESA local and global weight

Attributes	Local Weight %	Elements	Local weight %	Global Weight	Ranking
User Observation A1	12.2	A_{11}	35.8	0.043676	8
		A_{12}	24.2	0.029524	12
		A_{13}	15.9	0.019398	16
		A_{14}	6.7	0.008174	24
		A_{15}	5.5	0.00671	25
		A_{16}	11.9	0.014518	22
Accreditation and Audit A2	22.7	A_{21}	29.4	0.066738	5
		A_{22}	49.4	0.112138	2
		A_{23}	6.5	0.014755	21
		A_{24}	14.6	0.033142	10
SELF ASSESSMENT A3	14.8	A_{31}	50.1	0.074148	4
		A_{32}	22.9	0.033892	9
		A_{33}	13.8	0.020424	15
		A_{34}	13.1	0.019388	17
	4.9	A_{41}	49.7	0.024353	13

Monitoring and Benchmarking A4		A_{42}	5.7	0.002793	30
		A_{43}	32.0	0.01568	20
		A_{44}	12.6	0.006174	26
SLA A5	6.5	A_{51}	3.3	0.002145	31
		A_{52}	4.6	0.00299	29
		A_{53}	34.5	0.022425	14
		A_{54}	27.4	0.01781	18
		A_{55}	15.7	0.010205	23
		A_{56}	5.9	0.003835	28
		A_{57}	8.6	0.00559	27
Computational Framework A6	39.0	A_{61}	15.1	0.05889	6
		A_{62}	35.3	0.13767	1
		A_{63}	24.1	0.09399	3
		A_{64}	4.5	0.01755	19
		A_{65}	7.7	0.03003	11
		A_{66}	13.3	0.05187	7

Table 6.5: ESC local and global weight

Characteristics	Local Weight %	Elements	Local weight %	Global Weight %	Ranking
Load Balancing and availability C1	5.3	C_{11}	34.8	0.18444	21
		C_{12}	11.1	0.05883	30
		C_{13}	16.6	0.08798	28
		C_{14}	23.6	0.12508	25
		C_{15}	14.0	0.0742	29
SSO C2	24.0	C_{21}	10.6	0.2544	15
		C_{22}	30.0	0.72	3
		C_{23}	25.7	0.6168	5
		C_{24}	18.6	0.4464	8
		C_{25}	15.1	0.3624	10
Life Cycle C3	11.7	C_{31}	11.4	0.13338	24
		C_{32}	20.6	0.24102	17
		C_{33}	26.4	0.30888	14
		C_{34}	41.6	0.48672	6
Privacy C4	8.1	C_{41}	18.9	0.15309	23

		C_{42}	28.5	0.23085	20
		C_{43}	11.9	0.09639	27
		C_{44}	40.7	0.32967	11
Standard C5	36.2	C_{51}	12.4	0.44888	7
		C_{52}	17.7	0.64074	4
		C_{53}	9	0.3258	12
		C_{54}	6.9	0.24978	16
		C_{55}	31.1	1.12582	1
		C_{56}	23.1	0.83622	2
Risk C6	14.8	C_{61}	7.1	0.10508	26
		C_{62}	15.6	0.23088	19
		C_{63}	27.4	0.40552	9
		C_{64}	12.2	0.18056	22
		C_{65}	21.5	0.3182	13
		C_{66}	16.2	0.23976	18

Selecting suitable and most relative trust elements are essential to creating a successful cloud identity for associated decision makers and meeting planners. Although the part has contributed to identifying many of the selection trust elements and make them assist the best CIdP trust framework. Viewing the selection of a CIdPs as an MCDM problem, the relative importance of each affecting factor can be effectively obtained using MCDM approaches. Therefore, this part has evaluated the critical criteria (Attributes, Characteristics, and elements) affecting the decision making of CIdP selection (CIdUs) and furthermore proposes an AHP model for them to evaluate CIdP selection. The advantage of the relative importance scale (Rank) and the research artefact (application) for CIdP selection by allowing decision makers to structure their unique problems into priority weights, which can reflect their priority considerations (user weight).

Besides the using Saaty scale model in this research, to check the validity of the result, other AHP scale methods (Goepel & Performance, 2017) similarly has been utilised as depicted in figures 6.5 and 6.6. This method assists the research to validate the data by using different AHP scale methods (Linear, Log, Sqrt, InvLin, Balanced, Power, Geom). Consequently, different scales have been used to translate interviewees into ratios (figure 6.5 and 6.6). It makes a new approach to compare different scale functions to derive the most important trust characteristics and attributes for the research artefact. From the figures 6.5 and 6.6, it can be observed that using seven AHP scale methods reveal the consistency result as no line crossing between the CIdP characteristics and trust attributes for all seven methods.

Not surprisingly, for this part, the researcher can now evaluate the artefact (Trust Framework Application), whereas aligned with the most important trust elements for the expert (interviewee). Based on the result for this part the application (trust framework) should measure the trust elements which are essential for the real CIdUs. Compared to other elements, the absolute weight of characteristics and attributes are the highest because all experts believe that these elements can significantly contribute to CIdP trust framework. This finding is in line with the view of artefact application (chapter five) trust measurements which effectively measure all essential trust elements.

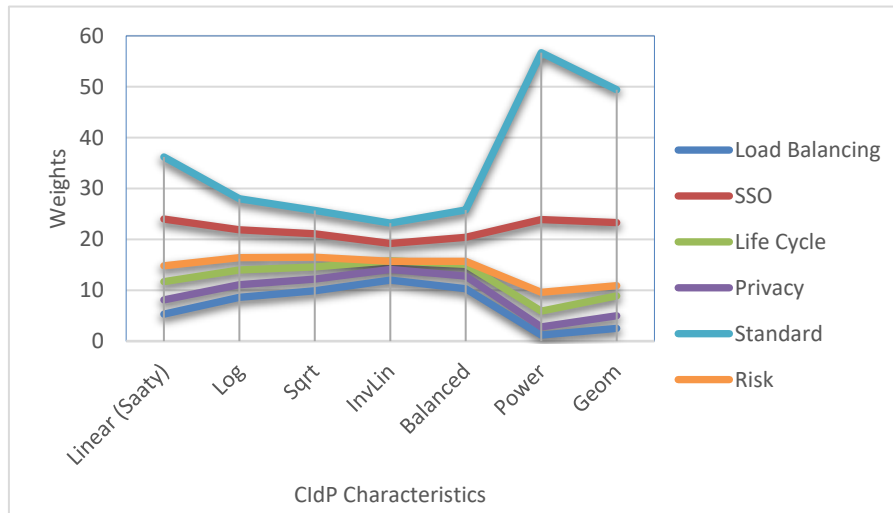


Figure 6.5: ESC and AHP scale methods

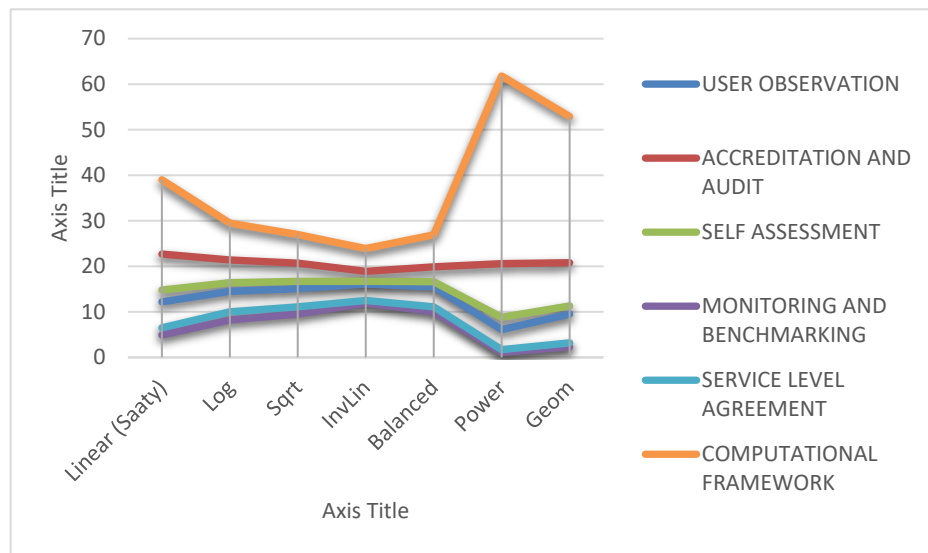


Figure 6.6: ESA and AHP scale methods

6.2 CLOUD IDENTITY STANDARDS AND GUIDELINES

As it has been identified, IAM is crucial part of the CC. However, application access, subscriptions, and physical access are the main criteria that should be covered by the cloud identity system architecture. Therefore, in regards of protecting user's information and identity, federal state, private organisations, and local agencies spend billions of dollars and go to great lengths to protect their digital access while at the same time trying to comply with legislation.

Three guidelines have been selected for this stage. 1) NIST 7874, 2) ENISA- Standardization in the field of Electronic Identities and (Trusted Service Provider) TSPs, and 3) CSA- IAM are the three best practices for identity environment. Therefore, this part will elaborate and discuss in detail, three ENISA legislative

Acts: ENISA auditing framework for TSPs, Standardisation in the field of electronic Identities, and Security framework that focus on trust identity service providers. Also, two IAM guidelines (CSA and NIST) that address the significant business and technical decisions that need to be considered by an organization seeking to implement the IAM component of Security as a Service (SecaaS) as part of the cloud environment, or an organization that is looking for guidance as to how to assess an IAM offering. It helps this research to be validated by comparing the criteria of these standards, and the research artefact tested as described in chapter three.

CSA Identity and Access Management guidance depicted that IAM includes processes, people, and systems are used to manage access to a provider's resources by assuring the identity of the customer's verification. Next, based on the least privilege policy, the correct level of access based on the protected resource is important and vital for both customers and providers. This guidance deliberates the significant technical and business decisions that need to be considered by a provider seeking to implement the IAM component to gain SecaaS as part of their environment. It is meant to serve as a source of reference for best practices in the industry today. Moreover, this guidance addresses personnel involved in the identification and implementation of the IAM solution in the cloud. It is of interest to those with the responsibility of designing, implementing and integrating the consumption of services of the IAM function within any cloud application of SecaaS.

On the other hand, ENISA Standardization in the Field of Electronic Identities and Trust Service Providers, strengthens the provisions for interoperability and mutual recognition of electronic identification schemes across borders, enhances current rules for electronic signatures and provides a legal framework for other types of trust services such as but not limited to electronic delivery services, electronic documents, electronic seals, website authentication, and time stamping services. This guideline explains why standards are important for cybersecurity, specifically in identity and TSPs. Some challenges associated with the definition and deployment of standards in cybersecurity are discussed in relation to standardisation activities associated with identity and TSPs.

The ENISA, NISTIR 7874 Guidelines for Access Control System Evaluation Metrics has provided Federal agencies with background information on

IAM properties, and to help IAM experts improve their assessment of the proper level security systems. This guidance also, discusses the performance, enforcement, administration, and support properties of IAM mechanisms. Even though this document covers most of the essential Access Control properties, the listed properties are not necessarily complete.

6.2.1 Standards' Comparisons

The CSA, NIST, and ENISA standards present the comprehensive and overlapping identity security features. From a wide array of security provisions perspective, CSA addresses all aspects of IAM technology and security. To fully grasp the overlapping information systems security features among the three-identity security standards, it has to compare the detailed essential system Characteristics provisions. Analysing data gathered by qualitative means involved sifting data, filtering out the significant information, identifying patterns, and constructing a framework for communicating the essence of what is revealed.

Based on the (Haley et al., 2017) analysing, qualitative data is a process of bringing structure, order, and meaning to the mass of collected data is often a vague, muddled, and time-consuming process. Moreover, qualitative data analysis assists to find the relationship between categories and themes of data. Furthermore, qualitative data is characterised by its richness, subjectivity, and comprehensive text-based information.

Traditionally, researchers utilised coloured pens to sort and then cut and categorised data; but nowadays, the qualitative data analysis software (NVIVO) is developed to manage the 'coding' procedures and is considered the best in this regards (Houghton et al., 2017). This software has an advantage in managing data and ideas, querying data, modelling visually and reporting. Overall, the qualitative researcher is strongly advised to pursue the use of this software in order to ease the muddled, vague and time-consuming tasks. It helps this thesis to organise and manage material and find insights in its data and analyses them based on the findings. In this regard, figure 6.7 shows the qualitative data analysing methodology

for the most frequently occurring words in the standards. In this step, similar words also have been considered. Figure 6.8 shows the most frequent word of CSA IAM standard.

Table 6.6: Identity standards overlaps and differences

ESC	NIST 7874	Weight	ENISA	Weight	CSA	Weight
Balancing	No	0	No	0	No	0
Single sign-on	Yes	3	No	0	Yes	23
Lifecycle	No	0	No	0	No	0
Privacy	Yes	23	Yes	4	Yes	5
Risk	Yes	4	yes	5	Yes	29
Standards	Yes	8	yes	20	Yes	14

Table 6.7: Identity standards and their most frequent words

NIST 7874	Weight	ENISA	Weight	CSA	Weight
Policy	415	Security	125	Access	271
XACML	81	Standard	177	Cloud	267
System Access	431	Trust	51	Security (SecaaS)	284
Control	99	Signature	109	Identity Management	319
Rules	77	Algorithm	28	IAM	109
Security	58	Certificate	19	Control	60

6.2.2 Discussion and Analysis of the Result

As CIdPs deliver a unified, standards-based platform designed to support enterprise hybrid information technology environments, from multi-factor authentication and single sign-on to access security, directory and data governance, their capabilities work together to give CIdUs secure access to the cloud, mobile and on-premises applications that they need. The CIdP's mission is to secure and streamline the user experience from sign-on to sign-off, and scale to support hundreds of millions of identities across the world.

Therefore, these providers begin to tackle and adopt the comprehensive CSA IAM, NIST, and ENISA identity provisions and standards, and based on the present thesis's findings; there is a comprehensive common identity-based feature base that cuts across all three guidelines and standards. Because CSA IAM covers an extensive number of public and private identity features, consequently, organisations can surely save time and resources by implementing wide-reaching

tools for CSA compliance. The private and public sector would greatly benefit from research and development funding of similar efforts for the implementation of NIST and ENISA identity features that could be used by agencies. Standardization has traditionally proven its value as a cost-saver and quality improver, and the field of identity and access is no exception.

NIST has a comprehensive set of identity guidelines focused on the U.S. information security environment, but it should not overlook the equivalent and wide-reaching European potential of ENISA-Standardization in the field of Electronic Identities and TSPs. As it evolves, proves its efficiency, and gains the approval of and adoption by the European community, it will introduce provisions not included in the NIST bibliography, and it will also provide a fresh information security perspective with a European outlook.

The no-nonsense international identity approach adopted by CSA adds the structure of this standard's approach with Consensus Assessments Initiative (CAI) and Consensus Assessments Initiative Questionnaire (CAIQ). Moreover, the CSA IAM Standards Council continues its rigorous information security activities and looks increasingly promising in producing additional identity privacy, trust, and security standards (see table 6.8 and 6.9).

CSA IAM is more than adequately covered by NIST and NISA provisions contained in its special IAM (Access, Cloud, Identity, SecaaS, and control objective). However, the CSA main challenge lies in maintaining information privacy (5 compared with 23 of NIST). Therefore, the legislative act's provisions are complex and open to legal interpretation, and they require further development to standardise and streamline with rules and policy (see table 6.9).

Moreover, the tables 6.8, 6.9, and 6.10 are presenting the overall analysing of the guidelines. The deeper insight into the guidelines and relation between the trust frameworks and elements. These tables reveal that most common guidelines in the cloud and cloud identity also align with the deliverable of this research, and consequently, verify and validate the elements as well.

Table 6.8: ENISA and its relevant with ESC and ESA

Name	Files	References
A1 USER OBSERVATION	1	95
A2 ACCREDITATION AND AUDIT	1	114
A3 SELF ASSESSMENT	1	69
A4 MONITORING AND BENCHMARKING	1	98
A5 SERVICE LEVEL AGREEMENT	1	77
A6 COMPUTATIONAL FRAMEWORK	1	572
C1 BALANCING	1	110
C2 SSO	1	7
C3 LIFE CYCLE	1	93
C4 PRIVACY	1	116
C5 STANDARD	1	90
C6 RISK	1	233

Table 6.9: CSA IAM and its relevant with ESC and ESA

Name	Files	References
A1 USER OBSERVATION	5	1,4,1,6
A2 ACCREDITATION AND AUDIT	0	-
A3 SELF ASSESSMENT	0	-
A4 MONITORING AND BENCHMARKING	1	2
A5 SERVICE LEVEL AGREEMENT	0	-
A6 COMPUTATIONAL FRAMEWORK	1	2
C1 BALANCING	1	1
C2 SSO	4	5,7,1
C3 LIFE CYCLE	1	3,2
C4 PRIVACY	2	1
C5 STANDARD	5	6,2,1,9
C6 RISK	2	9,14

Table 6.10: NIST and its relevant with ESC and ESA

Name	Files	References
A1 USER OBSERVATION	7	19,72,123,24,65,28,77
A2 ACCREDITATION AND AUDIT	2	2,14
A3 SELF ASSESSMENT	2	2,257
A4 MONITORING AND BENCHMARKING	5	27,53,51,81,84
A5 SERVICE LEVEL AGREEMENT	8	72,73,68,70,64
A6 COMPUTATIONAL FRAMEWORK	6	122,60,64,35,68,79
C1 BALANCING	6	9,43,116,68,79
C2 SSO	5	71,110,17,103,67
C3 LIFE CYCLE	5	7,110,90,168,656
C4 PRIVACY	5	47,65,15,64,137
C5 STANDARD	7	54,29,41,5,101,82,3
C6 RISK	7	110,80,5,20,125,42,31

NVIVO and deep observation of the most relevance areas in the findings suggests that A guideline is aligning with the result, however, the B guideline is not aligning and covering the all elements and attributes, but, the C guideline is aligning and covering all characteristics and attributes of the cloud identity framework. As is shown in all the tables, the number of the relevant attributes is shown in the Files field. It shows the number of the attributes and sub-attributes covered by the guidelines, therefore, the higher number means, the higher alignment and relevancy.

Along with this, in order to have a better understanding of strength of relationship between guidelines and criteria, the researcher ran the analysis between standard (sample of the criteria) and guidelines. As a result, figure 6.9 shows that CSA is focusing on the x.500 and OASIS while ENISA is focusing on Federal Information Processing Standard (FIPS), SHA and cryptography (figure 6.10). On the other hand, figure 6.11 indicates that NIST guideline is concerned with XML and XACML standards with regard to access control formal methods. Overall these figures show that the standard is the vital part of the guidelines and also, they are accepting these standards from different perspectives and methods. Therefore, all

of these guidelines validate the using of standards as a vital criterion when choosing trustable identity providers.

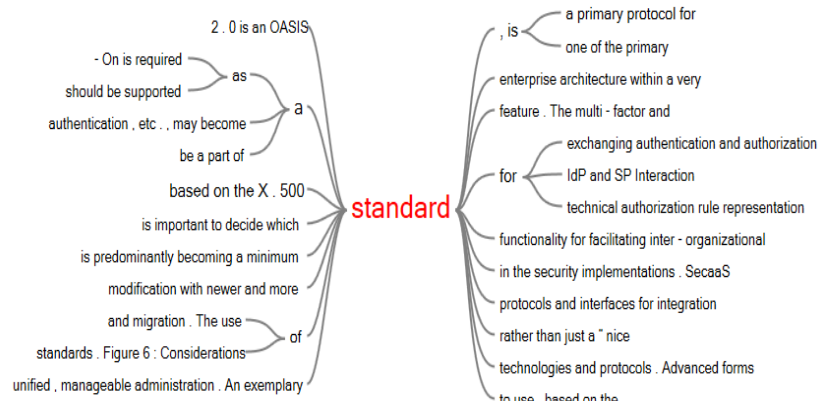


Figure 6.9: NVIVO text search criteria (CSA and Standard)

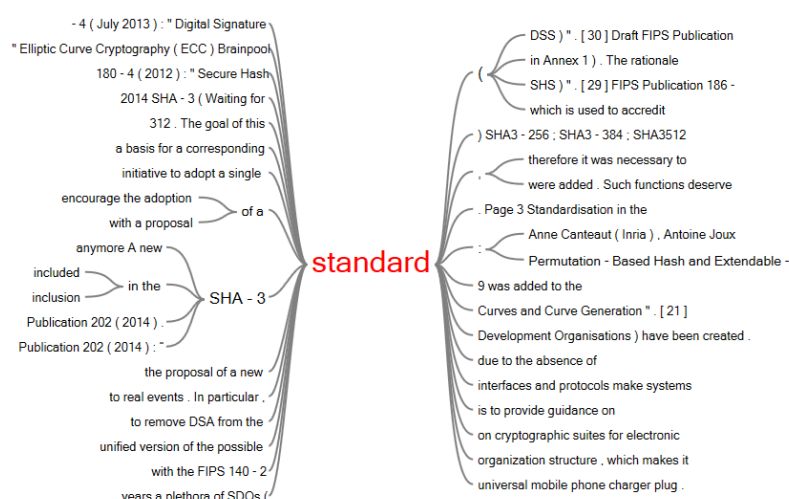


Figure 6.10: NVIVO text search criteria (ENISA and Standard)

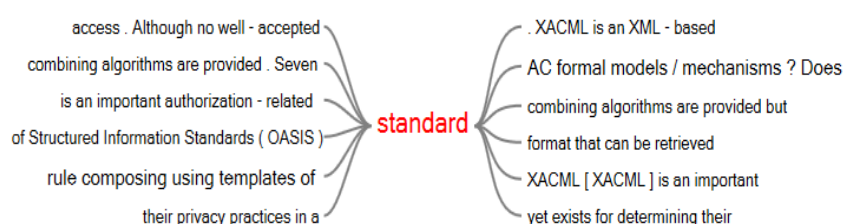


Figure 6.11: NVIVO text search criteria (NIST and Standard)

NVIVO by the enabling the analysing the particular criterion helps the researcher to identify the rational and relevant links between the guidelines, ESAs, and ESCs as summarised below:

- CSA believes that combination of SAML and WS brings trust, however, ENISA is believing that combination signature and validate application is the method to bring trust. On the other hand, NIST believes that security

check, functional privacy, and schema XML are providing trust for the CIdPs.

- In the audit, CSA believes that monitoring security event, collection of forensic evidence, regulatory, and policy compliance are vital, however, ENISA is assuming that recommendation and governance are essential, but NIST believes that audit by the customised information is providing the capabilities for the trust management frameworks.
- In the monitoring, CSA is proposing monitoring the cloud resources for the user access and privileged access, however, NIST believes that monitoring is the efficient method for the trust management frameworks with dynamic compliance function.
- In the SLA perspective, CSA believes that SLA is the vital agreement to have an appropriate trust framework.
- CSA advise the CIdP to align with IAM SaaS, industry standards, adopting token to gain security, but, ENISA is recommending using Information Security Management System (ISMS), trusted list providers with their signature for the trusted providers, on the other hand, NIST is advising to enable a richer set of security by enterprise management, distributed system and multi-level policies.
- On the point of the privacy, CSA shows that the geographical location of provider is the main issue for the privacy, but European privacy of information is the response to this issue. However, ENISA is assuming that privacy is enhancing the trust and perceived as a vital element for trust framework, on the other hand, NIST believes that privacy management for both user and provider enable providers to be in the best compliance.
- CSA advise the CIdP to quantify the risk exposure and residual risk to enforce segregation of duties, but, ENISA believes that risk management is a requirement for the trustworthy providers, on the other hand, NIST is identifying the critical access control decision, application level, and policy rules are the main risks for providers.
- On the point of SSO, CSA shows that SSO requires to work seamlessly for any provider; however, ENISA is promoting the SSO for cyber security product, on the other hand, NIST shows that to meet the trusted access

control requirement, current authentication system should achieve the SSO characteristics.

- CSA shows that network connectivity issues such as DDoS attack might jeopardise the availability of the provider; however, ENISA believes that availability, elasticity, and load balancing still is the remaining issues of the identity providers.

Overall, this analysis is providing this thesis with validity based on the available cloud identity standards. Moreover, it is allowing CIdUs to make more knowledgeable decisions while selecting potential Identity standards that best suits their functional and security requirements. In addition, it shows that the field of identity and access domain is in an evolutionary flux. Therefore, there is more work to be accomplished. It will require the collaboration and the consensus of identity, trust, and security stakeholders worldwide.

6.3 FEASIBILITY VALIDATION

The main goal of the evaluation is to demonstrate the applicability and technical feasibility of the contributions in the domain of the thesis (Cloud and cloud identity environment). In this regard, after the implementation of the proposed artefact and checking the usability of the artefact, is challenging the feasibility of the artefact by applying threat modelling (Widiantari & Budiman, 2018).

Therefore, to measure the result of the feasibility checking in this thesis the qualitative data obtained from threat modelling methods which are aligned with the Security Development Lifecycle (SDL) are used (Felderer & Katt, 2015). Thus, this section identifies the threat modelling and attack patterns conducted aiming to validate the feasibility (Tormo et al., 2015) of the artefact solution.

In this regard, developing a use case (first assumption for the artefact) helps to identify the artefact issues from the perspective of attackers. It also allows the researcher to decide and document how the artefact should react to mitigate the issues. Therefore, it is validating the feasibility of the research. In the following section, a conceptual threat model based on the STRIDE threat modelling tool for Ouath2.0 (scenario) is presented, as one of the most common federate identity management system. For this, the set Data Flow, Datastore, External Interactor, Process, and Trust Boundary are used to create a data flow diagram of the Ouath2.0 scenario. This proposed model will be tested to effectively mitigate the threats and

resolve identity theft, misuse of identity information, and trust relationship concerns in federated identity management system.

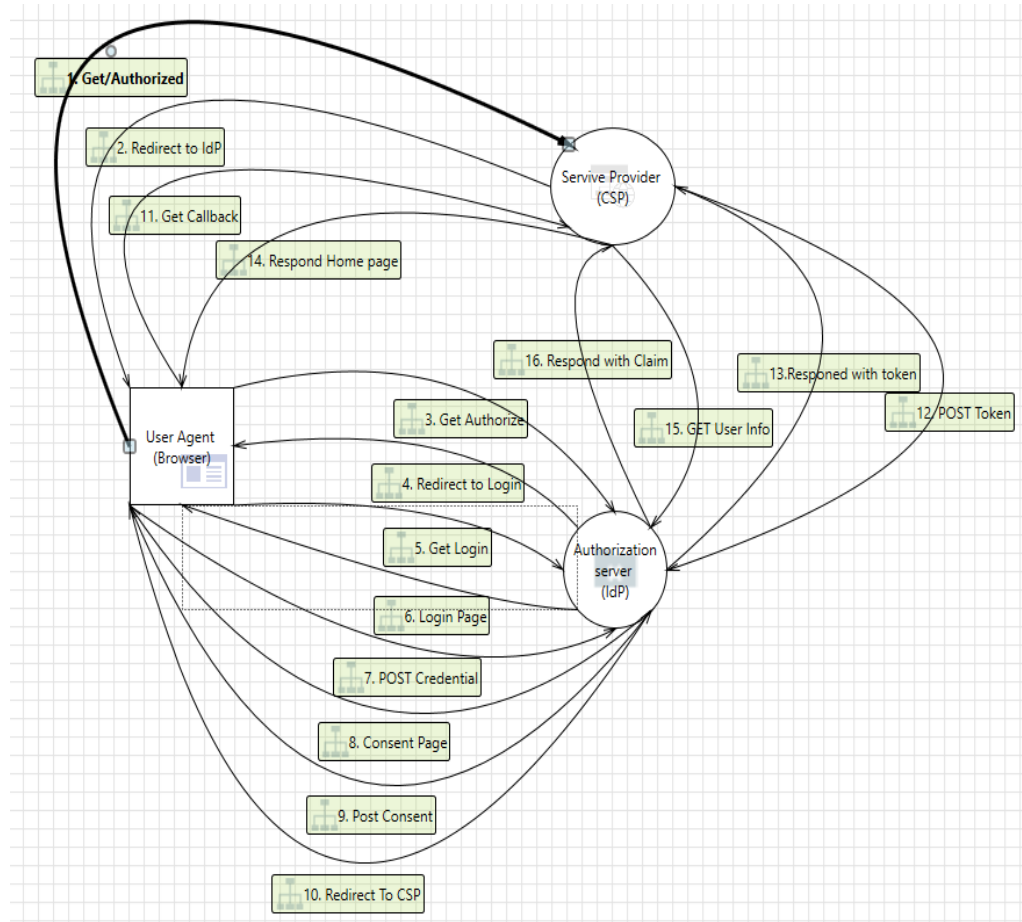


Figure 6.12: Oauth2.0 data flow diagram

The section discusses a method for checking the feasibility of the thesis artefact based on the threat modelling and attack patterns (Yuan et al., 2015). To do so, a comprehensive threat modelling exercises based on the Oauth2.0 protocol is performed by using popular threat modelling (STRIDE threat modelling 2016) (Scandariato et al., 2015) methods, including STRIDE threat modelling with respect to the attack tree, attack surface, and attack graph (Manzoor et al., 2018).

Therefore, in the first step, the potential artefact threats are analysed by following STRIDE's threat modelling process. Based on the identified threats (Amini et al., 2015), the initial artefact (abuse case) is generated. Next, the attack pattern library is searched, and attack patterns relevant to the artefact are retrieved. The information retrieved from the attack patterns are used to extend the initial artefact and suggest mitigation methods. Therefore, this method has the capability

to help the researcher to validate the artefact properly, and therefore mitigate the identity theft which is a main objective for this thesis.

6.3.1 Threat Modelling

STRIDE threat modelling is ranked for identifying risks to architecture and design level artefacts which is the main objective for this method use. Yuan et al. (2015) stated that hypothesising potential security threats, evaluating the threats, ranking the threats, and suggesting mitigation strategies are four steps in the threat modelling which is considered in this thesis. However, the STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege) is the security threat model which is utilised. Table 6.11 illustrates the rationale between the DFD elements and STRIDE threats. Therefore, based on these assumptions, in this section artefact evaluation and trust framework validity is based on the four activities, which are briefly described.

Table 6.11: DFD and the STRIDE threat types

DFD	STRID
Data Flow	Tampering, Information Disclosure, Denial of Service
Data Stores	Tampering, Information Disclosure, Denial of Service
Processes	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege
Interactors	Spoofing, Repudiation

In order to validate the results and findings, in step 1, the data flow diagram of the Ouath2.0 is modelled as depicted in figure 6.12. This model is based on the Ouath2.0 data flow in the (Fett et al., 2016) which defined the protocol's scope to be analysed, and consequently, produce a model of the system to be used for the elicitation of the threats. Figure 6.13 shows the Ouath2.0 DFD layer 0, which is a representation of the Cloud IAM system. In this study, level 1 DFD will not be discussed as per the complexity and diversity of the implementation model

(Dhillon, 2011). Figure 6.13 shows the sixteen steps of information exchange between the user, CSP, and CIdP.

Threat Modeling Report

Created on 9/06/2018 10:59:50 PM

Threat Model Name: AUT Digital forensic Lab

Owner: Eghbal Ghazizadeh

Reviewer: Dr. Brian Cusack

Contributors:

Description: OAuth 2 is an authorization framework that enables applications to obtain limited access to user accounts on an HTTP service, i account. OAuth 2 provides authorization flows for web and desktop applications, and mobile devices.

Assumptions:

External Dependencies:

Threat Model Summary:

Not Started	98
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	0
Total	98
Total Migrated	0

Diagram: Oauth2.0

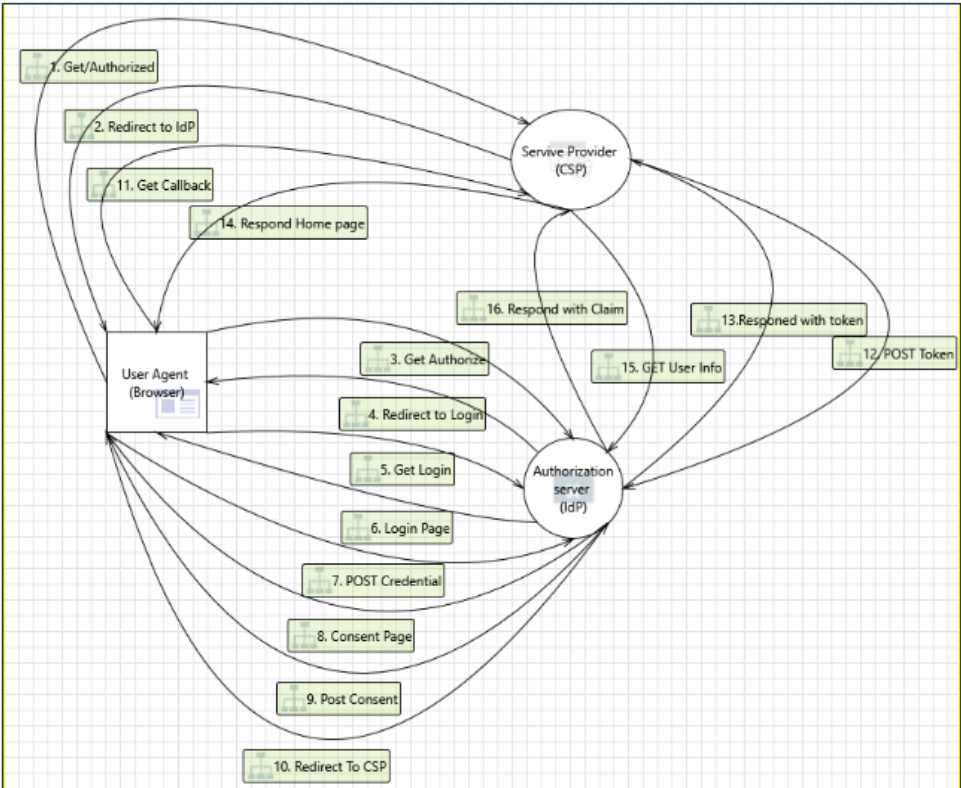


Figure 6.13: Oauth2.0 threat modelling report

Next, in step 2, based on the table 6.11, the DFD elements mapped with the STRIDE threats. Thus, every Oauth2.0 element has been connected and related to one or

more threats as mentioned in the table 6.12. STRIFDE threat analyser 2016, has been utilised in this step to map the steps with the threats.

In step three, the threat modelling tool analysed the view of the DFD regarding elicit the threats and provide a better view of the relation between the data flow, data store, external interactor, process, and trust boundary. Figure 6.13 illustrated the full Ouath2.0 threat modelling report (98 threats) by considering: Not started, Need Investigation, Not Applicable, and Mitigated threat.

As the figure 6.13 shows, STRIDE threat modelling provides very long (98 threats) lists of threats (organised by the six threat categories) that the researcher had to select for the trust framework for the system under analysis (Ouath2.0).

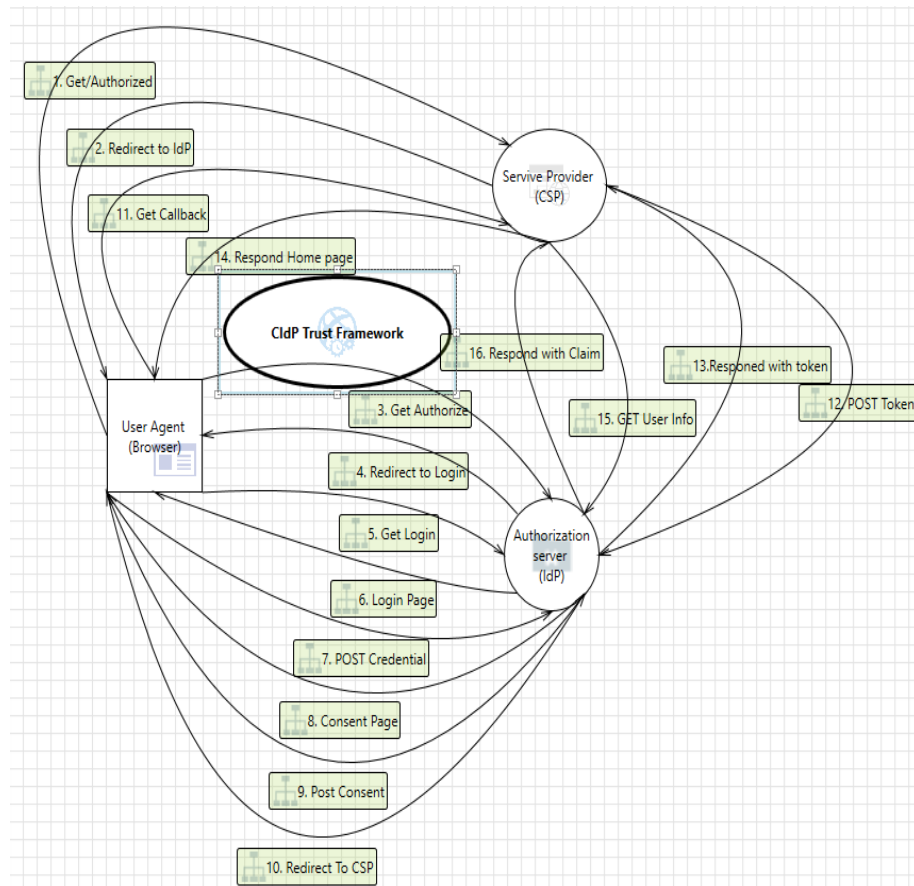


Figure 6.14: The CIdP trust framework concept

In this part, to validate the feasibility of the artefact, it has been applied the propose trust framework concept as discussed in section 3.2 and has pictorial representation of the proposed model illustrated in the figure 6.14. The main point to analyse is whether this proposed model could mitigate identity theft by proposing a solution for all the mentioned threats in the STRIDE threat modelling tools, and consequently, in the analysing view to get approval by the threat report.

Therefore, based on the threat list in the report (figure 6.13), abuse case (the list of the attack (table 6.12) can be identified (Yuan et al., 2015). Accordingly, Justification, as well as possible mitigation of the threats, have been identified and explained. Finally, as per SDL phases (Diagram, Identify threats, mitigate, and Validate) (Potter, 2009), all the mitigation methods have been validated by the reviewer of the threat report (Main Supervisor and reviewer of the thesis). On the other hand, as a contribution for this thesis, this method leverages the knowledge base of STRIDE threat modelling and Ouath2.0 attack patterns with the goal of validation of the proposed artefact, to develop meaningful and useful trust framework, as well as mitigating identity theft. The summary shows, the researcher, first identified the list of the methods to prevent attacks and consequently mitigate the threats. However, in the justification, it has been justified how these techniques provide a trustable and secure environment. Moreover, in the last column, relevant trust framework elements, it has been identified the rational between the proposed model and mitigation threats.

6.3.2 Discussion and Analysis of the Result

In this section, the method for evaluating the feasibility of the trust framework. The method builds on techniques, metrics, and guidelines from STRIDE threat modelling and more recent work in ubiquitous threat modelling. However, the goal of the section is to provide a method to challenge the feasibility of the thesis propose method and identify the threat justification of the scenario threat modelling (Ouath2.0), key areas of possible mitigation, and relevant keys between the CIdP trust frameworks.

While the feasibility method in this thesis is based on STRIDE threat modelling, it is believed that the threat mitigation plan is the foundation for developing feasibility metrics for cloud trust frameworks. Thus, the goal is to develop a method to ensure all the threats are mitigated by the artefact and get approval for this plan from the reviewer of the method as a final cycle of the SDL.

Table 6.12: Threat list, properties, and mitigation method by using the propose model (Interaction: 1. Get/Authorized)

Category	Description	Justification	Possible Mitigation	Relevant Trust Framework elements
Denial of Service	An adversary can perform an action on behalf of another user due to lack of controls against cross-domain requests.	These techniques can change data and functions on behalf of the user to mitigate Cross-Site Request Forgery Vulnerabilities. Moreover, they can overflow/deny service to process spam data.	Include the unique token in a hidden field. CAPTCHA. ESAPI (Enterprise Security API). Intrusion detection APIs. Filtering. Parameterized API. White-list validations. Monitor use resource. Monitor bandwidth throttling. Validate and filter input.	$A_2, A_3, A_4, A_6,$ C_{22}, C_{51}, C_1
Elevation of Privileges	An adversary may bypass critical steps or perform actions on behalf of other users (victims) due to improper validation logic.	Least privilege, the minimum required access with considering granularity of access prevents bypassing the access control system.	The principle of least privilege Use least privilege accounts. Consider granularity of access. Enforce separation of privileges. Use multiple gatekeepers. Secure system resources against system identities.	$A_2, A_3,$ C_1, C_2, C_3, C_6
Information Disclosure	An adversary can reverse weakly encrypted or hashed content.	These methods bring appropriate access control mechanisms deployment; therefore, only authorised users can access to data.	Strong authentication. Encryption.	$A_1, A_2, A_3, A_5, A_4, A_6,$
Information Disclosure	An adversary may gain access to sensitive data from log files.	These methods bring encryption for all	Cryptographic protocols.	C_2, C_3, C_4, C_5, C_6

Information Disclosure	An adversary may gain access to unmasked sensitive data such as credit card numbers.	sensitive data either in storage or during transit, therefore, only authorized users read this sensitive data.	Secure communication links. Single logout among applications and keep-alive.	
Information Disclosure	An adversary can gain access to certain pages or the site as a whole.	These methods bring secure communication links with protocols that provide message confidentiality.	Consumer education. Data filtering.	
Information Disclosure	An adversary can gain access to sensitive data by sniffing traffic to Web Application.	Random Number Generator (RNG), and Windows Data Protection API (DPAPI) methods prevent access to sensitive data from uncleared browser cache.	Escape all untrusted data based on HTML content.	
Information Disclosure	An adversary can gain access to sensitive information through error messages.		Loss of decryption keys. Do not store secrets in software. Encrypt sensitive data over the network.	
Information Disclosure	An adversary may gain access to sensitive data from the uncleared browser cache.		Secure the channel. Use RNG cryptography method. Use DPAPI. Periodically change your keys.	
Repudiation	An attacker can deny the malicious act and remove the attack footprints leading to repudiation issues.	All activities (such as successful and unsuccessful authentication) and sensitive data (e.g. cookies and authentication credentials) must be logged and recorded to prevent the non-repudiation.	Secure audit trails. Digital Signature. Identify malicious behaviour. Know the baseline. Know what good traffic looks like. Use application instrumentation to expose behaviour that can be monitored.	A_1, A_2, A_3, A_4, A_6 C_2, C_5, C_6
Spoofing	An adversary can get access to a user's session due to improper logout and timeout.	These techniques provide the secure channel with the encrypted credential to prevent get access by an adversary, steal cookies,	Strong authentication. Encryption.	A_1, A_2, A_3, A_4, A_6 C_2, C_5, C_3, C_6

Spoofing	An adversary can get access to a user's session due to insecure coding practices.	phishing, pharming, and spoof user agent.	Cryptographic protocols. Consumer Education. Data Filtering. Escape all untrusted data based on HTML content. Follow Security Requirements. Follow Secure Password Policies. Implement Account Locking. Disable “Auto-logons” Mutual Authentication. Avoid download from unreliable Source. Biometrics or multi-factor authentication mechanisms. Cryptographic protocols such as TLS/SSL. Do not store credentials. Use authentication mechanisms that do not require clear text credentials. Separate anonymous from authenticated pages.	
Spoofing	An adversary can get access to a user's session due to insecure coding practices.			
Spoofing	An adversary can get access to a user's session due to improper logout and timeout.			
Spoofing	An adversary can spoof the target web application due to insecure TLS certificate configuration.			
Spoofing	An adversary can steal sensitive data like user credentials.			
Spoofing	An attacker can steal user session cookies due to insecure cookie attributes.			
Spoofing	An adversary can create a fake website and launch phishing attacks.			
Spoofing	An adversary may spoof User Agent (Browser) and gain access to Web Application.	These techniques improve the web application security as well the communication security; therefore, all confidential data must be hashed and signed to ensure that the data is valid (untampered and came from the correct/expected source).	Role Based Access Control (RBAC) Strong authorisation. Data hashing and signing. Secure communication links.	$A_2, A_3, A_6, A_5,$ C_2, C_3, C_5
Tampering	An adversary can deface the target web application by injecting malicious code or uploading dangerous files.			
Tampering	An attacker steals messages off the network and replays them in order to steal a user's session.			

		Moreover, by using these methods, the attacker cannot steal the message and perform the SQL injection.	Filtering. Parameterized API. ESAPI filtering APIs. Individual accountability. Validate input: length, range, format, and type. Constrain, reject, and sanitize input. Encode output. Strictly defined AC. Proper Validation.	
Tampering	An adversary can gain access to sensitive data by performing SQL injection through the Web App.			
Tampering	An adversary can gain access to sensitive data stored in Web App's config files.			

As it has been found in the previous chapter, OpenID is a user-friendly method to eliminate additional sign on in the foundation of the security environment. Despite all the advantages of this method, it introduces the complexity of the authentication, authorisation, session coordination, and user interface. Central encrypted token with Standard Secure Token (STS) is the method to integrate with OpenID and SAML to secure them. Overall, if the researcher wants to summarise the threat tables, Non-secure session management, Malicious Data Injection, Bypass the Authentication, and Elevation of the privileges are the most common issues with this SSO design. The researcher came to this point where the application of defence in depth, implement with adequate strength, compliant with standards and regulation, protect data in the storage, apply security by default, Role Based Access Control, and enforce minimal trust are the common methods to mitigate these threats.

In this regard, in the figures 6.12 and 6.13, it has been shown that the data flow diagram and threat report of the scenario illustrate mitigation effects. Furthermore, table 6.11 presented the user identity and identity information threatened in the open networks (CC) especially via the scenario Ouath2.0. It has used the STRIDE threat method by assisting STRIDE threat modelling to identify and understand the existing threats such as but not limited identity theft (phishing, pharming), misused of identity information, and involvement of malicious users. Analysing the table and find the mitigating plan, and also, finding the role of the trust framework is the main contribution for this section. In this part, countermeasures are identified and relevant to: Interaction: 1. Get/Authorized, but it applies to Interaction: 11. Get Callback, Interaction: 12. POST Token, Interaction:13. Responded with token, Interaction: 15. GET User Info, Interaction: 16. Respond with Claim, Interaction: 3. Get Authorize, Interaction: 5. Get Login, Interaction: 7. POST Credential, and the Interaction: 7. POST Credential. As figure 6.14 presented CIdP trust framework is the solution to the threats explained in the table 6.11. However, based on this table, it is obvious that the artefact can resolve the interoperability and security of cloud by helping the cloud identity decision, whether they are good (protected in a secure manner) or bad (compromised to attacks). Therefore, the proposed artefact helps to establish a trust relationship between CIdU and CIdP by measuring the trust level of the CIdPs. It can also, helps the federated identity which is one of the main goals for the CIdPs and users.

6.4 CONCLUSION

This chapter focusses on the findings from the evaluation methods. These findings are used to validate the proposed method. Therefore, to identify the strengths and weaknesses of the proposed framework, four approaches have been adopted from chapter three. The evaluation result clearly showed that the problems of the proposed method and areas of improvement. So, it is required that the framework be dynamic to be aligned with the CC changes. Evaluating the artefact elements by using AHP (section 6.1), verification from the standards (section 6.2), and feasibility validation by using STRIDE threat modelling (section 6.3) approve that the framework is mitigating the identity theft of the cloud users (objective for this thesis).

Chapter seven evaluates the findings of the thesis. In the previous chapters, by using the novel methods, the researcher came to this point that the proposed method mitigates identity theft. Therefore, in the next chapter, the contributions of the employed mixed research methodology (figure 6.1) is critically evaluated for other researchers. The aim is to show the advantages of the methodology lifecycle and how this methodology helps to overcome research problems and deliver innovation and solutions. Therefore, to show this journey, it is important to identify the rationale between findings, research questions, and hypotheses by using a Quasi-Judicial method.

However, the rational argument is utilised to prove or refute the hypothesis in the analysis. On the other hand, chapter seven gives the final steps of the thesis based on the figure 6.1. Therefore, evaluation the result, scholarly publication, professional publication, and trust dissemination are the key points to be covered in chapter seven. Thus, research hypotheses evaluation, research question evaluation, implication of the results, contribution, and dissemination are the main topics in this chapter that cover all key points and give out the result of the thesis.

Chapter Seven

Discussion of Findings

7.0 INTRODUCTION

In chapter six, the artefact has been attested by using TDS methodology's evaluation approaches. Using these methods assists to validate the proposed framework as well as improve the trust features of the framework.

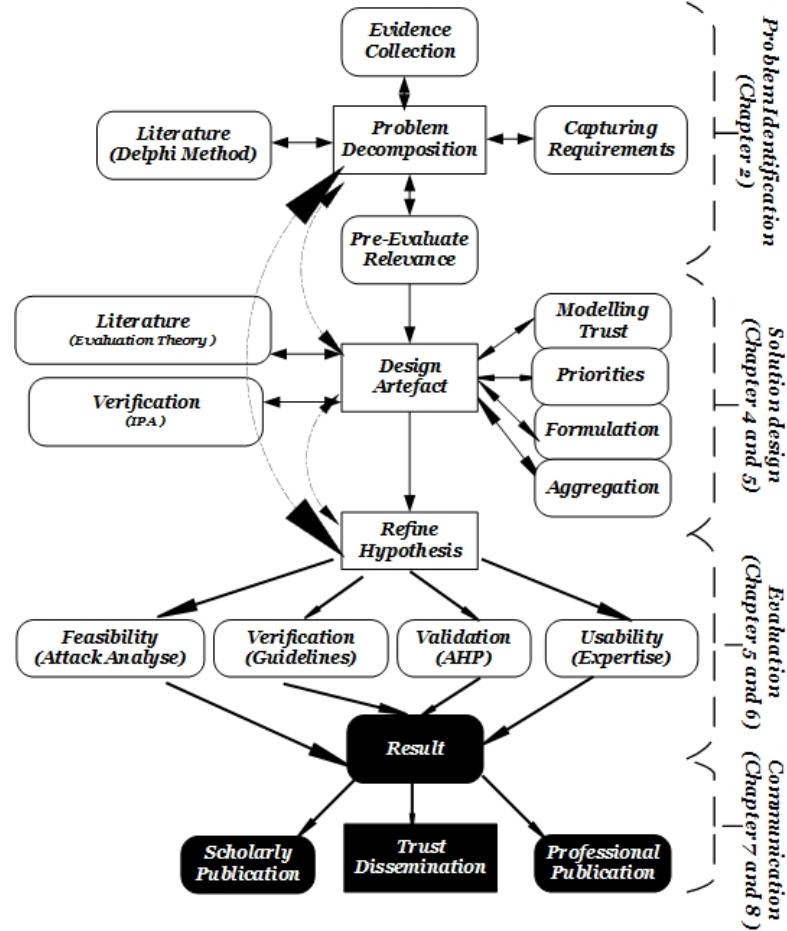


Figure 7.1: Chapter seven pathway

Figure 7.1 shows the plan for the thesis based on the proposed methodology, also the main topic of the chapter seven which is discussion of the thesis result. As mentioned in the section 1.2 the approach is to clarify the pathway and roadmap of the thesis by highlighting (black areas) the particular steps and sub steps to gain the main objective of the thesis. Therefore, this chapter is discussing the finding of the thesis based on the methodology which is the communication of the study (impact on the users as well as on the industry). In chapter five and six, by using the novel methods, the researcher came to this point that the proposed method mitigates the

identity theft. In this chapter, the contributions of the employed research methodology (figure 7.1) is evaluated for this thesis critical reflection. The aim is to show the advantages of the methodology lifecycle and how this methodology helps to overcome research problems to give innovation and outcomes.

Therefore, to complete the thesis journey, it is important to identify the rationale between findings, research questions, and hypotheses by using a Quasi-Judicial scholarly method. In the next sections, a rational argument is utilised to prove or refute the hypothesis and answer the questions. Also, the evaluation of the results in, scholarly publication, professional publication, and trust dissemination are the key points to be covered in this chapter shown in the communication step of figure 7.1. Thus, research hypotheses evaluation (7.1), research question evaluation (7.2), implication of the results (7.3), contribution (7.4), and dissemination (7.5) are the main topics in this chapter. They cover all key points and deliver the result of the thesis. On the other hand, this chapter is structured to take evidence from previous chapters and use them for qualitative testing. Moreover, by considering the result of section 7.1, the research questions are answered. The link between answers and hypotheses is discussed in the implication of the results, section 7.3. This chapter is analysing the theory and practical contribution to the body of the knowledge of the thesis. Finally, this chapter is concluding with the trust dissemination to the cloud customer by utilising the SAML method.

7.1 HYPOTHESES EVALUATION

The contributions of the mixed research methodology (trust and Design Science) is evaluated for this thesis study. Moreover, the four steps, Problem Identification, Solution Design, Evaluation, Innovation and the outcome of the study is discussed. In chapter three a set of hypotheses were formulated to test the researcher's artefact which developed from chapter two literature review. In this section, the rationale between questions, hypotheses and findings is evaluated from chapter two to chapter six. Moreover, the result from evaluation theory, expert feedback, AHP modelling, and threat modelling is discussed. However, the methodology for this part is based on the Quasi-Judicial (Cardozo, 2010) where the rational argument is utilised to prove or refute the hypothesis. The judgment argument against the hypothesis relies on the "for" weight of the judgment. Tables 7.1 to 7.3 summarise the hypotheses evaluation for this research.

Table 7.1: Hypothesis 1 evaluation

Hypothesis 1: A CIdUs' choice of CIdPs is going to be based largely on security, risk, and reputation.	
For	Against
<p>In chapter two, it has been concluded that the security, privacy, monitoring, and trust are the main issues of any CIdPs. Therefore, the CIdU decision is based on these criteria.</p> <p>Moreover, in chapter four, the evaluation theory indicated that ESA and ESC are crucial for CIdP's selecting by the CIdUs. On the other hand, tables 4.20 illustrated the weight and connectivity rate for elements of ESA and ESC. So, these tables have shown that CIdPs should improve the level of security, privacy and their reputation (Feedback, Standard, Self-assessment, Benchmarking, SLA) along with the IAM main characteristics (Load Balancing, SSO, Life Cycle, Privacy, Standard, and Risk mitigation) to have a higher chance to be selected by the CIdUs.</p> <p>In chapter five, first, the expert approved that security, mitigation of the risk, and well-known reputation would improve the chance of service provider selection. Moreover, in chapter six, the AHP method validates that these three factors are important for the CIdU's decision making. Besides, the guidelines also approved that in the best practices, these elements have the high priority for the cloud provider selection.</p>	<p>The thesis after systematic literature came to this hypothesis and even by refining the hypothesis in the other chapters, the Hypothesis 1 did not refute in all attestation methods. However, other method approved the security, risk, and reputation as the crucial criteria for any CIdU's decision making.</p>
<p>Goal > Verification from Literature Q1</p> <p>Goal > Verification from Guidelines Q1</p> <p>Goal > Verification from CIdUs&CIdPs Q1</p> <p>Goal > Element Validation Q1</p>	
Verdict: Accepted	

Delphi method (systematic literature), IPA method (chapter four), positive feedback from the interviewees (chapter five), Consistency Ratio and different scale method, identity standard overlaps (chapter six) are supporting the Hypothesis 1 and assist it to be accepted.	
--	--

Table 7.2: Hypothesis 2 evaluation

Hypothesis 2: <i>The modelling of a trust establishment in cloud identity needs to incorporate the ESA and ESC in order to produce a measurable trust relationship.</i>	
For	Against
<p>In chapter four, it has been mentioned that the user observation, Accreditation and Audit, Self-Assessment, Monitoring and Benchmarking, and Computational Trust framework are the modelling of trust establishment between CIdUs and CIdPs. Therefore, trust establishment needs to incorporate the ESA and ESC in order to produce a measurable trust relationship.</p> <p>In Chapter five, first, the expert approved that trust framework is depended on ESA and ESC. Moreover, in chapter six, the AHP method validates that these five trust frameworks are important to measure the trust relationship.</p>	<p>After refining the hypothesis in chapter four, the researcher came to this point that trust frameworks are incorporated with the trust elements. This hypothesis after refining in chapter five and six, did not refute in all attestation methods.</p>
<p>Goal > Verification from Literature Q2</p> <p>Goal > Verification from CIdUs&CIdPs Q2</p> <p>Goal > Element Validation Q2</p>	
<p>Verdict: Accepted</p> <p>IPA method in chapter four, positive feedback from the interviewees, Consistency Ratio, and different scale method are supporting Hypothesis 2 and assisting it to be accepted.</p>	

Table 7.3: Hypothesis 3 evaluation

Hypothesis 3: <i>The cloud identity trust framework facilitate trust making decision by cloud consumers.</i>	
For	Against
In chapter four, it has been prioritised the ESA and ESC elements. In chapter five, it has been illustrated by implementing the artefact, how to measure the trust elements derived from the chapter four. Consequently, in the chapter five, expert approved that the usability of the application (derived from the framework). Moreover, in chapter six, the STRIDE threat modelling, approve the feasibility of the framework by mitigating all possible threat and getting approval from the reviewer.	The feasibility and usability of the artefact has been added after chapter four. As per the methodology for this thesis refining the hypothesis is essential to be sure about the validity of the hypothesis. However, Hypothesis 3 did not refute in all attestation methods as explained in previous chapters.
Goal > Usability Assessment Q3 Goal > Feasibility Assessment Q3	
Verdict: Accepted Positive feedback for application (framework) usability from the interviewees in chapter five based on the implementation in chapter four; moreover, threat modelling results are supporting the Hypothesis 3 and assisting it to be accepted.	

7.2 RESEARCH QUESTION EVALUATION

This section is aiming to answer the research question. The research questions as stated in chapter three are:

1. *With respect to the Essential System Attributes (ESA) and Essential System Characteristics (ESC), how are the trusted-based relationship between CIdP and CIdU framed?*

2. *How is an evaluation done of the trust establishment framework from question one?*
3. *How might the framework from question one by using the evaluation method of question two affect the decision making of CIdUs and CIdPs?*

Therefore, as a part of findings, in this section, the relation between the result of the previous chapters with the research question is discussed to establish the research finding.

First, to answer question 1, it has been identified in chapter three based on the problem statement in chapter two, that a trust framework is essential to mitigate identity theft between CIdUs and CIdPs in order to protect the cloud user's identity. Using mixed trust and design science methodology (chapter three) helped to effectively make a trust framework between CIdPs and their users. In chapter four, by utilising the evaluation theory in the 4.6 (Synthesis Technique), it has been synthesised the current cloud trust frameworks along with the strengthens and weaknesses (figure 4.12). In the section 4.6.2, identified the most common trust frameworks with their essential system attributes. Figure 4.13 (ESA) and 4.15 (ESC) along with the modified IPA map for them (figure 4.16 and 4.17) are the main answer for the question 1. However, in hypothesis 1, it has been found that the decision making of the cloud users is based on security, risk and reputation which is supporting and confirming an answer to question one. However, the hypothesis 1 which derived from chapter two has been refined in other chapters (four, five, and six) to validate against other methods. To sum up, to answer the question 1, hypothesis 1 identified the criteria (security, risk, and reputation) to be measured by the result of the question 1.

Second, in the question 2, the researcher has aimed to evaluate the result of question 1. In this regard, to answer how the evaluation method is measuring, the researcher implemented the framework in chapter four in order to answer question 2. Hence, the question 1 answered by the result of chapter four, but there is a need for a formulation and integration method to evaluate the result of question 1. Therefore, this testbed (implementation) helps CIdPs and CIdUs go through a rational framework (integrated and computational) which is implemented in chapter five to measure the trust framework. Chapter five illustrated the architecture, design, and computational formulas for the proposed application (Framework). To evaluate the question 2, in chapter five, industry interviews, in the chapter six, AHP method, and professional

guidelines have been adopted to evaluate the measurable result. So, as output for these evaluation methods, verification from real cloud users (expert people), verification from most common identity standards, and element validation answered the question 2. These validation methods indicated that the proposed novel method provided the valid and reliable result, and consequently, pass the validation test as the main objective for question 2. However, the hypothesis 2 which derived from chapter four has been refined in other chapters (five and six) to validate against other methods. To sum up, measurable trust relationship (Hypothesis 2) with validation of the trust framework determined that suitable trust framework can be established in the cloud identity area.

In question 1 the relation trust framework has been answered, however, in question 2 the framework has been validated by verification from expert people, guidelines, and AHP method, therefore, the usability and feasibility of the proposed novel method still are left to be evaluated. Therefore, as a response to question 3, to check how the trust framework affect the user's decision making and help them for knowledge-based decision making, using expert interview to check the feasibility the application (framework) as well as using the threat modelling to check feasibility of the framework (application) are the main evaluation approaches. In chapter five, section 5.5 discussed the feedback from expert people to approve the usability of the framework; however, chapter six adopted the STRIDE threat modelling to challenge the feasibility of the framework. These evaluation methods indicated that the framework is beneficial for the cloud users to make a knowledge-based decision. Furthermore, they show that this framework is consistent with the user and provider expectation for selecting CIdPs. In addition, the reliability of the framework for the users also established as the expert approved it in their interview. Also, the threat mitigation for the dynamic environment (Oauth2.0) shows that this framework is reliable to use as a trust framework for both users and providers.

7.3 IMPLICATION OF THE RESULTS

The researcher in this thesis came to this point while customers as a decision maker are facing risk and security issues, trust acts as a facilitator for them to make an appropriate decision. However, trust assessment frameworks should consider security as a vital factor. Therefore, in this thesis, it has been elaborated a method to improve customer's trust in choosing a CIdPs by considering functional and non-functional trust elements.

The research has started with systematic literature to evaluate the level of trust for the main scope of this thesis (CIdP) from the perspective of the customers as well as providers. The detailed analysis in chapter two and evaluation method in chapter four helped this thesis to identify the most relevant and essential trust elements of the CIdPs. Therefore, these metrics, elements, characteristics, and attributes provide the measurable elements for the proper trust level of the CIdP.

It has been also elaborated that selecting the best provider is a complicated method and also a challenging task for the cloud users. The analysis of the current literature supports the finding, but still, there is a limitation to generalise these methods as per their weaknesses.

Moreover, in section 6.4, the main goal of the evaluation is to demonstrate the applicability and technical feasibility of the results in the domain of research. There are three methods to implicate the result: Block box, inside-out, and outside-in. In the point of block box, the trustworthiness of a proposed framework is evaluated taking into account only the observed output, however, in the perspective of inside-out approach, trustworthiness is derived based on the knowledge about the architecture of the service (cloud identity) and the trustworthiness of its components (Standard, IAM protocol, Risk assessment, Self-Assessment). Nevertheless, outside-in approach requires knowledge about the internal architecture of a service as well as its components as input and information stating the observed behaviour of the overall service (integrated method, weighting, SLA). Hence, in this thesis, it has used a combination of these approaches to have a transparent value (trust value) which means they can easily and confidently (user by using the web-based application and share their weight and feedback) make a trust-based decision. To make the trust values transparent and comprehensible, users need to be supplied with an intuitive representation of trust together with enough information regarding the relevant parameters as depicted in the figure 5.15. As this figure depicted, a cloud user would have the granular (intuitive representation) of risk, security, protocols, SLA, standard, feedback and the overall result.

7.4 CONTRIBUTION

In order to analyse the contribution of this thesis that has made to the body of the knowledge, this section will discuss the main contributions of the research based on the publishing of peer reviewed papers (see pp. vi – vii). As it has been discussed in section 3.9, in the mixed methodology, the final phase of TDSRM is known as *Communication*.

The aim is, to publicly challenge the idea, finding, and contribution. Therefore, by publishing the papers, somehow, the thesis has completed the life cycle of the contribution (brainstorm, literature, synthesis the idea, analysis, compare and comparison, evolution, evaluation) and also bring the utility and novelty for the proposed method, the rigor of its design artefact, and its effectiveness. Evaluation in this stage means that the most relevant expert people (auditor and reviewer of the journals and conferences) in the research area approved the contribution and findings of the papers, as well as, the thesis.

The thesis idea and PhD journey have been started by the continuing the previous papers (area of research) that have been published in the journals and conferences before starting this research such as:

- A trust-based model for federated identity architecture to mitigate identity theft (Ghazizadeh, Zamani, et al., 2012)
- A survey on security issues of federated identity in the cloud computing (Ghazizadeh, Manan, et al., 2012)
- Implementation and evaluation of lightweight encryption algorithms suitable for RFID (Alizadeh et al., 2013)
- Trusted computing strengthens cloud authentication (Ghazizadeh, Zamani, et al., 2014)
- Secure OpenID authentication model by using Trusted Computing (Ghazizadeh, Shams Dolatabadi, et al., 2014)
- Paint-doctored JPEG image forensics based on blocking artefacts (Ebrahimi et al., 2015)

As these papers state, the researcher area of research is cloud, cloud identity, and security. Therefore, the thesis has been started by the literature and related work to find the current literature and find the research gap. As stated in chapter two, section 2.1, the Delphi method has been adopted to find the research gap. Therefore, chapter two has sought to contribute to this literature gap in three parts. First, the purpose of this study was to identify the most important issues related to the CC, cloud identity, and trust computing adoption decisions in enterprises. Second, the relative significance of the identified issues has been determined. Third, the importance of the identified issues has been noted.

In chapter two, the researcher has come to this point that still there are various issues and threats that can compromise the cloud identity management system behaviour (*Gap*). The issues and threats are classified into the three categories (Privacy,

security, and trust). As a contribution to this part, the researcher published two papers in the 2015 and 2016 SRI Security Congress Perth (Ghazizadeh & Cusack, 2015), and (Cusack & Ghazizadeh, 2016). It has been mentioned that business use of the CC services is motivated by ease of use and potential financial cost reductions. Service failure may occur when the service provider does not protect information or when the use of the services becomes overly complex and difficult. The benefits of the CC also bring optimisation challenges for the information owners who must assess service security risks and the degree to which new human behaviours are required. In these papers, the risk of identity theft is presented when ease of service access is provided through an SSO. Moreover, the researcher was looking for the optimal behavioural expectations for a cloud service information owner. Furthermore, it has been briefly reviewed in the literature and then proposes a working solution that optimises the trade-off between disclosure risk, human user risk, and service security based on the finding in section 2.

In section 3, the researcher has come to this point that the gap is “no proper and unified cloud identity trust framework for cloud service providers, CIdPs, and CIdUs”. However, in section 3.2, it has been stated that how to establish this trust framework. Consequently, the research questions and hypotheses based on the response to gap have been discussed in section 3.3. The method how to respond to the gap is another contribution from this part. Therefore, the researcher has published *Formulating Methodology to Build a Trust Framework for Cloud Identity Management* (Ghazizadeh & Cusack, 2016c) and *Analysing Trust Issues in Cloud Identity Environments*. The core of these papers is based on the sub-section 3.4.1, figure 3.5, sub-section 3.4.2.2, and figure 3.6. In the first paper, an approach to design research in the area of information systems was presented based on the literature (Gap).

Identity and advanced cloud identity management are the ways to overcome many of the issues which cloud users are facing when attempting to use cloud services. Moreover, it addresses the problem faced by cloud users as they attempt to assess the trust that may be had in any CIdP. It has been argued that the methodology that has been developed integrated four requirements for building an improved security artefact: Trust and the capability to calculate a trust value for an entity; calculate a reputation measurement for an organisation; collect the evidence required by the second process group; and, building and evaluating a security

artefact. This has been demonstrated the DS framework (figure 3.5) which has been adopted in the thesis. It has been cited that this methodology integrated the research processes into a methodology of multiple entry points and potential quality improvement cycles. Moreover, the proposed trust framework in cloud identity (figure 3.6) to support the cloud customers in reliably identifying trustworthy cloud providers has been explained. In the second paper, it has been stated that the end user of the provider requires greater evidence. It should be based on trusting decisions regarding service supply, however, the complexity of the situation is compounded by the nature of the cloud environment that allows service providers to move between contractual arrangements and jurisdictions regardless of where the end user may be located. In chapter two and chapter four, the researcher systematically analysed numerous solutions, but, at the conclusion of the paper, it has come to the point that further research is required into optimal assessment criteria, framework architectures, and the adequacy of feedback and review loops.

In chapter four, the main contribution is utilising evaluation theory to derive the trust element for this thesis. Figure 4.1 indicated the components of evaluation theory, and figure 4.2 illustrated the visualised adopted evaluation theory for cloud identity trust evaluation framework. Finding the most common trust frameworks with their essential system attributes and finding the most relevant trust characteristics are the main objectives for the chapter four. In the subsection 4.5.2, it has come to this point that load balancing, SSO, Lifecycle, Privacy, and Risk are the main characteristics for the cloud identity environment. In section 4.7 by using IPA method (another contribution for this chapter), and comparing the ESC and ESA with trust elements, it gets approval and validation for both ESA and ESC. Therefore, the aim is to publish at least five papers based on the five characteristics. However, it has published SSO papers (Ghazizadeh & Cusack, 2015, 2016b), but also it has acceptance for the below papers:

- Satisfying Secure **Load Balancing** Expectations in the Cloud, The 24th Americas Conference on Information Systems, 2018
- Cloud Security Issues that Impact **Privacy** in Digital Identity Management, 2018 Cyber Forensics and Security International Conference
- A Synthesis Technique for Cloud **Life-Cycle** Evaluation, 2018 Cyber Forensics and Security International Conference

Moreover, to cover the risk issues, this has been published (Ghazizadeh & Cusack, 2017a). In this short paper, it has been presented that “there must be cloud identity governance in terms of who can provision identity, what data can be loaded into an environment, what security controls need to be put in place (risk assessment), and how the standardisation of security services are adopted and implemented.” A part of chapter four, table 4.9 has been published in the (Ghazizadeh & Cusack, 2016a).

In chapter five, the trust framework (artefact) has been implemented. In chapter three, it has been mentioned that usability checking is one of the evaluation methods. In chapter four, it has identified the trust framework method (Integrated and computational (ESA)) and Trust elements (ESC) to be measured to benchmark the level of trust. As a response to the chapter two and three (main contribution for this part), therefore, the artefact (framework) has been implemented in the cloud area to be evaluated by the expert people. This implantation assists the thesis to first, visualise the artefact, and second, check the usability of the artefact.

Evaluation is the crucial step for any researchers. However, most of the research papers lack proper evaluation methods. Thus, in this thesis, the proposed mix methodology utilised the Industry Interview, Professional Guidelines, Implementation, Threat Modelling, and Analytic Hierarchy Process (AHP) approaches to usability assessment, Verification of Guidelines, Verification from providers and users, Elements validation. This part aims to publish at least five papers (five approaches). Currently, the researcher has published Trust Assessment for CIdPs Using Analytical Hierarchy Process (Ghazizadeh & Cusack, 2017b) and has got acceptance for the Verification of Guidelines as below:

- Cloud Surfing: A General Comparison of Cloud Identity Standards and Guidelines, 2018 Eleventh International Conference on Mobile Computing and Ubiquitous Network (ICMU)

Therefore, the plan is to publish at least three more papers (contribution to the body of knowledge) in the unpublished area.

To sum up, this section, this thesis has a contribution in both theory and practice. As it has been stated, the objective and artefact are novel as compared with the other methods and approved by the peer review community. Besides, the research outcome has communicated with the adequate audience from both academic and industry in the same area and field and also being evaluated by going under the specific mitigation model. Based on the previous discussion, they acknowledge that the outcome of this research is new and enhances the practical mitigation of identity theft

as well as communicated through the theoretical scholarly and professional publications. The contribution has articulated to both audiences from theory and business. As it has been stated in chapter four, nowadays, a trust framework has an essential role in the service provider decision making. The proposed trust model aims to remove the end user's doubt about security, privacy, and security practices that might be encountered in the cloud identity area. On the other hand, this framework is the opportunity for the industry (identity providers) to enhance their trust factors to relieve the end user and benchmark themselves based on this framework. Last but not least, the proposed model has enhanced the business as well as end-user security, privacy, and trust objectives.

7.5 DISSEMINATION

Once trust has been calculated, it needs to be readily accessible to CIdUs and CIdPs while remaining resilient to alteration. Calculated values must be effectively disseminated to them and made available upon request. This part is publicly available, and all types of users can access the result of the information because it is the responsibility of a trust system falling within the dissemination dimension. Although, granular data is available for the cloud users which includes the result of the trust level based on the criteria (Risk, security, Protocols, Standards, feedback, and overall trust rank) as shown in the figure 5.15.

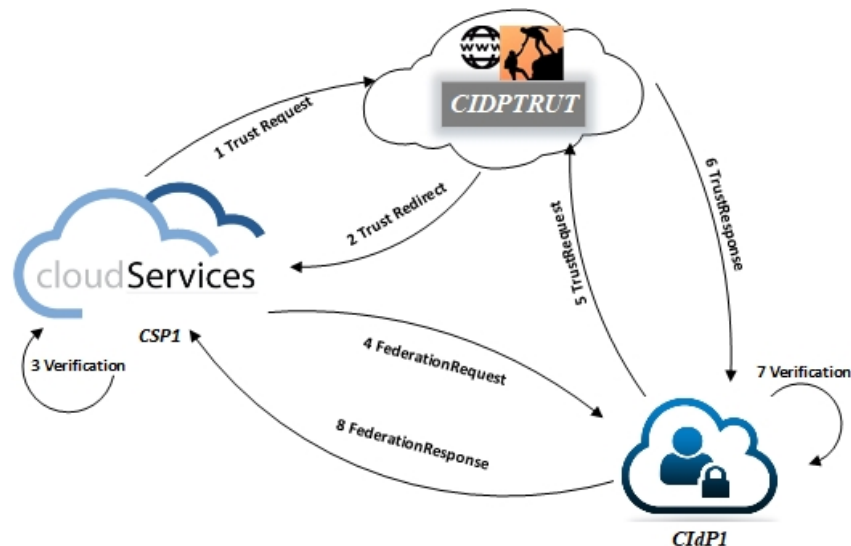


Figure 7.2: Overall workflow of proposed trust framework

Moreover, this result could help federation by using a federation standard such as but not limited to SAML. Therefore, the underlying protocol of the proposed trust evaluation model is based on the integrating SAML (Hughes & Maler, 2005)

(XML-based standard) with trust federation (Kanwal, Masood, & Shibli, 2014). CIdPs and CSP need to have a trusted relationship that leads them to participate in Cloud federation for sharing of their available resources and services. Accordingly, in this part, the proposed protocol helps to establish a bi-directional trust between service providers and identity providers that is based on the exchange of trust credentials issued by the proposed framework.

The SAML has been extended by introducing a new type of assertion that satisfies the extension mechanism described in to assure the compatibility. This new SAML assertion contains “<Trustassertion>” which has trust attributes namely Risk, security, Protocols, Standards, feedback, and overall trust rank. In the header section of Trust assertion, the <Issuer> is the CIdPTRUT whereas, the <Subject> tag either contains the CSP or CIdP for which the trust credentials have been requested. The body of this trust assertion includes different attributes namely overall trust rank which contains the aggregated trust value from Risk, security, Protocols, Standards, feedback, and overall trust rank of the requested CIdP. This < Trustassertion > is exchanged through newly defined “Trust Response” and “Request” Protocol in SAML, where the request and response formats are in line with the defined rules of SAML schema extension. The name of this adopted SAML is Cloud Identity Trust Exchange (CITE) which is including the new assertion “< Trustassertion >”, the “Trust Request/Response” protocol and “SAML SOAP” binding.

As shown in figure 7.2, the CITE use case scenario for this thesis, the CIdPTRUT acts as a trusted third party responsible for providing the requested trust assertions about registered CIdPs. CSPs and CIdPs are the subjects for which the trust assertions are requested. The CITE accepts the “<TrustRequest>” from CIdPs as well as CSPs and generates the corresponding “<TrustResponse>” that contains the asserted trust credentials (trust level) for corresponded CIdP. The overall workflow of this case scenario illustrated in figure 7.2. Following are the main steps involved in two-way trust establishment using the proposed protocol.

In first step, the CSP1 send a <TrustRequest> to the CIdPTRUT and asks for the trust credentials of CIdP1.

” <Samlp:TrustRequest>

<Saml:Issuer>CSP1

</Saml:Issuer>

```

        <Saml:Subject>
Attest the level trust of the CIdP1
        </Saml:Subject>
        <Samlp:RequestedTrustLevelandScore>
        <Saml:TrustLevelScoreClassRef>
urn: oasis:name:tc:SAML:2.0:ac:Classes: CIDPTRUT
        </Saml:TrustLevelScoreClassRef>
        </Samlp:RequestedTrustLevelandScore>
        </Samlp:TrustRequest>”

```

Next, The CIDPTRUT verifies the trust request and recheck the trust level of requested CIdP1 based on dynamic nature of trust. Consequently, CIDPTRUT generates a <TrustRedirect> containing the CIDPTRUT address. The subject of this asertion is the *Re-Attest the level trust of the CIdP1* whereas CIDPTRUT is the <Issuer> of the assertion. The CIDPTRUT acts as a trust redirector, as a TrustResponder. The SAML assertion is signed with private key of CIDPTRUT and then encrypted with the public key of CIDPTRUT.

```

“<Samlp:TrustResponse>
<Saml:TrustStatement>
<Saml:TrustContext>
<Saml: TrustContextClassRef>
The level of the trust for CIdP1
        </Saml: TrustContextClassRef>
        </Saml:TrustContext>
        <Saml:TrustScore> $T_{Feedback}, T_{Compliance}, T_{Certain}, T_{SLA}, T_{Risk}, T_{Scheck}$ 
        </Saml:TrustScore>
        <Saml:OverallTrust>  $T_{Final}$ 
        </Saml: OverallTrust >
        </Saml: TrustStatement >
        </Samlp:TrustResponse>”

```

In the third step, the CSP1 is redirected to CIDPTRUT to check the trust level and trust score. It verifies the assertion through certificate of CSP1 after decrypting the assertion with its own private key. Next, the CSP1 check the T_{Final} , if the level of trust is acceptable based on CSP1 internal policy, the federation request is sent to the CIdP1 based on the SOAP11 communication protocol.

```

“<fedp:Federationrequest>
  <fedp:issuer> CSP1
    </fedp:issuer>
  <ResourceType> “XMLFederationResource”
    </ResourceType>
  </ fedp:Federationrequest >”

```

Next the CIdP1 verifies the trust request from CIDPTRUT and sends Trust request to re-evaluate the level of trust. CIdP1 fill up the forms again and send it to the CIDPTRUT as follow:

```

“<Samlp:TrustResponse>
  <Saml:TrustStatement>
    <Saml:TrustContext>
      <Saml:TrustScore>  $T_{Feedback}, T_{Compliance}, T_{Certain}, T_{SLA}, T_{Risk}, T_{Scheck}$ 
        </Saml:TrustScore>
      <Saml:OverallTrust>  $T_{Final}$ 
        </Saml: OverallTrust>
    <Saml:Subject>
      Re-evaluate the trust
    </Saml:Subject>
  </Saml:TrustStatement>
</Samlp:TrustResponse>”

```

Finally, in the last step, the CSP1 receives this trust information from CIDPTRUT and verifies the signed assertion. After verifying the assertion and extracts the trust credentials with checking the trust score with its own pre-defined score, if the level of trust is acceptable and satisfactory, the federation is accepting.

7.6 CONCLUSION

In chapter seven, the research findings of chapter four, five, and six were tested in the ration to the research questions and hypotheses which were presented in chapter three. This chapter is the most crucial chapter for any thesis because of the finding the relation between the research questions and hypotheses. However, in the hypotheses evaluation, section 7.1, the evidence to attest the hypotheses from chapter four, five and six have been processed. Moreover, in the section 7.2, research question evaluation, the research questions have been answered. Likewise,

the results have validated the outcome of chapter two and three (Problem statement and proposed method). However, in order to get the implication of the result (section 7.3), the overall impact of the thesis has been discussed in section 7.3.

Moreover, in the section 7.4, the body of knowledge and novelty of the research has been discussed. This section has illustrated the contribution of the research by considering the research publications. However, dissemination could be a part of chapter five but based on the figure 7.1 the trust dissemination is in the last step. This section also utilised a combination of SAML method along with the trust framework.

In chapter eight, the researcher will summarise the research by identifying the key points, research challenges, limitation of the study, and areas for the further research. Therefore, in the research summary based on the figure 7.1, all steps with their contribution will be reviewed by considering the research questions and sub questions. In section 8.2, the research challenges due to the subjective and context-sensitive nature of trust, and the selection of providers by trust level is evaluated. Furthermore, in the section 8.3, the crucial limitation for the research with considering the figure 7.1 will be analysed. Finally, in the section 8.4, based on the rapid growth in the cloud and cloud identity areas and their significant impact on the both industry and users, the future work and study based on the current thesis are outlined.

Chapter Eight

Conclusion

8.0 INTRODUCTION

In Chapter seven, the contribution of the research is identified by analysing the evidence to answer the research questions, test hypothesis and establish justification for the outcomes. The hypotheses and research questions are evaluated using a Quasi-Judicial method. Furthermore, the overall deliverable of the thesis is explained in the implication of the result. Also, by discussing the published paper contribution to the thesis the contribution to the body of knowledge and communication is made. Chapter seven concluded by the dissemination of the trust which demonstrated the integration of the trust framework with the SAML exchange method.

However, to conclude the thesis, in this chapter, the researcher is summarising the research by identifying the key points, research challenges, limitation of the study, and areas for the further research. Therefore, the chapter eight is structured as follows: section 8.1 summarises all the key points of the thesis from chapter two to chapter seven. Section 8.2 is discussing the challenges of the research in both theory and practical perspectives. The limitation of study from chapter one to chapter six are explained. The thesis, as well as this chapter, is concluded by the future work for ongoing study.

8.1 RESEARCH SUMMARY

In this section the summary of the literature, problem identification, and the proposed trust framework is discussed. Moreover, the research methodology with the evaluation method is evaluated in this section accordingly. The main objective for the chapter two is to identify the gaps and problems in the cloud, cloud identity, and trust computing. As the title of the research cited the main goal is mitigation of identity theft by using a trust framework in the cloud. Therefore, to “Control” the cloud identity and identity theft, this research is trying to find the most relevant trust elements to be “measured” and suggests the adoption of the integrated trust framework to help the cloud user to make the best decision. However, in chapter two, it has been found that the Control and visibility are two initial parts of the trust in the cloud. So,

establishing trust first requires control integrated with the level of visibility (level of trust) that can be expanded for service providers.

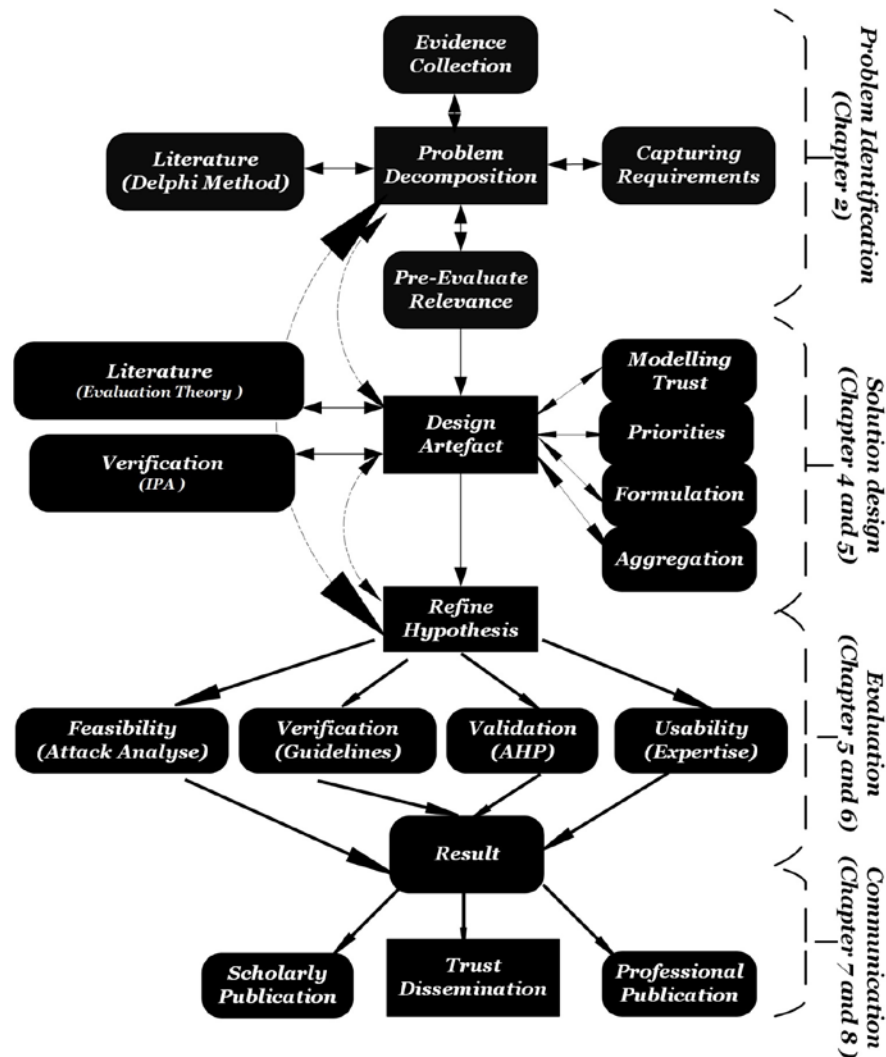


Figure 8.1: Thesis methodology

To aid this part with professional explanation, same as previous chapter the figure 8.1 is assisting to summarise the pathway of the research. This figure is based on the proposed methodology. Likewise, the figure shows that the chapter eight covers and analyses all steps of the methodology which all steps are black (compare with the figures 2.1, 4.1, 5.1, 6.1, and 7.1).

In chapter two, by adopting the Delphi method, it has been found that IAM systems are exposed to several issues and threats that can compromise their behaviour, and accordingly privacy, security, and trust issues are classified. Also, chapter two has been concluded by the comparison of the current IAM solution and prioritising them based on the figure 2.24.

The current questions regarding the monitoring, trust, CC, and cloud identity have been evaluated. Based on the analysing of the current IAM, proposed the trust framework to overcome the security, trust, monitoring, and privacy issued of the cloud identity management system as depicted in figure 3.3. Research questions and hypotheses have been elaborated and explained in the section 3.3. Following the gap finding, response to the gap is another finding and contribution for this thesis which has been explained in section 3.4. Figure 3.5 shows the summarised *Cloud Trust Design Science Method* which is the plan and pathway for the thesis. Nevertheless, figure 8.1 highlighted the cloud trust framework and its elements. Based on figure 3.7, *Systematic literature, professional guidelines, implementation, industry interview, and threat modelling* have been chosen to evaluate the *assumption from the literature, verification from the guidelines, usability assessment, and feasibility checking*. However, table 3.1 is showing the relation between these assumptions and methods. The chapter three is ending with an explanation of each method; also, how these methods are assisting the thesis to answer the research questions and test the hypotheses.

In the following chapter, there are two main question to be answered. The researcher adopted the evaluation theory to answer these two questions:

- Between cloud provider and cloud consumer, what are the ESA of trust establishment?
- Between CIdPs and CIdUs, what are the ESC of published trust establishment method?

To answer these two questions, first trust management elements have been identified and explained based on the systematic literature. These elements are the main elements for any trust framework; also, the evaluation system architecture (section 4.2) is used to make sure that the evaluation trust level in the identity environment is comprehensive and reliable. Figure 4.2 depicted the adopted evaluation theory for the cloud identity trust framework. Target, criteria, yardstick, data gathering, synthesis techniques, and the evaluation process are the main steps for the implemented evaluation theory in chapter four. As a finding for this research and summary for the chapter four, table 4.20 shows the weight and connectivity rate for the ESA and ESC elements. Furthermore, figures 4.16 and 4.17 depicted the modified IPA map for the ESC and ESA.

In the chapter five, the artefact based on the findings in chapter two, three, and four has been implemented. This application with novel method to evaluate the level of trust is the novelty for this chapter as well as for the thesis. Therefore, chapter five

is dedicated to the implementation and usability study of the proposed artefact trust management system in the cloud identity environment. Moreover, the objective of the chapter five is to ensure applicability in practice as well as to improve the method's quality by including solutions to problems encountered based on the trust and reputation definition. Figure 5.1 shows the application architecture and also figure 5.2 depicts the application workflow along with the main interface of the application (figure 5.3). Formulation and dissemination of the application explained and elaborated in the sections 5.4 and 5.5. Figure 4.16 shows the overall workflow of the proposed trust framework. Moreover, in chapter five, in section 5.5, the expert usability evaluation has been analysed. Based on the mixed method methodology in section 5.5.1, the usability testing that brought validity to the application with an extensive range of questions has been reported. The main aim for this method is to gain compelling insights and genuine evidence of the real users (expert people) to test the hypothesis (trust framework). Critical reflection on experts' evaluation results shows that overall interviewees were satisfied with the application after changing the criteria and their comment in the sub-section 5.5.2 and they have a positive attitude about the artefact. Moreover, expert people have mentioned that the application (which is based on the artefact) is very effective, thoughtful, and has the real-world trust perspective.

In chapter six, in section 6.1, AHP method has been adopted to evaluate the artefact elements. Applying the AHP procedure includes three basic steps:

- Decomposition, or the hierarchy construction.
- Comparative judgments or defining and executing data collection to obtain pairwise comparison data on elements of the hierarchical structure.
- Synthesis of priorities or constructing an overall priority rating.

The Satty method has been utilised in the research to identify the most relevant trust element based on the expert people. In the sub-section 6.1.1, the trust evaluation hierarchy has been developed. Tables 6.5 and 6.6 summarised the consistency test, and both ESC and ESA global weights. As a finding for this part, all CR values in table 6.5 and 6.6 are lower than 0.1; therefore, gives validity for this research based on the Satty method. Also, it shows the consistency between the judgments (interviewees) and accuracy of the trust elements. Finally, tables 6.7 and 6.8 indicated the local and global weight for both ESA and ESC. Moreover, to check the validity of the result, other AHP scale methods similarly has been utilised as depicted in figures 6.9 and 6.10.

In section 6.2, cloud identity standards and guidelines, three main standards have been utilised to get verification from the standards. NIST 7874, ENISA-

Standardization in the field of Electronic Identities and TSPs, and CSA- IAM are the three guidelines for the cloud identity environment. The granulated analysis and qualitative analysis of this part revealed that the artefact elements are aligned with the industry standards which bring the verification for this research. Figure 6.9 is a methodology for this section to analyse the guidelines. Table 6.11 and 6.12 are the results that show the identity standards overlaps and differences.

Section 6.3, to attest to the artefact, it has been challenging the feasibility of the artefact by applying STRIDE threat modelling. Therefore, to measure the result of the feasibility checking in this thesis assists to use the qualitative data obtained from threat modelling method which align with the Security Development Lifecycle (SDL). Consequently, developing abuse case (first assumption for the artefact) helps this thesis to identify the artefact issues from the perspective of the attackers, and accordingly allows the researcher to decide and document how the artefact should react to mitigate the threats and therefore validate the feasibility of the proposed method. Figure 6.11 shows the Ouath2.0 data flow diagram which has implemented in the STRIDE threat modelling. To validate the feasibility of the artefact, the trust framework concept is applied to analyse whether this proposed model could mitigate identity theft in the artefact for all mentioned threats, and consequently, get approval by the threat report reviewer. Tables 6.13 to 6.22 indicated the justification, possible mitigation, and relevant trust framework elements.

In chapter seven, the findings of the research, research questions and hypothesis, and the contribution of the research to the knowledge have been discussed. Finally, the research has been concluded by the chapter eight, conclusion, which the summary of the research, challenges, limitation of the study, and future work have been discussed.

Likewise, one of the innovative phenomena is federation; but, the thesis question is how the public and private sectors increase economic growth by enabling the federation. Cloud federation as analysed in chapter two, and nowadays, is not innovation but it is the reality of the cloud. This thesis found that the trust framework is the answer for users and providers and can bring the CIdUs up to speed on the state of identity systems.

After the critical analysing, the thesis found trust frameworks are critical to the industry not only in the contemporary technology but also in the anticipation of the cloud requirements in the future. This has given a notion of hard work to make something simple and the simple thing trying to do is the solid operational definition

of the trust framework. The best example for the trust framework is the credit card which is used by most people. The card allows the merchants and financial institutions, service providers, and stockholders an opportunity to participate in the worthy business legal and technical requirements. It is the great beauty of the trust framework which is represented by credit cards.

Moreover, the trust framework is importantly integrating government (standard and legislation) and private agencies (providers and customers) as part of the work. However, the framework shows the state of the identity system in different perspectives and different ecosystems. The benefit of the trust frameworks is that by nature they are interoperable; so, in the global identity ecosystem or an ecosystem that involves federated and local identity systems, interoperability is the essential key. Moreover, it is not just guidance for the trust identity framework but also structure for the other cloud service frameworks. Besides, each of the participants in the trust framework should have a very clear understanding of their duties and the responsibilities. Also, the trust framework can be trusted by all the stakeholders in system. Also, it allows for better trust on the rescannable and technical scale. The equation 8.1 is summarises these concerns for the trust framework.

$$\text{User's Feedback} + \text{Technology Tools} + \text{Governing Roles} = \text{Trust} \quad (8.1)$$

This formula clearly indicates that three stets of the codes bases, based on the user's perspective, technologies' perspective and governance's perspective lead the trust framework. It shows that this system is the same as any other systems requires rules for the variety of reasons. On the other hand, the strong part of the thesis is that the trust framework also governs the whole identity system as equation 8.2 shows.

$$\text{Tools} + \text{Trust framework} = \text{Govern Trust Framework} \quad (8.2)$$

Therefore, the details of any identity system are going to be governed comprehensively by the proposed trust framework. However, the researcher came to this point that the trust framework is a legally enforceable, set of specifications, set of rules, and set of agreements that govern identity systems. Moreover, the main characteristics of the proposed trust framework are scope (particular trust framework for particular identity system as per their rights, responsibilities, and obligation to the principles), operational (functional property), address the legal issue, trustworthy (trust the rules and act in the reliance on them), purpose (define the governs the operation of a specific identity system), form (self-contained or incorporate pre-existing standards or requirements), enforceable, and generalised (generalised the identity system).

8.2 RESEARCH CHALLENGES

The main challenge for the novel research is the lack of the relevant research and works in the E-library as most of the research has focused on the provider perspective and very little on the user perspective. Therefore, based on the traditional trust solutions from the literature, it has been found some difficulties and issues when adopting in the cloud environment. These points are rarely discussed in the trust context from both perspectives which is one of the main features of trust. However, due to the subjective and context-sensitive nature of trust, the selection of providers with the proper level of trust and appropriate services is one of the most challenging issues in the multi-tenant cloud environment.

Likewise, after establishing the artefact, the researcher faced the implementation challenges for the research artefact. Desktop and cloud solutions were the solution for this research which is based on the cloud nature of the research and the Amazon platform (AWS) was used. Getting feedback from the experts and asking them how to improve the artefact raised other problems. Therefore, by having advice from the research supervisor and international network (LinkedIn) the researcher found the five most useful experts in the research area of the cloud to get the feedback. Moreover, based on the research PGR9 report, AUT supported with sufficient financial support for the research infrastructure.

8.3 LIMITATIONS OF THIS STUDY

The processes of the artefact were tested and evaluated using expert people, guidelines and threat modelling. These methods helped to illustrate the artefact's capabilities to preserve a structured and logical flow. This provides the feasibility, reliability, the usability of the proposed model. The tests ensure that the principles of validity and acceptability are satisfied. However, despite the framework being theoretically evaluated and tested in the virtual environment, it has yet to be applied to a real commercial cloud environment (cloud users, customers, and providers).

Moreover, the crucial limitation for the research is the methodology which has been adopted. Validity and reliability which has been discussed in chapter three are the main issues and a limitation for this initial phase of the research. However, as the research method is design science the main concern was the iteration and absence of the differences in the result if the research was to be further iterated. In chapter four, the evaluation theory helped the researcher to elaborate each step of

the theory and made the content elements which contributes to the building the artefact. However, with respect to the evaluation theory, the validation of the chapter four result was another limitation of this research. Despite any errors incurred, the researcher has taken these and limitations as an opportunity for improving the result of the study as well as future quality improvement of the study. Implementation of the artefact was another challenge for this study because the researcher wanted to implement the artefact in a cloud-based context while considering the confidentiality of the research contribution.

Furthermore, it was difficult to find expert people in the research area (chapter five) to contribute to the research. The researcher sent more than 30 invitation letters, and finally, five interviewees replied with the positive attitude as per their time limitation and area of expertise. The variation in their ideas and opinion was helpful to validate and improve the artefact (chapter six). Checking the validity of the proposed model by guidelines was a new method, which it was difficult to find a related method to assist this research, but, finally the researcher by using the NVIVO software and three main guidelines overcame the problem. Furthermore, validation by threat modelling was a novel method for this research as per the novelty of both threat modelling methods (STRIDE threat modelling) and cloud identity management system (Oauth2.0). This limitation has been commented in section 6.3 to validate the feasibility of the proposed framework. Based on the comments and idea from the chapter six the artefact has gone through the iteration to produce a prototype, which would deliver the result according to the user's perspective.

Finally, yet importantly, as per the high level of subjectively in the data, which is used in this research, there is always a limitation in all steps and stages. Therefore, the artefact continuously needs to improve usability and feasibility based on the stakeholders' feedback. On the other hand, based on the research theory and idea, it is possible to adopt the artefact in the cloud identity environment and it can be generalised into a multiplicity of contexts. The novel methodology of the research assists the research to meet the objectives as well as mitigate the cloud user's identity theft despite all the mentioned limitations. Therefore, at this point, the research can go in a multiplicity of the directions. Therefore, the following section will discuss the future work of this research.

8.4 AREAS FOR FUTURE RESEARCH

The rapid growth in the cloud and cloud identity area has posted the significant concerns for the cloud trust and cloud user's decision making. The evaluation methodology for this research which was used to test the hypothesis confirmed the usability and feasibility of the artefact. Besides, The SLA which has been evaluated manually in this research is automatically evaluated by using semantic web technologies. It means that the semantic web mechanisms represent SLA graph structures. Therefore, the SLA is added into the RDF graph using graph homeomorphisms and then are annotated with ESA and ESC or the new version of constraints in a single structure.

Furthermore, one of the main issues that have not been addressed is the updating the cloud and cloud identity policies, particularly the General Data Protection Regulatory (GDPR). It provides for the standard's adequacy and how the GDPR is combined in the user's identity processing practices, since with new technologies and use cases are private and public.

The future development of this research can focus on working on mechanisms to derive opinions from other available sources such as TPM-based attestation to validate the artefact assessment. Additionally, performing experiments in the context of the artefact considering consumers' preferences in selecting reliable sources of opinions. Cloud identity's behaviour in selecting trustworthy CIdPs independent of the rating is considered as an ESC to calculate trustworthiness. Thus, the integration of such parameters in the artefact as future work will improve the artefact. Moreover, it will be also focus on designing threat models, and their mitigation approaches as a part of the future work. Nevertheless, practical encouragement mechanisms need to be integrated into the proposed artefact to encourage a bigger portion of CIdPs as well as users to use the artefact. Hence, use of the existing encouragement mechanisms can be enhanced in the area of trust management in order to develop a suitable one for the future work.

Currently, Cloud Access Security Brokers (CASB) have become the main attribute of any strategy for the cloud area to help both providers and users make a decision about cloud service providers and also help them to protect sensitive data. However, CASB should align with vendors to address specific use-case requirements. As the main target for this research (find the role as a CASB in the

cloud identity area) in the future is improving cloud identity service discovery databases, to help CIdU to perform better decision making between the CIdPs. Therefore, the artefact is expanded further into identity security and privacy with the addition of Federated Identity Management and SSO method for popular CIdPs. Improving the application dashboard to display important indicators of trust posture along with recommended remediation of limitations.

It is obvious that the new technology such as cloud and cloud identity is dynamic and assists the enabling of the use of advanced protocols, hardware, security features and most update policies; therefore, the cloud has this potential to expand to areas such as IoT and Smart city. The IoT (section 4.6.2.2) also expands to the healthcare systems and includes healthcare applications. Along with IoT, there is another technology, called Mobile Cloud Computing (MCC), a new generation of cloud services which aims to provide access to the information and the data from anywhere at any time by restricting or eliminating the need for hardware equipment. Likewise, the proposed method alongside with IoT, smart city, and MCC technologies such as this thesis will utilise the numerous attributes and characteristics (most related) of them and update the customise trust model to be used in this area. It could be used as useful bases for both IoT and cloud identity to provide improvements on their functions.

Last but not least, there needs to be other methods to identify and prioritise the trust elements in order to address the issues that mentioned for the artefact. However, this research made a strong contribution in the area of cloud identity not only for the users but also to identify the essential trust attributes and characteristics of the CIdPs.

References

- Aceto, G., Botta, A., De Donato, W., & Pescapè, A. (2013). Cloud monitoring: A survey. *Computer Networks*, 57(9), 2093-2115.
- Aguirre, E., Mahr, D., Grewal, D., de Ruyter, K., & Wetzels, M. (2015). Unraveling the personalization paradox: the effect of information collection and trust-building strategies on online advertisement effectiveness. *Journal of Retailing*, 91(1), 34-49.
- Ahmad, Z., Ab Manan, J.-L., & Sulaiman, S. (2010). User requirement model for federated identities threats, *Symposium conducted at the meeting of the 2010 Advanced Computer Theory and Engineering (ICACTE)*, Chengdu, China. IEEE
- Al-Sharawneh, J., & Williams, M. (2010). Credibility-based social network recommendation: Follow the leader. *The 21st Australasian Conference on Information Systems (ACIS 2010)*, Brisbane, Australia: AIS.
- Alabool, H. M., & Mahmood, A. K. B. (2015). A novel evaluation framework for improving trust level of Infrastructure as a Service. *Cluster Computing*(19(1)), 389-410.
- Alaqla, A., Fischer-Hübner, S., Groß, T., Lorünser, T., & Slamanig, D. (2016). Signatures for Privacy, Trust and Accountability in the Cloud: Applications and Requirements. *IFIP International Summer School on Privacy and Identity Management*, 79-96.
- Albakri, S. H., Shanmugam, B., Samy, G. N., Idris, N. B., & Ahmed, A. (2014). Security risk assessment framework for cloud computing environments. *Security and Communication Networks*, 7(11), 2114-2124.
- Aldaya, A. C., Sarmiento, A. J. C., & Sánchez-Solano, S. (2016). AES T-Box tampering attack. *Journal of Cryptographic Engineering*, 6(1), 31-48.
- Alhamad, M., Dillon, T., & Chang, E. (2010). Sla-based trust model for cloud computing. *13th International Conference on Network-Based Information Systems*, Takayama, Japan: IEEE.
- Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information sciences*, 305, 357-383.
- Alizadeh, M., Hassan, W. H., Zamani, M., Karamizadeh, S., & Ghazizadeh, E. (2013). Implementation and evaluation of lightweight encryption algorithms suitable for RFID. *Journal of Next Generation Information Technology*, 4(1), 65.
- Alliance, C. (2011). Security guidance for critical areas of focus in cloud computing v3. 0. *Cloud Security Alliance*.
- Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: user strategies for combating phishing attacks. *International Journal of Human-Computer Studies*, 82, 69-82.
- Alshehri, M. D., & Hussain, F. K. (2015). A Comparative Analysis of Scalable and Context-Aware Trust Management Approaches for Internet of Things. *Symposium conducted at the meeting of the International Conference on Neural Information Processing*, Cham, Switzerland: Springer.
- Alturki, A., Gable, G. G., & Bandara, W. (2013). *The design science research roadmap: in progress evaluation*. presented at the meeting of the PACIS 2013 proceedings, Jeju Island, Korea.

- Alzaid, H., Alfaraj, M., Ries, S., Jøsang, A., Albabtain, M., & Abuhaimed, A. (2013). Reputation-based trust systems for wireless sensor networks: A comprehensive review. *Symposium conducted at the meeting of the IFIP International Conference on Trust Management*, Berlin, Heidelberg: Springer
- Amini, A., Jamil, N., Ahmad, A., & Zaba, M. (2015). Threat modeling approaches for securing cloud computing. *Journal of Applied Science*, 15(7), 953-967.
- Anbarasu, A. K. (2012). *Cloud Reference Architecture*. Retrieved from <http://www.oracle.com/technetwork/topics/entarch/oracle-wp-cloud-ref-arch-1883533.pdf>
- Arias-Cabarcos, P., Almenárez-Mendoza, F., Marín-López, A., Díaz-Sánchez, D., & Sánchez-Guerrero, R. (2012). A metric-based approach to assess risk for “on cloud” federated identity management. *Journal of Network and Systems Management*, 20(4), 513-533.
- Avatier. (2016). *Identity Management Architecture*. Retrieved from <http://www.avatier.com/products/identity-management/architecture/>
- AWS. (2016). *AWS Cloud Compliance, Assurance programs for finance, healthcare, government and more*. Retrieved from <https://aws.amazon.com/compliance/>
- Azzopardi, E., & Nash, R. (2013). A critical evaluation of importance–performance analysis. *Tourism Management*, 35, 222-233.
- Badger, L., Grance, T., Patt-Corner, R., & Voas, J. (2011). Draft cloud computing synopsis and recommendations. *NIST special publication*, 800, 146.
- Balamurugan, B., & Krishna, P. V. (2015). Enhanced Role-Based Access Control for Cloud Security. In *Artificial Intelligence and Evolutionary Algorithms in Engineering Systems* (pp. 837-852): Springer.
- Barnett-Page, E., & Thomas, J. (2009). Methods for the synthesis of qualitative research: a critical review. *BMC medical research methodology*, 9(1), 1.
- Barry, D. K. (2014). *Categories of Cloud Providers*. Retrieved from http://www.service-architecture.com/articles/cloud-computing/cloud_computing_categories.html
- Bashir, G. M. M., Hoque, A. S. M. L., & Nath, B. C. D. (2016). E-learning of PHP based on the solutions of real-life problems. *Journal of Computers in Education*, 3(1), 105-129.
- Basney, J., & Gaynor, J. (2011). An OAuth service for issuing certificates to science gateways for TeraGrid users. *Symposium conducted at the meeting of the Proceedings of the 2011 TeraGrid Conference: Extreme Digital Discovery*, Salt Lake City, Utah, USA: ACM.
- Bazeley, P., & Jackson, K. (2013). *Qualitative data analysis with NVivo*. London, UK: Sage Publications Limited.
- Berndtsson, H., & Olsson, J. B., Lundell, B. (2008). *Thesis Projects A Guide tfor Students in Computer Science and Information Systems*. 2nd Edition. London: Springer-Verlag.
- Berndtsson, M., Hansson, J., Olsson, B., & Lundell, B. (2008). Developing your Objectives and Choosing Methods. *Thesis Projects: A Guide for Students in Computer Science and Information Systems*, 54-70.
- Bertino, E., & Takahashi, K. (2011). *Identity Management: Concepts, Technologies, and Systems*. Norwood, USA: Artech House.

- Bertocci, V., Serack, G., & Baker, C. (2007). *Understanding windows cardspace: an introduction to the concepts and challenges of digital identities*. CA, USA: Pearson Education.
- Bezzi, M., Kaluvuri, S. P., & Sabetta, A. (2011). Ensuring trust in service consumption through security certification. *Symposium conducted at the meeting of the Proceedings of the International Workshop on Quality Assurance for Service-Based Applications*, Lugano, Switzerland:ACM.
- Blaze, M., Feigenbaum, J., & Lacy, J. (1996). Decentralized trust management. *Proceedings 1996 IEEE Symposium on Security and Privacy*, Oakland, CA, USA, USA :IEEE
- Bray, T. (2017). The javascript object notation (json) data interchange format. *RFC 8259(IETF)*, 16. <https://doi.org/10.17487/RFC8259>
- Breiter, G., & Behrendt, M. (2009). Life cycle and characteristics of services in the world of cloud computing. *IBM Journal of Research and Development*, 53(4), 3: 1-3: 8.
- Calheiros, R. N., Ranjan, R., Beloglazov, A., De Rose, C. A., & Buyya, R. (2011). CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms. *Software: Practice and Experience*, 41(1), 23-50.
- Campbell, B., Jones, M., & Mortimore, C. (2015). Security Assertion Markup Language (SAML) 2.0 Profile for OAuth 2.0 Client Authentication and Authorization Grants.
- Cardozo, B. N. (2010). *The nature of the judicial process*: Quid Pro Books.
- Chakraborty, S., & Roy, K. (2012). An SLA-based framework for estimating trustworthiness of a cloud. *11th International Conference of the Trust, Security and Privacy in Computing and Communications (TrustCom)*, Liverpool, UK: IEEE.
- Chan, H., & Chieu, T. (2010). Ranking and mapping of applications to cloud computing services by SVD, *Symposium conducted at the meeting of the Network Operations and Management Symposium Workshops (NOMS Wksp)*, Osaka, Japan:IEEE/IFIP.
- Chard, K., Lidman, M., Bryan, J., Howe, T., McCollam, B., Ananthakrishnan, R., . . . Foster, I. (2014). Globus Nexus: Research Identity, Profile, and Group Management as a Service, *10th International Conference on Symposium conducted at the meeting of the e-Science (e-Science)*, Sao Paulo, Brazil:IEEE.
- Chauhan, T., Chaudhary, S., Kumar, V., & Bhise, M. (2011). Service level agreement parameter matching in cloud computing, *Symposium conducted at the meeting of the Information and Communication Technologies (WICT)*, Mumbai, India: IEEE.
- Chen, C.-F. (2006). Applying the analytical hierarchy process (AHP) approach to convention site selection. *Journal of Travel Research*, 45(2), 167-174.
- Chew, E., Swanson, M., Stine, K. M., Bartol, N., Brown, A., & Robinson, W. (2008). SP 800-55 Rev. 1. *Performance Measurement Guide for Information Security*, National Institute of Standards & Technology, Gaithersburg, MD.
- Chhabra, S., & Dixit, V. S. (2015). Cloud computing: State of the art and security issues. *ACM SIGSOFT Software Engineering Notes*, 40(2), 1-11.
- Chou, D. C., & Chou, A. Y. (2009). Information systems outsourcing life cycle and risks analysis. *Computer Standards & Interfaces*, 31(5), 1036-1043.

- Choudhury, P., Sharma, M., Vikas, K., Pranshu, T., & Satyanarayana, V. (2012). Service ranking systems for cloud vendors. *Symposium conducted at the meeting of the Advanced Materials Research*: Trans Tech Publ.
- Churchman, C. W., & Ackoff, R. L. (1954). An approximate measure of value. *Journal of the Operations Research Society of America*, 2(2), 172-187.
- Commission, E. (2016). *Cloud computing service level agreements*. Retrieved from <http://ec.europa.eu>
- Cooper, B. F., Ramakrishnan, R., Srivastava, U., Silberstein, A., Bohannon, P., Jacobsen, H.-A., Yerneni, R. (2008). PNUTS: Yahoo!'s hosted data serving platform. *Proceedings of the VLDB Endowment*, 1(2), 1277-1288.
- Council, C. S. C. (2016). *Practical Guide to Cloud Service Agreements, Version 2.0*. Retrieved from <http://www.cloud-council.org>
- Coveillo, A., Elias, H., Gelsinger, P., & Mcaniff, R. (2011). Proof, not promises: creating the trusted cloud. RSA White paper.
- Cusack, B., & Ghazizadeh, E. (2016). Evaluating single sign-on security failure in cloud services. *Business Horizons*, 59(6), 605-614.
- Cusack, B., & Zadeh, E. (2015). Evaluating single sign on security failure in cloud services.
- da Costa Cordeiro, W. L., Santos, F. R., Mauch, G. H., Barcelos, M. P., & Gaspary, L. P. (2012). Identity management based on adaptive puzzles to protect P2P systems from Sybil attacks. *Computer Networks*, 56(11), 2569-2589.
- Dane, E., Rockmann, K. W., & Pratt, M. G. (2012). When should I trust my gut? Linking domain expertise to intuitive decision-making effectiveness. *Organizational Behavior and Human Decision Processes*, 119(2), 187-194.
- Dhillon, D. (2011). Developer-driven threat modeling: Lessons learned in the trenches. *IEEE Security & Privacy*, 9(4), 41-47.
- Di Vimercati, S. D. C., Foresti, S., & Samarati, P. (2012). Managing and accessing data in the cloud: Privacy risks and approaches, *7th International Conference of the Risk and Security of Internet and Systems (CRiSIS)*, 2012, Cork, Ireland: IEEE.
- DiMaria, J. (2016). *CloudTrust Protocol Working Group* Retrieved from <https://cloudsecurityalliance.org/group/cloudtrust-protocol/>
- Disterer, G. (2013). Iso/iec 27000, 27001 and 27002 for information security management.
- Dixon-Woods, M. (2011). Using framework-based synthesis for conducting reviews of qualitative studies. *BMC medicine*, 9(1), 1.
- Dixon-Woods, M., Cavers, D., Agarwal, S., Annandale, E., Arthur, A., Harvey, J., Smith, L. (2006). Conducting a critical interpretive synthesis of the literature on access to healthcare by vulnerable groups. *BMC medical research methodology*, 6(1), 1.
- Djemame, K., Armstrong, D., Guitart, J., & Macias, M. (2014). A Risk Assessment Framework for Cloud Computing, *IEEE Transactions on Cloud Computing*, (1), 1-1.
- Dólera Tormo, G., Gómez Mármol, F., & Martínez Pérez, G. (2012). On the application of trust and reputation management and user-centric techniques for identity management systems, *Symposium conducted at the meeting of the XII Spanish meeting on cryptology and information security (RECSI 2012)*, San Sebastián, Spain

- Dondio, P., & Longo, L. (2011). Trust-based techniques for collective intelligence in social search systems. In *Next Generation Data Technologies for Collective Computational Intelligence* (pp. 113-135): Springer.
- Donepudi, H., Bhavineni, B., & Galloway, M. (2016). Designing a Web-Based Graphical Interface for Virtual Machine Management. In *Information Technology: New Generations* (pp. 401-411): Springer.
- Dong, X., Yu, J., Luo, Y., Chen, Y., Xue, G., & Li, M. (2014). Achieving an effective, scalable and privacy-preserving data sharing service in cloud computing. *computers & security*, 42, 151-164.
- Duncan, A., Creese, S., & Goldsmith, M. (2015). An overview of insider attacks in cloud computing. *Concurrency and Computation: Practice and Experience*, 27(12), 2964-2981.
- Dynatrace. (2016). *CloudSleuth*. Retrieved from <http://www.dynatrace.com/en/index.html>
- Ebrahimi, A., Ibrahim, S., Ghazizadeh, E., & Alizadeh, M. (2015). Paint-doctored JPEG image forensics based on blocking artifacts. *International Conference and Workshop of the Computing and Communication (IEMCON)*, 2015, Vancouver, BC, Canada: IEEE.
- Edwards-Jones, A. (2014). Qualitative data analysis with NVIVO: Taylor & Francis.
- El-Gazzar, R., Hustad, E., & Olsen, D. H. (2016). Understanding cloud computing adoption issues: A Delphi study approach. *Journal of Systems and Software*, 118, 64-84.
- El-Najdawi, M., & Stylianou, A. C. (1993). Expert support systems: integrating AI technologies. *Communications of the ACM*, 36(12), 55-ff.
- El Maliki, T., & Seigneur, J.-M. (2007). A survey of user-centric identity management technologies, *Symposium conducted at the meeting of the The International Conference on Emerging Security Information, Systems, and Technologies (SECUREWARE 2007)*, Valencia, Spain: IEEE.
- Fang, H., Zhang, J., Şensoy, M., & Thalmann, N. M. (2012). SARC: subjectivity alignment for reputation computation, *Proceedings of the 11th International Conference on Autonomous Agents and Multiagent Systems*, Valencia, Spain: ACM.
- Faraji, M., Kang, J.-M., Bannazadeh, H., & Leon-Garcia, A. (2014). Identity access management for Multi-tier cloud infrastructures, *2014 IEEE Network Operations and Management Symposium (NOMS)*, Krakow, Poland: IEEE.
- Felderer, M., & Katt, B. (2015). A process for mastering security evolution in the development lifecycle: Springer.
- Fera, M. A., Natarajan, I., Brinda, K., & Darathiprincy, R. (2015). Enhancing Security in Cloud Using Trusted Monitoring Framework. *Procedia Computer Science*, 48, 198-203.
- Fernandez, A., Insfran, E., & Abrahão, S. (2011). Usability evaluation methods for the web: A systematic mapping study. *Information and Software Technology*, 53(8), 789-817.
- Ferraiolo, D., Chandramouli, R., Kuhn, R., & Hu, V. (2016). Extensible Access Control Markup Language (XACML) and Next Generation Access Control (NGAC), *the Proceedings of the 2016 ACM International Workshop on Attribute Based Access Control*, New Orleans, Louisiana, USA: ACM.
- Fett, D., Küsters, R., & Schmitz, G. (2016). A comprehensive formal security analysis of oauth 2.0. *Symposium conducted at the meeting of the*

Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria: ACM.

- Fitó, J. O., & Guitart, J. (2014). Business-driven management of infrastructure-level risks in Cloud providers. *Future Generation Computer Systems*, 32, 41-53. <https://doi.org/http://dx.doi.org/10.1016/j.future.2012.05.008>
- Forum, T. (2016). *Cloud computing reference architecture*. Retrieved from <https://www.tmforum.org>
- Fournaris, A. P., & Keramidas, G. (2014). From Hardware Security Tokens to Trusted Computing and Trusted Systems. In *System-Level Design Methodologies for Telecommunication* (pp. 99-117): Springer.
- Fragoso-Rodriguez, U., Laurent-Maknavicius, M., & Incera-Dieguez, J. (2006). Federated identity architectures, *1st Mexican Conference on Informatics Security 2006 (MCIS'2006)*
- Gantner, J., Demetz, L., & Maier, R. (2015). All You Need is Trust—An Analysis of Trust Measures Communicated by Cloud Providers, *Symposium conducted at the meeting of the On the Move to Meaningful Internet Systems*, Cham: Springer
- Garg, S. K., Versteeg, S., & Buyya, R. (2013). A framework for ranking of cloud computing services. *Future Generation Computer Systems*, 29(4), 1012-1023.
- Ghazizadeh, E., & Cusack, B. (2015). Evaluating single sign-on security failure in cloud services. *13th Australian Information Security Management Conference*, Perth, WA: AIS.
- Ghazizadeh, E., & Cusack, B. (2016a). Analysing Trust Issues in Cloud Identity Environments, *The 27th Australasian Conference on Information Systems*, Wollongong: AIS.
- Ghazizadeh, E., & Cusack, B. (2016b). Evaluating single sign-on security failure in cloud services. *Business Horizons*, 8(2), 10. <https://doi.org/http://dx.doi.org/10.1016/j.bushor.2016.08.002>
- Ghazizadeh, E., & Cusack, B. (2016c). Formulating Methodology to Build a Trust Framework for Cloud Identity Management, *presented at the meeting of the 22nd Americas Conference on Information Systems (AMCIS 2016)*, San Diego, California: AIS.
- Ghazizadeh, E., & Cusack, B. (2017a). Evaluating Identity Theft Protections by Trust-Based Model for Cloud Computing, *presented at the meeting of the The 11th Annual Postgraduate Research Symposium*, Auckland, New Zealand.
- Ghazizadeh, E., & Cusack, B. (2017b). Trust Assessment for Cloud Identity Providers Using Analytical Hierarchy Process. *presented at the meeting of the The 2017 International Conference on Computational Science and Computational Intelligence (CSCI'17)*, Las Vegas, USA.
- Ghazizadeh, E., Manan, J.-I. A., Zamani, M., & Pashang, A. (2012). A survey on security issues of federated identity in the cloud computing, *4th International Conference of the Cloud Computing Technology and Science (CloudCom)*, Taipei, Taiwan: IEEE.
- Ghazizadeh, E., Shams Dolatabadi, Z., Khaleghparast, R., Zamani, M., Manaf, A. A., & Abdullah, M. S. (2014). Secure OpenID authentication model by using Trusted Computing, *Abstract and Applied Analysis*, 2014: Hindawi Publishing Corporation.

- Ghazizadeh, E., Zamani, M., Ab Manan, J.-I., & Alizadeh, M. (2014). Trusted computing strengthens cloud authentication. *The Scientific World Journal*, 2014: Hindawi Publishing Corporation.
- Ghazizadeh, E., Zamani, M., Ab Manan, J.-I., Khaleghparast, R., & Taherian, A. (2012). A trust based model for federated identity architecture to mitigate identity theft, *International Conference of the Internet Technology And Secured Transactions*, London, UK: IEEE.
- Gikas, C. (2010). A General Comparison of FISMA, HIPAA, ISO 27000 and PCI-DSS Standards. *Information Security Journal: A Global Perspective*, 19(3), 132-141.
- Goepel, K. D. (2013). Implementing the analytic hierarchy process as a standard method for multi-criteria decision making in corporate enterprises—a new AHP excel template with multiple inputs, *In Proceedings of the international symposium on the analytic hierarchy process* (Vol. 2013, pp. 1-10): Creative Decisions Foundation Kuala Lumpur.
- Gonzales, D., Kaplan, J. M., Saltzman, E., Winkelman, Z., & Woods, D. (2017). Cloud-trust—A security assessment model for infrastructure as a service (IaaS) clouds. *IEEE Transactions on Cloud Computing*, 5(3), 523-536.
- Goode, J. (2012). The importance of identity security. *Computer Fraud & Security*, 2012(1), 5-7.
- Gopalakrishnan, A. (2009). Cloud computing identity management. *SETLabs briefings*, 7(7), 45-55.
- Gopinath, P. G., & Vasudevan, S. K. (2015). An in-depth analysis and study of Load balancing techniques in the cloud computing environment. *Procedia Computer Science*, 50, 427-432.
- Gunter, C. A., Liebovitz, D., & Malin, B. (2011). Experience-based access management: A life-cycle framework for identity and access management systems. *IEEE Security & Privacy*, 9(5), 48.
- Haber, D. (2006). Life review: Implementation, theory, research, and therapy. *The International Journal of Aging and Human Development*, 63(2), 153-171.
- Habib, S. M., Hauke, S., Ries, S., & Mühlhäuser, M. (2012). Trust as a facilitator in cloud computing: a survey. *Journal of Cloud Computing*, 1(1), 1-18.
- Habib, S. M., Ries, S., & Mühlhäuser, M. (2011a). Towards a trust management system for cloud computing. *10th International Conference on Symposium conducted at the meeting of the Trust, Security and Privacy in Computing and Communications (TrustCom)*, Changsha, China: IEEE.
- Habiba, U., Masood, R., Shibli, M. A., & Niazi, M. A. (2014). Cloud identity management security issues & solutions: a taxonomy. *Complex Adaptive Systems Modeling*, 2(1), 1-37.
- Haley, D. F., Vo, L., Parker, K. A., Frew, P. M., Golin, C. E., Amola, O., Lancaster, K. (2017). Qualitative Methodological Approach. In *Poverty in the United States* (pp. 9-23): Springer.
- Hallappanavar, V. L., & Birje, M. N. (2016). Trust Management in Cloud Computing. *Security Solutions for Hyperconnectivity and the Internet of Things*, 151.
- Harmony, C. (2016). *CloudHarmony, transparency for the cloud*. Retrieved from <https://cloudharmony.com>
- Håvaldsrud, T., Møller-Pedersen, B., Solhaug, B., & Stølen, K. (2012). DeSPoT: A Method for the Development and Specification of Policies for Trust Negotiation. In *Computer Science and Convergence* (pp. 93-104): Springer.

- Hedberg, R., Gulliksson, R., Jones, M. B., & J. Bradley. (2018). *OpenID Connect Federation 1.0 - draft 04*. Retrieved from <https://openid.net/specs/openid-connect-federation-1.0.html>
- Hevner, A., & Chatterjee, S. (2010). *Design science research in information systems*: Springer.
- Hevner, A., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS quarterly*, 28(1), 75-105.
- Hilgers, R., & Auger, G. (2015). Public Cloud Security Final Report.
- Hoffman, K., Zage, D., & Nita-Rotaru, C. (2009). A survey of attack and defense techniques for reputation systems. *ACM Computing Surveys (CSUR)*, 42(1), 1.
- Houghton, C., Murphy, K., Meehan, B., Thomas, J., Brooker, D., & Casey, D. (2017). From screening to synthesis: using nvivo to enhance transparency in qualitative evidence synthesis. *Journal of clinical nursing*, 26(5-6), 873-881.
- Hu, V. C., Ferraiolo, D., Kuhn, R., Schnitzer, A., Sandlin, K., Miller, R., & Scarfone, K. (2014). Guide to attribute based access control (ABAC) definition and considerations. *NIST Special Publication*, 800, 162.
- Huang, He, L., Liao, X., Dai, H., & Ji, M. (2016). Developing a trustworthy computing framework for clouds. *International Journal of Embedded Systems*, 8(1), 59-68.
- Huang, & Nicol, D. M. (2013). Trust mechanisms for cloud computing. *Journal of Cloud Computing*, 2(1), 1-14.
- Hughes, J., & Maler, E. (2005). Security assertion markup language (saml) v2. 0 technical overview (pp. 29-38): OASIS SSTC
- Iriberri, A., & Leroy, G. (2009). A life-cycle perspective on online community success. *ACM Computing Surveys (CSUR)*, 41(2), 11.
- Ivanov, T., Niemann, R., Izberovic, S., Rosselli, M., Tolle, K., & Zicari, R. V. (2015). Performance Evaluation of Enterprise Big Data Platforms with HiBench, *Symposium conducted at the meeting of the Trustcom/BigDataSE/ISPA*, 2015, Helsinki, Finland: IEEE.
- Jahani, A., & Khanli, L. M. (2016). Cloud service ranking as a multi objective optimization problem. *The Journal of Supercomputing*, 1-30.
- Jansen, W. (2011). Cloud hooks: Security and privacy issues in cloud computing, *44th Hawaii International Conference on Symposium conducted at the meeting of the System Sciences (HICSS)*, Kauai, Hawaii USA: IEEE.
- Johannesson, P., & Perjons, E. (2014a). *An introduction to design science*: Springer.
- Johannesson, P., & Perjons, E. (2014b). A Method Framework for Design Science Research. In *An Introduction to Design Science* (pp. 75-89): Springer.
- Joshi, K. P., & Pearce, C. (2015). Automating cloud service level agreements using semantic technologies, *International Conference of the Cloud Engineering (IC2E)*, Tempe, AZ, USA: IEEE.
- Joshi, K. P., Yesha, Y., & Finin, T. (2014). Automating cloud services life cycle through semantic technologies. *Services Computing, IEEE Transactions on*, 7(1), 109-122.
- Jyotiyana, J. P., & Mishra, A. (2016). Secure Authentication: Eliminating Possible Backdoors in Client-Server Endorsement. *Procedia Computer Science*, 85, 606-615.

- Kanstrén, T., & Evesti, A. (2015). Security Metrics, Secure Elements, and Operational Measurement Trust in Cloud Environments. In *Security and Trust Management* (pp. 37-51): Springer.
- Kanwal, A., Masood, R., & Shibli, M. A. (2014). Evaluation and establishment of trust in cloud federation, *Proceedings of the 8th International Conference on Ubiquitous Information Management and Communication*, Siem Reap, Cambodia: ACM.
- Kanwal, A., Masood, R., Shibli, M. A., & Mumtaz, R. (2014). Taxonomy for Trust Models in Cloud Computing. *The Computer Journal*, bxu138.
- Khalid, U., Ghafoor, A., Irum, M., & Shibli, M. A. (2013). Cloud based secure and privacy enhanced authentication & authorization protocol. *Procedia Computer Science*, 22, 680-688.
- Khalil, Khreishah, A., & Azeem, M. (2014). Cloud computing security: a survey. *Computers*, 3(1), 1-35.
- Khodashahri, N. G., & Sarabi, M. M. H. (2013). Decision Support System (DSS). *Singaporean Journal of Business, Economics and Management Studies*, 1(6), 95-102.
- Kim, K. I., Ishag, M. I. M., Kim, M., Kim, J. S., & Ryu, K. H. (2016). Proposal of a Resource-Monitoring Improvement System Using Amazon Web Service API. Symposium conducted at the meeting of the International Conference on Computer Science and its Applications: Springer.
- Kostopoulos, A., Sfakianakis, E., Chochliouros, I., Pettersson, J. S., Krenn, S., Tesfay, W., Hörandner, F. (2017). Towards the Adoption of Secure Cloud Identity Services, *Symposium conducted at the meeting of the Proceedings of the 12th International Conference on Availability, Reliability and Security*: Reggio Calabria, Italy: ACM.
- Kshetri, N. (2013). Privacy and security issues in cloud computing: The role of institutions and institutional evolution. *Telecommunications Policy*, 37(4), 372-386.
- Lai, L. S., & To, W. (2010). Importance-performance analysis for public management decision making: An empirical study of China's Macao special administrative region. *Management Decision*, 48(2), 277-295.
- Latif, R., Abbas, H., Assar, S., & Ali, Q. (2014). Cloud computing risk assessment: a systematic literature review. In *Future Information Technology* (pp. 285-295): Springer.
- Leandro, M. A., Nascimento, T. J., dos Santos, D. R., Westphall, C. M., & Westphall, C. B. (2012). Multi-tenancy authorization system with federated identity for cloud-based environments using shibboleth, *The Eleventh International Conference on Networks Symposium conducted at the meeting of the ICN 2012*, Saint Gilles, Reunion Island
- Lee, J.-K., Kim, S.-J., Woo, J., & Park, C. Y. (2015). Analysis and Response of SSH Brute Force Attacks in Multi-User Computing Environment. *KIPS Transactions on Computer and Communication Systems*, 4(6), 205-212.
- Lehrig, S., Eikerling, H., & Becker, S. (2015). Scalability, elasticity, and efficiency in cloud computing: A systematic literature review of definitions and metrics, *Symposium conducted at the meeting of the Proceedings of the 11th International ACM SIGSOFT Conference on Quality of Software Architectures*, Montréal, QC, Canada: ACM.

- Leicher, A., Schmidt, A. U., & Shah, Y. (2012). Smart OpenID: a smart card based OpenID protocol. *International Information Security Conference of the IFIP*, Berlin, Heidelberg: Springer.
- Lewis, R. (2004). Importance-performance analysis. *Australasian Journal of Engineering Education*, 2, 1-8.
- Li, A., Yang, X., Kandula, S., & Zhang, M. (2010). CloudCmp: comparing public cloud providers, *10th ACM SIGCOMM conference on Internet measurement*, Melbourne, Australia: ACM.
- Li, W., & Mitchell, C. J. (2014). Security issues in OAuth 2.0 SSO implementations, *International Conference on Information Security*: Springer.
- Li, X., & Du, J. (2013). Adaptive and attribute-based trust model for service level agreement guarantee in cloud computing. *Information Security, IET*, 7(1), 39-50.
- Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., & Leaf, D. (2011). NIST cloud computing reference architecture. *NIST special publication*, 500(2011), 292.
- Liu, F., Wang, J., Bai, H., & Sun, H. (2015). Access Control Model Based on Trust and Risk Evaluation in IDMaas. *12th International Conference on Symposium conducted at the meeting of the Information Technology-New Generations (ITNG)*, Las Vegas, NV, USA: IEEE.
- Liu, Z., Nadim, F., Garcia-Aristizabal, A., Mignan, A., Fleming, K., & Luna, B. Q. (2015). A three-level framework for multi-risk assessment. *Georisk: Assessment and Management of Risk for Engineered Systems and Geohazards*, 9(2), 59-74.
- Lonea, A. M., Tianfield, H., & Popescu, D. E. (2013). Identity management for cloud computing. In *New Concepts and Applications in Soft Computing* (pp. 175-199): Springer.
- Lopez, M. (2000). *An evaluation theory perspective of the architecture tradeoff analysis method (ATAM)*: DTIC Document.
- Loutfi, I., & Jøsang, A. (2015). Fido trust requirements. In *Secure IT Systems* (pp. 139-155): Springer.
- Luo, Liu, J., Xiong, J., & Wang, L. (2015). Defending Against Whitewashing Attacks in Peer-to-Peer File-Sharing Networks. *4th International Conference on Computer Engineering and Networks*: Springer.
- Luo, C., Zhan, J., Jia, Z., Wang, L., Lu, G., Zhang, L., Sun, N. (2012). Cloudrank-d: benchmarking and ranking cloud computing systems for data processing applications. *Frontiers of Computer Science*, 6(4), 347-362.
- Macedo, R., Ghamri-Doudane, Y., & Nogueira, M. (2015). Mitigating dos attacks in identity management systems through reorganizations. *Symposium conducted at the meeting of the Network Operations and Management Symposium (LANOMS)*, Joao Pessoa, Brazil: IEEE.
- Madsen, P., Koga, Y., & Takahashi, K. (2005). Federated identity management for protecting users from ID theft. *Symposium conducted at the meeting of the Proceedings of the 2005 workshop on Digital identity management*: ACM.
- Mahalle, P. N., Anggorojati, B., Prasad, N. R., & Prasad, R. (2013). Identity authentication and capability based access control (iacac) for the internet of things. *Journal of Cyber Security and Mobility*, 1(4), 309-348.
- Mantelaers, P. (1997). Acquiring expert knowledge on IS function design. In *Information Systems and Qualitative Research* (pp. 324-340): Springer.

- Manuel, P. (2015). A trust model of cloud computing based on Quality of Service. *Annals of Operations Research*, 233(1), 281-292.
- Manzoor, S., Zhang, H., & Suri, N. (2018). Threat Modeling and Analysis for the Cloud Ecosystem, *International Conference on Symposium conducted at the meeting of the Cloud Engineering (IC2E)*, Orlando, FL, USA: IEEE.
- Mármol, F. G., Girao, J., & Pérez, G. M. (2010). TRIMS, a privacy-aware trust and reputation model for identity management systems. *Computer Networks*, 54(16), 2899-2912.
- Martilla, J. A., & James, J. C. (1977). Importance-performance analysis. *The journal of marketing*, 77-79.
- Marudhadevi, D., Dhatchayani, V. N., & Sriram, V. S. (2014). A Trust Evaluation Model for Cloud Computing Using Service Level Agreement. *The Computer Journal*, bxu129.
- Mathew, B. A., Sebastian, S., Sabu, V., & Joseph, S. (2015). Trusted Load Balancing Mechanism for MANET, *International Conference on Advanced Computing and Communication Techniques for High Performance Applications :Foundation of Computer Science (FCS)*
- Mell, P., & Grance, T. (2011). The NIST definition of cloud computing.
- Méndez, A. P., López, R. M., & Millán, G. L. (2016). Providing efficient SSO to cloud service access in AAA-based identity federations. *Future Generation Computer Systems*, 58, 13-28.
- Messina, F., Pappalardo, G., Rosaci, D., Santoro, C., & Sarné, G. M. (2013). A trust-based approach for a competitive cloud/grid computing scenario. In *Intelligent Distributed Computing VI* (pp. 129-138): Springer.
- Messina, F., Pappalardo, G., Rosaci, D., & Sarné, G. M. (2014). A trust-based, multi-agent architecture supporting inter-cloud vm migration in iaas federations. *International Conference on Internet and Distributed Computing Systems*: Springer, Cham.
- Mittal, S., Joshi, K. P., Pearce, C., Joshi, A., Nair, S., Mittal, S., Pearce, C. (2016). Automatic Extraction of Metrics from SLAs for Cloud Service Management, *International Conference on Cloud Engineering (IC2E 2016)*, Berlin, Germany: IEEE.
- Mohammadkhanli, L. J., Arezoo. (2014). Ranking Approaches for Cloud Computing Services Based on Quality of Service: A Review *ARPJ Journal of Systems and Software*, 4(2), 50-57.
- Moreno-Vozmediano, R., Montero, R. S., & Llorente, I. M. (2013). Key challenges in cloud computing: Enabling the future internet of services. *Internet Computing, IEEE*, 17(4), 18-25.
- Mostowski, W., & Vullers, P. (2011). Efficient U-Prove implementation for anonymous credentials on smart cards. *International Conference on Security and Privacy in Communication Systems*, Berlin, Heidelberg :Springer.
- Na, S. H., & Huh, E. N. (2014). A broker-based cooperative security-SLA evaluation methodology for personal cloud computing. *Security and Communication networks*.
- Nicolaidou, I. L., & Georgiades, C. (2017). The GDPR: New Horizons. In *EU Internet Law* (pp. 3-18). Cham, Switezland: Springer.
- Niedbalski, J., & Ślęzak, I. (2017). Computer Assisted Qualitative Data Analysis Software. Using the NVivo and Atlas. ti in the research projects based on

- the methodology of grounded theory. In *Computer Supported Qualitative Research* (pp. 85-94): Springer.
- NIST. (2013a). *Final Version of NIST Cloud Computing Definition Published*. Retrieved from <http://www.nist.gov/itl/csd/cloud-102511.cfm>
- NIST. (2013b). *NIST Cloud Computing Standards Roadmap*
- Noor, T. H., & Sheng, Q. Z. (2011). Trust as a service: a framework for trust management in cloud environments. In *Web Information System Engineering–WISE 2011* (pp. 314-321): Springer.
- Noor, T. H., Sheng, Q. Z., Maamar, Z., & Zeadally, S. (2016). Managing Trust in the Cloud: State of the Art and Research Challenges. *Computer*, 49(2), 34-45.
- Noor, T. H., Sheng, Q. Z., Zeadally, S., & Yu, J. (2013). Trust management of services in cloud environments: Obstacles and solutions. *ACM Computing Surveys (CSUR)*, 46(1), 12.
- Offermann, P., Levina, O., Schönherr, M., & Bub, U. (2009). Outline of a design science research process. *4th International Conference on Design Science Research in Information Systems and Technology*, Philadelphia, Pennsylvania: ACM.
- Okoli, C., & Nguyen, J. (2015). Business Models for Free and Open Source Software, *21st Americas Conference on Information Systems*. Puerto Rico: AIS.
- Oliver, S., Harden, A., Rees, R., Shepherd, J., Brunton, G., Garcia, J., & Oakley, A. (2005). An emerging framework for including different types of evidence in systematic reviews for public policy. *Evaluation*, 11(4), 428-446.
- Omar, M., Challal, Y., & Bouabdallah, A. (2009). Reliable and fully distributed trust model for mobile ad hoc networks. *Computers & Security*, 28(3), 199-214.
- OpenID. (2016). *RISC (Risk and Incident Sharing and Coordination) WG*. Retrieved from <http://openid.net/wg/risc/>
- Parker, R. B. (2017). A definition of privacy. In *Privacy* (pp. 83-104): Routledge.
- Patel, R., Borisaniya, B., Patel, A., Patel, D., Rajarajan, M., & Zisman, A. (2010). Comparative analysis of formal model checking tools for security protocol verification. In *Recent Trends in Network Security and Applications* (pp. 152-163): Springer.
- Pearson, S. (2013). Privacy, security and trust in cloud computing. In *Privacy and Security for Cloud Computing* (pp. 3-42): Springer.
- Pecori, R. (2016). S-Kademlia: A trust and reputation method to mitigate a Sybil attack in Kademlia. *Computer Networks*, 94, 205-218.
- Peffer, K., Rothenberger, M., Tuunanen, T., & Vaezi, R. (2012). Design science research evaluation. *International Conference on Design Science Research in Information Systems*, Berlin, Heidelberg: Springer.
- Peffer, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of management information systems*, 24(3), 45-77.
- Philips, Z., Ginnelly, L., Sculpher, M., Claxton, K., Golder, S., Riemsma, R., . . . Glanville, J. (2004). Review of guidelines for good practice in decision-analytic modelling in health technology assessment.
- Posey, L. (2016). *Introduction to the Consensus Assessments Working Group*. Retrieved from https://cloudsecurityalliance.org/group/consensus-assessments/#_overview

- Potter, B. (2009). Microsoft SDL threat modelling tool. *Network Security*, 2009(1), 15-18.
- Power, D. J., Sharda, R., & Burstein, F. (2015). *Decision support systems*: Wiley Online Library.
- Prasad, A. V. K. (2016). Architecture for Improving Security in Web Environment. *Design Solutions for Improving Website Quality and Effectiveness*, 316.
- Prat, N., Comyn-Wattiau, I., & Akoka, J. (2014). Artifact Evaluation in Information Systems Design-Science Research-a Holistic View. *Symposium conducted at the meeting of the PACIS*: Citeseer.
- Qu, L., Wang, Y., & Orgun, M. A. (2013). Cloud service selection based on the aggregation of user feedback and quantitative performance assessment. *International Conference of the Services Computing (SCC)*, Santa Clara, CA, USA: IEEE.
- Quinn, S. D., Souppaya, M., Cook, M., & Scarfone, K. (2011). National Checklist Program for IT Products—Guidelines for Checklist Users and Developers. *NIST Special Publication*, 800, 70.
- Rannenber, K., Camenisch, J., & Sabouri, A. (2015). *Attribute-based credentials for trust*. . Bern, Switzerland: Springer.
- Raykova, M., Zhao, H., & Bellovin, S. M. (2012). Privacy enhanced access control for outsourced data sharing. In *Financial cryptography and data security* (pp. 223-238): Springer.
- Recordon, D., & Reed, D. (2006). OpenID 2.0: a platform for user-centric identity management, *the second ACM workshop on Digital identity management*, Alexandria, Virginia, USA: ACM.
- Richer, O. J., & Tschofenig, H. (2012). OAuth 2.0 Message Authentication Code (MAC) Tokens draft-ietf-oauth-v2-http-mac-02.
- Ries, S. (2007). Certain trust: a trust model for users and agents. *ACM symposium on Applied computing*, Seoul, Korea: ACM.
- Ries, S., Habib, S. M., Mühlhäuser, M., & Varadharajan, V. (2011). Certainlogic: A logic for modeling trust and uncertainty. *International Conference on Trust and Trustworthy Computing*: Springer.
- Riquet, D., Grimaud, G., & Hauspie, M. (2012). Large-scale coordinated attacks: Impact on the cloud security, *Sixth International Conference of the Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS)*, Palermo, Italy: IEEE.
- Rittinghouse, J. W., & Ransome, J. F. (2016). *Cloud computing: implementation, management, and security*: CRC press.
- Robinson, O. C. (2014). Sampling in interview-based qualitative research: A theoretical and practical guide. *Qualitative Research in Psychology*, 11(1), 25-41.
- Rolls, D. (2003). Service Provisioning Markup Language (SPML) Version 1.0: OASIS Committee Specification.
- Rountree, D. (2012). *Federated identity primer*: Newnes.
- Ruiz, M. D. M. L., & Pedraza, J. (2016). Privacy Risks in Cloud Computing. In *Intelligent Agents in Data-intensive Computing* (pp. 163-192): Springer.
- Russell, B. (2016). *Internet of Things Working Group*. Retrieved from <https://cloudsecurityalliance.org/group/internet-of-things/>
- Saaty, T. L. (1989). Group decision making and the AHP. In *The Analytic Hierarchy Process* (pp. 59-67). Berlin, Heidelberg: Springer.

- Saaty, T. L. (2005). *Theory and applications of the analytic network process: decision making with benefits, opportunities, costs, and risks*: RWS publications.
- Saaty, T. L., & Kearns, K. P. (2014). *Analytical planning: The organization of system* (Vol. 7): Elsevier.
- Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., & Mortimore, C. (2014). Openid connect core 1.0. *The OpenID Foundation*, S3.
- Saleem, Y., Iqbal, M. M., Amjad, M., Bashir, M. S., Faisal, M., Farhan, M., . . . Shah, A. A. (2012). High Security and Privacy in Cloud Computing Paradigm through Single Sign On 1.
- Saleh, A. S. A., Hamed, E. M. R., & Hashem, M. (2014). Building trust management model for cloud computing, *9th International Conference of the Informatics and Systems (INFOS)*, Cairo, Egypt: IEEE.
- Samani, R., Reavis, J., & Honan, B. (2014). *CSA Guide to Cloud Computing: Implementing Cloud Privacy and Security*: Syngress.
- Samuel, O., Omisore, M., & Ojokoh, B. (2013). A web based decision support system driven by fuzzy logic for the diagnosis of typhoid fever. *Expert Systems with Applications*, 40(10), 4164-4171.
- Sato, H., Kanai, A., & Tanimoto, S. (2010). A cloud trust model in a security aware cloud. *10th IEEE/IPSJ International Symposium of the Applications and the Internet (SAINT)*, Seoul, South Korea: IEEE.
- Satty, T. L. (1980). *The analytic hierarchy process*. Berlin, Heidelberg: Springer.
- Scandariato, R., Wuyts, K., & Joosen, W. (2015). A descriptive study of Microsoft's threat modeling technique. *Requirements Engineering*, 20(2), 163-180.
- Schäffer, B. (2011). Authentication and Authorization in Spatial Data Infrastructures.
- Schneider, S., & Sunyaev, A. (2016). Determinant factors of cloud-sourcing decisions: reflecting on the IT outsourcing literature in the era of cloud computing. *Journal of Information Technology*, 31(1), 1-31.
- Schryen, G., Volkamer, M., Ries, S., & Habib, S. M. (2011). A formal approach towards measuring trust in distributed systems. *ACM Symposium on Applied Computing*, TaiChung, Taiwan: ACM
- Sethi, S., & Sruti, S. (2018). Cloud Security Issues and Challenges. In *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications* (pp. 77-92). Sarang, India: IGI Global.
- Shaikh, R., & Sasikumar, M. (2013). Identity Management in Cloud Computing. *International Journal of Computer Applications*, 63(11).
- Shaikh, R., & Sasikumar, M. (2015). Trust Model for Measuring Security Strength of Cloud Computing Service. *Procedia Computer Science*, 45, 380-389.
- Shin, S., & Kobara, K. (2010). Towards secure cloud storage. *CloudCom2010*, 2, 8.
- Shirley Crompton, M. W. (2011). *Consequence: the context-aware data-centric information sharing*. Retrieved from <http://www.consequence-project.eu>.
- Siegel, J., & Perdue, J. (2012). Cloud services measures for global use: the Service Measurement Index (SMI). *Annual SRII Global Conference*, San Jose, CA, USA: IEEE.
- Skopik, F., Schall, D., & Dustdar, S. (2010). Modeling and mining of dynamic trust in complex service-oriented systems. *Information Systems*, 35(7), 735-757.

- Sobel, W., Subramanyam, S., Sucharitakul, A., Nguyen, J., Wong, H., Klepchukov, A., Patterson, D. (2008). Cloudstone: Multi-platform, multi-language benchmark and measurement tools for web 2.0, *in Proc. of CCA (vol 8)*
- Song, L., Wei, J., Wang, L., Cao, C., & Niu, X. (2015). Identity-based storage management and integrity verify protocol for secure outsourcing in multi-cloud. *Concurrency and Computation: Practice and Experience*, 28(6), 1870-1871.
- spotcloud. (2016). *A Global Market for Cloud Capacity*. Retrieved from <http://www.spotcloud.com/>
- Sprague Jr, R. H. (1980). A framework for the development of decision support systems. *MIS quarterly*, 4(4), 1-26.
- Stergiou, C., Psannis, K. E., Kim, B.-G., & Gupta, B. (2018). Secure integration of IoT and cloud computing. *Future Generation Computer Systems*, 78, 964-975.
- Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, 34(1), 1-11.
- Sun, & Liu, Y. (2012). Security of Online Reputation Systems: The evolution of attacks and defenses. *IEEE Signal Process. Mag.*, 29(2), 87-97.
- Sun, D., Chang, G., Sun, L., & Wang, X. (2011). Surveying and analyzing security, privacy and trust issues in cloud computing environments. *Procedia Engineering*, 15, 2852-2856.
- Sun, Y. L., & Liu, Y. (2012). Security of Online Reputation Systems: The evolution of attacks and defenses. *IEEE Signal Process. Mag.*, 29(2), 87-97.
- SWIFT. (2015). Secure widespread identities for federated telecommunications. Germany: Fraunhofer Gesellschaft Zur Foerderung Der Angewandten Forschung.
- Tanimoto, S., Hiramoto, M., Iwashita, M., Sato, H., & Kanai, A. (2011). Risk management on the security problem in cloud computing, *International Conference on Computers, Networks, Systems and Industrial Engineering (CNSI)*, Jeju Island, South Korea: IEEE.
- Theoharidou, M., Tsalis, N., & Gritzalis, D. (2013). In cloud we trust: Risk-Assessment-as-a-Service, *International Conference on Trust Management*, Berlin, Heidelberg: Springer.
- Tormo, G. D., Mármol, F. G., & Pérez, G. M. (2014). Identity Management in Cloud Systems. In *Security, Privacy and Trust in Cloud Systems* (pp. 177-210). Berlin, Heidelberg: Springer.
- Tormo, G. D., Mármol, F. G., & Pérez, G. M. (2015). Dynamic and flexible selection of a reputation mechanism for heterogeneous environments. *Future Generation Computer Systems*, 49, 113-124.
- Tzeng, G.-H., & Huang, J.-J. (2011). *Multiple attribute decision making: methods and applications*: CRC press.
- Vapen, A., Carlsson, N., Mahanti, A., & Shahmehri, N. (2015). Information sharing and user privacy in the third-party identity management landscape. *International Information Security Conference*, Hamburg, Germany: Springer.
- Viganò, L. (2006). Automated security protocol analysis with the AVISPA tool. *Electronic Notes in Theoretical Computer Science*, 155, 61-86.

- Vu, L. H., Zhang, J., & Aberer, K. (2014). Using Identity Premium for Honesty Enforcement and Whitewashing Prevention. *Computational Intelligence*, 30(4), 771-797.
- Vujin, V., Simić, K., & Kovačević, B. (2014). Digital Identity Management in Cloud. In *Handbook of Research on High Performance and Cloud Computing in Scientific Research and Education* (pp. 56-81): IGI Global.
- Wagle, S. S., Guzek, M., Bouvry, P., & Bisdorff, R. (2015). An evaluation model for selecting cloud services from commercially available cloud providers, *7th International Conference on Cloud Computing Technology and Science* (CloudCom), Vancouver, BC, Canada: IEEE.
- Wang, & Lin, K.-J. (2008). Reputation-oriented trustworthy computing in e-commerce environments. *Internet Computing, IEEE*, 12(4), 55-59.
- Wang, H., Fan, C., Yang, S., Zou, J., & Zhang, X. (2011). A new secure OpenID authentication mechanism using one-time password (OTP), Symposium conducted at the meeting of the 7th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM) Wuhan, China: IEEE.
- Wang, L., Li, X., Yan, X., Qing, S., & Chen, Y. (2015). Service Dynamic Trust Evaluation Model based on Bayesian Network in Distributed Computing Environment. *distributed computing*, 9(5).
- Wang, W., Zeng, G., Zhang, J., & Tang, D. (2012). Dynamic trust evaluation and scheduling framework for cloud computing. *Security and Communication Networks*, 5(3), 311-318.
- Wang, X., Lao, G., DeMartini, T., Reddy, H., Nguyen, M., & Valenzuela, E. (2002). XrML--eXtensible rights Markup Language, the 2002 ACM workshop on XML security, Fairfax, VA, USA: ACM
- Weber, A., Herbst, N., Groenda, H., & Kounev, S. (2014). Towards a Resource Elasticity Benchmark for Cloud Environments. *2nd International Workshop on Hot Topics in Cloud service Scalability*, Dublin, Ireland: ACM.
- Welsh, E. (2002). Dealing with data: Using NVivo in the qualitative data analysis process. *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research*, 3(2).
- Werner, J., Westphall, C. M., & Westphall, C. B. (2017). Cloud identity management: A survey on privacy strategies. *Computer Networks*, 122, 29-42.
- West, A. W. (2016). Avoiding Some of the Pitfalls of a CMS Website. In *Practical Web Design for Absolute Beginners* (pp. 397-401). Apress, Berkeley, CA: Springer.
- Widiantari, M. M., & Budiman, A. (2018). Development of Presentation Model with Cloud Based Infrastructure, *MATEC Web of Conferences: EDP Sciences*.
- Wu, X., Zhang, R., Zeng, B., & Zhou, S. (2013). A trust evaluation model for cloud computing. *Procedia Computer Science*, 17, 1170-1177.
- Xiao, Z., & Xiao, Y. (2013). Security and privacy in cloud computing. *Communications Surveys & Tutorials, IEEE*, 15(2), 843-859.
- Yan, L., Rong, C., & Zhao, G. (2009). Strengthen cloud computing security with federal identity management using hierarchical identity-based cryptography S, *International Conference on Cloud Computing*, Beijing, China: Springer.

- Yaniv, I., & Kleinberger, E. (2000). Advice taking in decision making: Egocentric discounting and reputation formation. *Organizational behavior and human decision processes*, 83(2), 260-281.
- Yao, J., Chen, S., Wang, C., Levy, D., & Zic, J. (2010). Accountability as a service for the cloud, *International Conference on Services Computing (SCC)*, Miami, FL, USA: IEEE.
- Yuan, X., Nuakoh, E. B., Williams, I., & Yu, H. (2015). Developing Abuse Cases Based on Threat Modeling and Attack Patterns. *JSW*, 10(4), 491-498.
- Zhang, & Zhang, X. (2012). A trust vector approach to transaction context-aware trust evaluation in e-commerce and e-service environments, *5th IEEE International Conference on Service-Oriented Computing and Applications (SOCA)*, Taipei, Taiwan: IEEE.
- Zhang, M., & Huo, B. (2013). The impact of dependence and trust on supply chain integration. *International Journal of Physical Distribution & Logistics Management*, 43(7), 544-563.
- Zhang, N., Lou, W., Jiang, X., & Hou, Y. T. (2014). Enabling Trusted Data-intensive execution in cloud computing, *Conference on Communications and Network Security (CNS)*, San Francisco, CA, USA: IEEE.
- Zhang, X., Wuwong, N., Li, H., & Zhang, X. (2010). Information security risk management framework for the cloud computing environments, *10th International Conference on Computer and Information Technology (CIT)*, Bradford, UK: IEEE.
- Zheng, Z., Wu, X., Zhang, Y., Lyu, M. R., & Wang, J. (2013). QoS ranking prediction for cloud services. *Parallel and Distributed Systems, IEEE Transactions on*, 24(6), 1213-1222.
- Zhu, L., & Tung, B. (2015). Public Key Cryptography for Initial Authentication in Kerberos (PKINIT). Network Working Group.
- Zimmermann, H.-J. (2012). *Fuzzy sets, decision making, and expert systems* (Vol. 10): Springer Science & Business Media.
- Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, 28(3), 583-592.

Appendix A

Ethic application approval from AUTECH



AUTECH Secretariat
Auckland University of Technology
D-88, WU406 Level 4 WU Building City Campus
T: +64 9 921 9999 ext. 8316
E: ethics@aut.ac.nz
www.aut.ac.nz/researchethics

10 April 2017
Brian Cusack
Faculty of Design and Creative Technologies

Dear Brian

Re Ethics Application: **17/86 Evaluating identity theft protections by trust-based model for cloud computing**

Thank you for providing evidence as requested, which satisfies the points raised by the Auckland University of Technology Ethics Committee (AUTECH).

Your ethics application has been approved for three years until 10 April 2020.

As part of the ethics approval process, you are required to submit the following to AUTECH:

- A brief annual progress report using form EA2, which is available online through <http://www.aut.ac.nz/researchethics>. When necessary this form may also be used to request an extension of the approval at least one month prior to its expiry on 10 April 2020;
- A brief report on the status of the project using form EA3, which is available online through <http://www.aut.ac.nz/researchethics>. This report is to be submitted either when the approval expires on 10 April 2020 or on completion of the project.

It is a condition of approval that AUTECH is notified of any adverse events or if the research does not commence. AUTECH approval needs to be sought for any alteration to the research, including any alteration of or addition to any documents that are provided to participants. You are responsible for ensuring that research undertaken under this approval occurs within the parameters outlined in the approved application.

AUTECH grants ethical approval only. If you require management approval from an institution or organisation for your research, then you will need to obtain this.

To enable us to provide you with efficient service, please use the application number and study title in all correspondence with us. If you have any enquiries about this application, or anything else, please do contact us at ethics@aut.ac.nz.

All the very best with your research,



Kate O'Connor
Executive Secretary
Auckland University of Technology Ethics Committee

Cc: eghaziza@aut.ac.nz

Appendix B

Consensus Assessments

- 1. Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)? *

☒ YES ☐ NO ☐ N/A

- 2. Do you monitor and log privileged access (e.g., administrator level) to information security management systems? *

☒ YES ☐ NO ☐ N/A

- 3. Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes? *

User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer

(tenant) ☒ YES ☐ NO ☐ N/A

- 4. Do you provide metrics to track the speed with which you are able to remove systems access that is no longer required for business purposes? *

☒ YES ☐ NO ☐ N/A

- 5. Do you use dedicated secure networks to provide management access to your cloud service infrastructure? *

☒ YES ☐ NO ☐ N/A

- 6. Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access? *

☒ YES ☐ NO ☐ N/A

- 7. Do you manage and store the user identity of all personnel who have network access, including their level of access? *

☒ YES ☐ NO ☐ N/A

- 8. Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering? *

☒ YES ☐ NO ☐ N/A

- 9. Are controls in place to prevent unauthorized access to your application, program, or object source code, and assure it is restricted to authorized personnel only? *

☒ YES ☐ NO ☐ N/A

- 10. Are controls in place to prevent unauthorized access to tenant application, program, or object source code, and assure it is restricted to authorized personnel only? *

☒ YES ☐ NO ☐ N/A

- 11. Do you provide multi-failure disaster recovery capability? *

☒ YES ☐ NO ☐ N/A

- 12. Do you monitor service continuity with upstream providers in the event of provider failure? *

☒ YES ☐ NO ☐ N/A

- 13. Do you have more than one provider for each service you depend on? *

☒ YES ☐ NO ☐ N/A

- 14. Do you provide access to operational redundancy and continuity summaries, including the services you depend on? *

☒ YES ☐ NO ☐ N/A

- 15. Do you provide the tenant the ability to declare a disaster? *

☒ YES ☐ NO ☐ N/A

- 16. Do you provide a tenant-triggered failover option? *

☒ YES ☐ NO ☐ N/A

- 17. Do you share your business continuity and redundancy plans with your tenants? *

☒ YES ☐ NO ☐ N/A

- 18. Do you document how you grant and approve access to tenant data? *
☒ YES ☐ NO ☐ N/A
- 19. Do you have a method of aligning provider and tenant data classification methodologies for access control purposes? *
☒ YES ☐ NO ☐ N/A
- 20. Does your management provision the authorization and restrictions for user access prior to their access to data and any owned or managed applications, infrastructure systems, and network components? *
☒ YES ☐ NO ☐ N/A
- 21. Do you provide upon request user access to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components? *
☒ YES ☐ NO ☐ N/A
- 22. Do you require at least annual certification of entitlements for all system users and administrators (exclusive of users maintained by your tenants)? *
☒ YES ☐ NO ☐ N/A
- 23. If users are found to have inappropriate entitlements, are all remediation and certification actions recorded? *
☒ YES ☐ NO ☐ N/A
- 24. Will you share user entitlement remediation and certification reports with your tenants, if inappropriate access may have been allowed to tenant data?
☒ YES ☐ NO ☐ N/A
- 25. Is timely deprovisioning, revocation, or modification of user access to the organizations systems, information assets, and data implemented upon any change in status of employees, contractors, customers, business partners, or involved third parties? *
☒ YES ☐ NO ☐ N/A
- 26. Is any change in user access status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization? *

☒ YES ☐ NO ☐ N/A

- 27. Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service? *

☒ YES ☐ NO ☐ N/A

- 28. Do you use open standards to delegate authentication capabilities to your tenants? *

☒ YES ☐ NO ☐ N/A

- 29. Do you support identity federation standards (e.g., SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users? *

☒ YES ☐ NO ☐ N/A

- 30. Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access? *

☒ YES ☐ NO ☐ N/A

- 31. Do you have an identity management system (enabling classification of data for a tenant) in place to enable both role-based and context-based entitlement to data? *

☒ YES ☐ NO ☐ N/A

- 32. Do you provide tenants with strong (multifactor) authentication options (e.g., digital certs, tokens, biometrics, etc.) for user access? *

☒ YES ☐ NO ☐ N/A

- 33. Do you allow tenants to use third-party identity assurance services? *

☒ YES ☐ NO ☐ N/A

- 34. Do you support password (e.g., minimum length, age, history, complexity) and account lockout (e.g., lockout threshold, lockout duration) policy enforcement? *

☒ YES ☐ NO ☐ N/A

- 35. Do you allow tenants/customers to define password and account lockout policies for their accounts? *

☒ YES ☐ NO ☐ N/A

- 36. Do you support the ability to force password changes upon first logon? *

☒ YES ☐ NO ☐ N/A

- 37. Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge questions, manual unlock)? *

☒ YES ☐ NO ☐ N/A

- 38. Are utilities that can significantly manage virtualized partitions (e.g., shutdown, clone, etc.) appropriately restricted and monitored? *

☒ YES ☐ NO ☐ N/A

- 39. Do you have the capability to detect attacks that target the virtual infrastructure directly (e.g., shimming, Blue Pill, Hyper jumping, etc.)? *

☒ YES ☐ NO ☐ N/A

- 40. Are attacks that target the virtual infrastructure prevented with technical controls? *

☒ YES ☐ NO ☐ N/A

Appendix C

Risk Assessment

- 1. How LIKELY would be compromised and misused the log data? *
☐ RARE ☐ UNLIKELY ☒ POSSIBLE ☐ LIKELY ☐ FREQUENT
- 2. How LIKELY would be compromised and misused least privilege based on job function? *
☐ RARE ☐ UNLIKELY ☒ POSSIBLE ☐ LIKELY ☐ FREQUENT
- 3. How LIKELY would be compromised access segmentation to sessions and data in multi-tenant architectures by any third party? *
☐ RARE ☐ UNLIKELY ☒ POSSIBLE ☐ LIKELY ☐ FREQUENT
- 4. How LIKELY would be compromised and misused account credential life-cycle management from instantiation through revocation? *
☐ RARE ☐ UNLIKELY ☒ POSSIBLE ☐ LIKELY ☐ FREQUENT
- 5. How LIKELY would be compromised and reuse account credential? *
☐ RARE ☐ UNLIKELY ☒ POSSIBLE ☐ LIKELY ☐ FREQUENT
- 6. How LIKELY would be compromised and misused non-shared authentication secrets? *
☐ RARE ☐ UNLIKELY ☒ POSSIBLE ☐ LIKELY ☐ FREQUENT
- 7. How LIKELY would be compromised and misused rules for access to data and sessions? *
☐ RARE ☐ UNLIKELY ☒ POSSIBLE ☐ LIKELY ☐ FREQUENT
- 8. How LIKELY would be compromised and misused legal, statutory, or regulatory compliance requirements? *
☐ RARE ☐ UNLIKELY ☒ POSSIBLE ☐ LIKELY ☐ FREQUENT
- 9. How LIKELY would be compromised and misused access to configuration port of authorized individuals and applications? *

☐ RARE ☐ UNLIKELY ☒ POSSIBLE ☐ LIKELY ☐ FREQUENT

- 10. How LIKELY would be compromised and misused level of access to infrastructures?? *

☐ RARE ☐ UNLIKELY ☒ POSSIBLE ☐ LIKELY ☐ FREQUENT

- 11. How LIKELY would be compromised segregation of duties and conflict of interest? *

☐ RARE ☐ UNLIKELY ☒ POSSIBLE ☐ LIKELY ☐ FREQUENT

- 12. How LIKELY would be compromised and misused Source Code Access Restriction? *

☐ RARE ☐ UNLIKELY ☒ POSSIBLE ☐ LIKELY ☐ FREQUENT

- 13. How LIKELY would be the risk of third-party access to the organization's information systems and data? *

☐ RARE ☐ UNLIKELY ☒ POSSIBLE ☐ LIKELY ☐ FREQUENT

- 14. How LIKELY would be the risk of permissible storage and access of user's identity? *

☐ RARE ☐ UNLIKELY ☒ POSSIBLE ☐ LIKELY ☐ FREQUENT

- 15. How LIKELY would be the risk of user access revocation? *

☐ RARE ☐ UNLIKELY ☒ POSSIBLE ☐ LIKELY ☐ FREQUENT

- 16. How LIKELY would be the risk of user ID credential disclosure? *

☐ RARE ☐ UNLIKELY ☒ POSSIBLE ☐ LIKELY ☐ FREQUENT

- 17. How LIKELY would be the risk of compromising utility program access? *

☐ RARE ☐ UNLIKELY ☒ POSSIBLE ☐ LIKELY ☐ FREQUENT

- 18. How LIKELY would be the risk of policy expiration assignment? *

☐ RARE ☐ UNLIKELY ☒ POSSIBLE ☐ LIKELY ☐ FREQUENT

- 19. How LIKELY would be the risk of policy conflicts (if multiple policies enforcement is available) of Identity and access Management (IAM)? *

☐ RARE ☐ UNLIKELY ☒ POSSIBLE ☐ LIKELY ☐ FREQUENT

- 20. How LIKELY would be the risk of IAM leaking of permissions? *

☐ RARE ☐ UNLIKELY ☒ POSSIBLE ☐ LIKELY ☐ FREQUENT

- 21. How LIKELY would be the risk of bypassing non-reputation system between provider and subscriber? *

☐ RARE ☐ UNLIKELY ☒ POSSIBLE ☐ LIKELY ☐ FREQUENT

- 22. How LIKELY would be the risk of Identity theft? *

☐ RARE ☐ UNLIKELY ☒ POSSIBLE ☐ LIKELY ☐ FREQUENT

- 23. How LIKELY would be the risk of Vendor lock-in issue? *

☐ RARE ☐ UNLIKELY ☒ POSSIBLE ☐ LIKELY ☐ FREQUENT

- 24. How LIKELY would be the risk of insider threat? *

☐ RARE ☐ UNLIKELY ☒ POSSIBLE ☐ LIKELY ☐ FREQUENT

- 25. How LIKELY would be the risk of privileged escalation? *

☐ RARE ☐ UNLIKELY ☒ POSSIBLE ☐ LIKELY ☐ FREQUENT

- 26. How LIKELY would be compromised and misused the delegation of authorizations/ entitlement? *

☐ RARE ☐ UNLIKELY ☒ POSSIBLE ☐ LIKELY ☐ FREQUENT

- 27. How LIKELY would be compromised and misused password management? *

☐ RARE ☐ UNLIKELY ☒ POSSIBLE ☐ LIKELY ☐ FREQUENT

- 28. How LIKELY would be the risk of non-real time provisioning and de-provisioning? *

☐ RARE ☐ UNLIKELY ☒ POSSIBLE ☐ LIKELY ☐ FREQUENT

- 29. How **LIKELY** would be compromised and misused transparency to the user? *

☐ RARE ☐ UNLIKELY ☒ POSSIBLE ☐ LIKELY ☐ FREQUENT