

UNIVERSITY OF SOUTHAMPTON

FACULTY OF PHYSICAL SCIENCES AND ENGINEERING

Electronics and Computer Science (ECS)

Cyber physical Systems (CPS)

A Security Model for Cloud Computing Adoption in Saudi Arabian Government Organisations

By

Madini Alassafi

M.S., California Lutheran University, Thousand Oaks, USA, 2013

B.S., King Abdulaziz University, Jeddah, KSA, 2006

Thesis for the degree of Doctor of Philosophy in Computer Science

February 2018

Dedicated To

My father and my mother

For raising me to believe that anything is possible

My brothers and sisters

My wife

For making everything possible

And, my sons

For making everything possible incredible

WITHOUT THEIR SUPPORT THIS WORK WOULD NOT HAVE BEEN ACCOMPLISHED

UNIVERSITY OF SOUTHAMPTON

ABSTRACT

FACULTY OF PHYSICAL SCIENCES AND ENGINEERING

Electronics and Computer Science

Doctor of Philosophy

**A Security Model for Cloud Computing Adoption in Saudi Government
Organisations**

By

Madini Alassafi

Cloud computing plays an essential role in public organisations and private sector companies, while also reducing the cost of using information technology services. Not only is cloud computing available for users to access anytime and anywhere, but also makes it possible for them to pay for only what they use. In Middle Eastern developing countries, such as Saudi Arabia, cloud computing is still not extensively adopted compared with countries in the West. In order to encourage the adoption of cloud services, this research addresses the essential to investigate the security factors which are associated with cloud computing, and which influence organisations' desire to adopt the cloud services. Subsequently, this study has developed a theoretical framework that associates security in cloud adoption.

In light of the above, the main contribution of this study is the Security Cloud Adoption Framework development in order to support an investigation into the security factors that influence the adoption of cloud computing in KSA government organisations. This research proposes a framework which can be used to understand and evaluate security in cloud adoption; particular emphasis is placed on risks, social aspects, and benefits when implementing security in the cloud services. The proposed framework consists of three categories, namely the Security Social category, the Cloud Security Risks category, and the Cloud Security Benefits category. The framework factors were identified by critically reviewing studies found in the literature, together with factors from the industrial standards within the context of the KSA. The methods used in this confirmatory study were expert interviews and questionnaires. Interviews were conducted with 12 security experts in different Saudi government organisations to confirm the aforementioned factors and to

identify those omitted from previous studies. The second method used was questionnaires, which were distributed to 32 IT and security experts from different Saudi government organisations in order to confirm the security factors in the security cloud adoption framework. This framework was subsequently developed. The outcomes from the expert interviews exposed that the proposed security factors in the security cloud adoption framework are statistically significant. In addition to this, the analysis of the interview outcomes and the questionnaire results indicated that there is an additional factor, namely Failure of Client-side encryption, which could potentially affect the adoption of cloud services in KSA government organisations. Experts and security specialists expressed the belief that this factor may influence cloud adoption. The findings of this research were used to improve the suggested framework.

Finally, in the validation study, a new instrument was used with 215 IT and security experts in different Saudi government organisations; the purpose of this was to explore the relationship among security factors and to test the model. The instrument was evaluated using a group of experiments; the security experts evaluated the instrument applying the content validity ratio, while the security experts had a part in the validation study. The validation study involved important two tests which examined the internal reliability and the correlation analyses. After applying Structural Equation Modelling (SEM), the resulting data clearly showed a good fit of the structural model and measurement analyses. The key outcomes of the validation study revealed that the relationships among security factors were discovered to have a direct and statistically significant effect in the model. This specifies that the proposed model fits the data and applies to the Saudi context.

The contributions of this research are as follows: firstly, it developed a security cloud framework within the KSA context and, secondly, the framework was extended to a security cloud instrument for measurement and validation of the model.

Overall, the outcomes of this study are of valuable information in terms of recommendations to cloud providers, government organisations, administrators, and policy makers. Simply put, these findings can assist in the implementation of cloud computing and encourage the spread of this phenomenon across countries in the Middle Eastern, particularly in Saudi Arabia.

Table of Contents

Table of Contents.....	iii
List of Tables.....	viii
List of Figures	xi
Declaration of Authorship.....	xiii
Publications	xv
Acknowledgements	xvii
Abbreviations	xix
Definitions	xxii
Chapter 1: Introduction.....	1
1.1 Background of Saudi Arabia Context.....	3
1.2 Motivation & Research Questions	4
1.3 Thesis Structure	8
1.4 Chapter Summary	12
Chapter 2: Background Literature	13
2.1 Overview of Cloud Computing	13
2.1.1 Essential Characteristics of Cloud Computing	14
2.1.2 Cloud Computing Service Models.....	15
2.1.3 Cloud Deployment Models.....	15
2.1.4 Fundamental Elements of Cloud for Government Organisations.....	16
2.1.5 Advantages and Disadvantages of Using Cloud Computing.....	18
2.1.6 Cloud Computing Adoption in Government Organisations.....	18
2.1.7 The Status of Cloud in Developed and Developing Countries	19
2.1.8 Cloud Computing Adoption Status in Saudi Government	20
2.2 Fundamentals of Cloud Computing Security	21
2.2.1 Cloud Computing Security Benefits	23
2.2.2 Cloud Computing Security Risks.....	24
2.3 Security Social Factors and Saudi Organisations.....	28
2.4 Review and Discussion of Related Work	29
2.5 Summary.....	33

Chapter 3: Cloud Security Framework for Saudi Government Organisations.....	35
3.1 The Framework Development and Confirmation Process	35
3.2 The Proposed Cloud Security Framework.....	39
3.2.1 Security Risk Factors	39
3.2.2 Security Social Factors	41
3.2.3 Security Benefits Factors	42
3.3 Summary.....	43
Chapter 4: Research Methodology Used in the First Stage for the Confirmatory Study.....	45
4.1 Background of Research Methods.....	46
4.1.1 Triangulation.....	47
4.1.2 Expert Interviews.....	48
4.1.3 Expert Interviews Sample Size	49
4.1.4 Questionnaire.....	49
4.2 Research Methods Used in the Confirmatory Study.....	50
4.2.1 Design of Expert Interviews.....	52
4.2.2 Piloting Interviews with Experts	54
4.2.3 Questionnaire Design	54
4.3 Summary.....	58
Chapter 5: Findings and Discussion for the Confirmatory Study .59	
5.1 Results of the Expert Review	59
5.1.1 Descriptive and Frequency Analyses of the Interviews	60
5.2 Results of the Questionnaire	69
5.2.1 Demographic Information	70
5.2.2 Descriptive and Frequency analyses of the Questionnaire	71
5.2.3 Analysis of Each Category Using One-Sample T-Test	77
5.2.4 Reliability Test of Questionnaire (Cronbach's Alpha)	79
5.3 Discussion of Findings	81
5.3.1 Findings Regarding the Categories in the Framework	81
5.3.2 Suggested Factors from Experts	84
5.4 Summary.....	85
Chapter 6: Research Methodology Used in the Second Stage for Developing and Validating the Instrument and the Model.....	87
6.1 Introduction.....	87

6.2	Research Philosophy.....	89
6.3	Research Approach	90
6.4	Research Strategy.....	91
6.5	Research Design.....	92
6.6	Population and Sample Size	93
6.7	Responses' Selection	94
6.8	Data Analysis and the Goodness of Instrument.....	95
6.8.1	Validity of the instrument	95
6.8.2	Reliability of the Instrument.....	95
6.8.3	Missing Values.....	97
6.9	Factors Analysis Procedures	98
6.9.1	Exploratory Factor Analysis (EFA)	99
6.9.2	Confirmatory Factor Analysis (CFA)	102
6.10	Ethics Approval Consideration	107
6.11	Summary.....	108
Chapter 7:	Results of the Development and Validation of the Instrument	111
7.1	Instrument Development and Design	111
7.2	Validity of the Instrument.....	114
7.2.1	The Instrument Pre-test.....	114
7.2.2	Content Validity of the Instrument.....	115
7.2.3	Results of Content Validity Ratio (CVR).....	116
7.3	Instrument Validation.....	119
7.3.1	Correlations Analysis of the Instrument.....	122
7.3.2	Correlation among Security Factors.....	123
7.4	Reliability of the Instrument	129
7.5	Discussion of the Validation Study and Reliability.....	130
7.6	Summary.....	132
Chapter 8:	Results and Discussion of the Model Validation Using Factor Analysis and Structural Equation Modelling (SEM).....	133
8.1	Preliminary Data Analysis.....	134
8.2	Handling Missing Values.....	135
8.3	Reliability Analysis Results of the Instrument.....	135

8.4	Demographic Data Analysis	136
8.5	Results of Exploratory Factor Analysis (EFA)	138
8.5.1	Assessment for Suitability of Data: Initial Considerations	138
8.5.2	Factor Extraction: Summarising Variables.....	139
8.5.3	Factor Rotation: Improving Interpretation of Factors	142
8.5.1	Factor Analysis Results.....	143
8.6	Results of Confirmatory Factor Analysis Using Structural Equation Modelling (SEM)	147
8.6.1	Analysis of Structural Measurement Model.....	147
8.6.2	The Assessment of Measurement Analysis Model Validity	148
8.6.3	Specifying Structural Model and Assessing the Relations	154
8.6.4	Structural Model Goodness of Fit (GoF)	158
8.6.5	Assessment of Hypotheses	161
8.7	Concluding Comments	174
Chapter 9:	Future Work.....	177
9.1	Conclusions	177
9.2	Fulfilling the Objectives of this Research.....	186
9.3	Research Contributions	188
9.3.1	First Contribution.....	188
9.3.2	Second Contribution	189
9.3.3	Third Contribution.....	189
9.4	Research Implications	190
9.4.1	Implications for Government Organisations.....	190
9.4.2	Implications for Security Practitioners.....	190
9.4.3	Implications for Researchers.....	191
9.5	Future Work Directions	191
9.6	Final Remarks	193
References	195
Appendix A	Confirmatory Study (Interviews)	207
A.1	Interview questions	207
A.2	Interview Analysis	209
A.3	Interview Themes Analysis.....	210
A.4	Interview Frequencies	212
Appendix B	Confirmatory Study (Questionnaire)	217
B.1	Questionnaire Frequencies.....	221

B.2	Questionnaire Reliability by Cronbach's Alpha.....	226
B.3	Questionnaire Analysis.....	227
Appendix C	Validation Study (Questionnaire)	230
C.1	Initial Instrument.....	230
C.2	Expert Evaluation Feedback	236
C.3	Content Validity Ratio Analysis.....	239
C.4	Content Validity Ratio Analysis for 67 Items.....	241
C.5	Correlations Matrix	242
C.6	Reliability.....	244
C.7	Improved Instrument.....	246
C.8	Exploratory Factor Analysis Results.....	251
C.8.1	Reliability among Security Factors.....	251
C.8.2	Correlations among Security Factors in the Instrument.....	252
C.8.3	KMO and Bartlett's Test.....	254
C.8.4	Communalities.....	254
C.8.5	Total Variance Explained.....	254
C.8.6	Scree Plot	256
C.8.7	Rotated Component Matrix	256
C.9	Confirmatory Factor Analysis Results.....	257
C.9.1	Construct Reliability.....	257
C.9.2	Measurement Model with Modifications Indices	258
C.9.3	Standardized Regression Weights	258
C.9.4	Standardized Estimates of the Model.....	259
C.9.5	Model Fit Summary.....	260

List of Tables

Table 2-1: Advantages and Disadvantages of Cloud Computing (Miller, 2009) ...	18
Table 2-2: Security Concepts (CIA) (Cherdantseva and Hilton, 2013).....	22
Table 2-3: Top Cloud Security Risks by Organisation Industries.	26
Table 2-4: Summary of the Top Security Risk Factors Studied.	27
Table 2-5: Summary of Review and Discussion of the Related Work.....	32
Table 4-1: Summary of the Interviewees with Their Position and Years of Experience	52
Table 4-2: Sample Size According to G*Power Software.....	56
Table 5-1: Frequency (Security Risk Factors)	62
Table 5-2: Frequency (Security Social Factors)	62
Table 5-3: Frequency (Security Benefit Factors)	64
Table 5-4: Expert Interviewees' Reasons for Using and Not Using Cloud Computing.	69
Table 5-5: Demographic Survey Frequency	70
Table 5-6: Security Risks Frequency	71
Table 5-7: Security Social Factors Frequency.....	74
Table 5-8: Security Benefits Frequency.....	75
Table 5-9: Analysis of Security Risk Factors Using One-Sample T-Test.....	77
Table 5-10: Analysis of Security Social Factors Using One-Sample Test.....	78
Table 5-11: Analysis of Security Benefits Factors Using One-Sample Test	79
Table 5-12: Reliability Statistics of Questionnaire	80

Table 5-13: Questionnaire Reliability Statistics Based on Cronbach's Alpha Measure	81
Table 6-1: Cronbach's Alpha Reliability Scores.....	96
Table 7-1: Measurement Items of Research Variables.....	113
Table 7-7-2: Content Validity Ratio among Items of the Instrument	118
Table 7-3: Validated Questionnaire's Items	119
Table 7-4: Strength for Correlation Coefficient (Cohen et al., 2011)	123
Table 7-5: Abbreviation Represented for Each Factor	123
Table 7-6: Correlation Matrix among Security Factors.....	128
Table 7-7: Cronbach's alpha reliability analysis for all Items	129
Table 7-8: Cronbach's alpha reliability analysis results	130
Table 8-1: Reliability Analysis Using Cronbach's Alpha	135
Table 8-2: The Demographic Data of the Participants' Responses.	136
Table 8-3: KMO Test Result.....	139
Table 8-4: Eigenvalues and Total Variance	140
Table 8-5: Factor Loading (Communalities) Using Orthogonal Rotation	142
Table 8-6: Latent Constructs and Indicator Variables	148
Table 8-7: Summarisation of Criteria for the Reliability of the Measurement Model	150
Table 8-8: Results of the Reliability Analysis Test for the Measurement Model	150
Table 8-9: Descriptions of Validity Types in Structural Equation Modelling with Their Requirements	151

Table 8-10: The Analysis of Convergent Validity.....	153
Table 8-11: Discriminant Validity Analysis Test	153
Table 8-12: The Hypotheses Measurement Paths in the Structural Model Specification (CFA Model)	154
Table 8-13: Squared Multiple Correlation between Construct Variables and Components	157
Table 8-14: Goodness of Fit Indexes with Their Level of Acceptance and References.....	159
Table 8-15: Goodness of Fit Indices Results for the Structural Model	160
Table 8-16: Model Fit Indices – RMSEA	160
Table 8-17: Summarisation of the Hypotheses Assessment and Results	161
Table 9-1: Summary of Methods Used in the First Stage of this Research.....	179
Table 9-2: Summary of Methods Used in the Second Stage of this Research....	182

List of Figures

Figure 1-1: Computing Paradigm Developments (1960s - 2017)	2
Figure 1-2: Summary of the Research Stages and Procedures.....	6
Figure 1-3: The Summary of the Research Flow and Chapters' Content	11
Figure 2-1: Conceptual View of Cloud Computing (NIST, 2011).....	14
Figure 2-2: Fundamental Elements of Cloud Computing for Government (Wyld and Robert, 2009)	17
Figure 3-1: Process for Developing Proposed Framework	38
Figure 3-2: Proposed Framework, Including Security Factors that Influence the Adoption of Cloud Computing in Saudi Government Organisations..	39
Figure 4-1: Research Methodology Process for Confirming the Framework	45
Figure 4-2: Methodological Triangulation Framework Validation	48
Figure 4-3: Methodological Triangulation for Confirming the Framework	51
Figure 5-1: Rating of Each Factor by Experts	60
Figure 5-2: Mean and Reliability Chart of the Questionnaire	80
Figure 5-3: Confirmed Framework Including Security Factors that Influence the Cloud Computing Adoption in Saudi Government Organisations	85
Figure 6-1: Research Design Steps for the Second Stage of this Research	88
Figure 6-2: Process of Stages for Structural Equation Modelling (Hair et al., 2010)	104
Figure 8-1: Factor Extraction Applied Scree Plot	141

Figure 8-2: Components and Constructs Retrieved from the Instrument.....	144
Figure 8-3: Screenshot of Specified Hypothesised and Standardised Output Estimates of Structural Model.....	156
Figure 8-4: Path Diagram of the Structural Model with Direct Effect	173

Declaration of Authorship

I, Madini Alassafi declare that this thesis, and the work presented in it, are my own and have been generated by me as the result of my own original research.

A Security Model for Cloud Computing Adoption in Saudi Government Organisations

I confirm that:

- This work was completed wholly or mainly while in candidature for a research degree at this university;
- Where any part of this thesis has previously been submitted for a degree or any other qualification at this university or any other institution, this has been clearly stated;
- Where I have consulted the published work of others, this is always clearly attributed;
- Where I have quoted from the work of others, the source is always provided. With the exception of such quotations, this thesis is entirely my own work;
- I have acknowledged all main sources of help;
- Where the thesis is based on work carried out by myself jointly with others, I have made clear exactly what has been done by others and what I have contributed myself;
- Parts of this work have been published as:

Alassafi, M. O., Alharthi, A., Alenezi, A., Walters, R. J., & Wills, G. B. (2016). Investigating the Security Factors in Cloud Computing Adoption: Towards Developing an Integrated Framework. *Journal of Internet Technology and Secured Transactions (JITST)*, 5(2), 486–494.

Alassafi, M. O., Hussain, R. K., Ghashgari, G., Walters, R. J., & Wills, G. B. (2017). Security in Organisations: Governance, Risks and Vulnerabilities in Moving to the Cloud. In *Enterprise Security*, Springer (pp. 241–258). https://doi.org/10.1007/978-3-319-54380-2_11

Alassafi, M. O., Alharthi, A., Walters, R. J., & Wills, G. B. (2017). Towards Developing an Integrated Framework for Investigating the Security Affect the Cloud Computing Adoption: *Journal of Internet Technology and Secured Transactions*.

Alassafi, M. O., Alharthi, A., Walters, R. J., & Wills, G. B. (2016). Security Risk factors that influence Cloud Computing Adoption in Saudi Arabia Government Agencies. I-Society Conference IEEE Advance Technology for Humanity, 1, 1–4. <https://doi.org/10.1109/i-Society.2016.7854165>

Alassafi, M. O., Alharthi, A., Walters, R. J., & Wills, G. B. (2017). A framework for critical security factors that influence the decision of cloud adoption by Saudi government agencies. Telematics and Informatics, 34(7), 996–1010. <https://doi.org/10.1016/j.tele.2017.04.010>

Signed:

Date:

Publications

- Alassafi, M. O., Alharthi, A., Alenezi, A., Walters, R. J., & Wills, G. B. (2016). Investigating the Security Factors in Cloud Computing Adoption: Towards Developing an Integrated Framework. *Journal of Internet Technology and Secured Transactions (JITST)*, 5(2), 486–494.
- Ahmed Albugmi; Alassafi, Madini O.; Robert, Walters; Gary, W. (2016). Data Security in Cloud Computing. *Fifth International Conference on FGCT IEEE*, 2(1), 1–169.
- Alassafi, M. O., Alharthi, A., Walters, R. J., & Wills, G. B. (2017). Towards Developing an Integrated Framework for Investigating the Security Affect the Cloud Computing Adoption: *Journal of Internet Technology and Secured Transactions*.
- Alassafi, M. O., Alharthi, A., Walters, R. J., & Wills, G. B. (2016). Security Risk factors that influence Cloud Computing Adoption in Saudi Arabia Government Agencies. *I-Society Conference IEEE Advance Technology for Humanity*, 1, 1–4. <https://doi.org/10.1109/i-Society.2016.7854165>
- Alassafi, M. O., Alharthi, A., Walters, R. J., & Wills, G. B. (2017). A framework for critical security factors that influence the decision of cloud adoption by Saudi government agencies. *Telematics and Informatics*, 34(7), 996–1010. <https://doi.org/10.1016/j.tele.2017.04.010>
- Alassafi, M. O., & Alsenani, Y. S. (2016). Inverse Matrix using Gauss Elimination Method by OpenMP. *International Journal of Information Technology and Computer Science*, 8(2), 41–46. <https://doi.org/10.5815/ijitcs.2016.02.05>
- Alharthi, A., Alassafi, M. O., Alzahrani, A. I., Walters, R. J., & Wills, G. B. (2017). Critical Success Factors for Cloud Migration in Higher Education Institutions: A Conceptual Framework. *International Journal of Intelligent Computing Research (IJICR)*, 8(1), 817–825.
- Alassafi, M. O., Hussain, R. K., Ghashgari, G., Walters, R. J., & Wills, G. B. (2017). Security in Organisations: Governance, Risks and Vulnerabilities in Moving to the Cloud. In *Enterprise Security*, Springer (pp. 241–258). https://doi.org/10.1007/978-3-319-54380-2_11
- Alharthi, A., Alassafi, M. O., Walters, R. J., & Wills, G. B. (2016). An exploratory study for investigating the critical success factors for cloud migration in the Saudi Arabian higher education context. *Telematics and Informatics*, 34(2), 664–678. <https://doi.org/10.1016/j.tele.2016.10.008>
- Alharthi, A., Alassafi, M. O., Walters, R. J., & Wills, G. B. (2017). Towards a framework to enable the migration process to educational clouds in Saudi higher education. In

International Conference on Information Society, i-Society 2016 (pp. 73–76).
<https://doi.org/10.1109/i-Society.2016.7854179>

Alzahrani, Abdullah, Alharthi, A., Alassafi, M. O., Walters, R. J., & Wills, G. B. (2018). A Framework for Gamified E-Learning Systems Acceptance in Saudi Arabian Universities : Gamified E-Learning ... *332nd International Conference on E-Education, E- Business, E-Management and E-Learning (IC4E)AtIstanbul, Turkey, (Feb)* (Accepted).

Atlam, H. F., Alassafi, M. O., Alenezi, A., Walters, R. J., & Wills, G. B. (2018). XACML to Build Access Control Policies for Internet of Things. *In Proceedings of the 3rd International Conference on Internet of Things, Big Data and Security (IoTBDs 2018)At19 - 21 March, 2018, Madeira - Portugal, (March)*. (Accepted)

Atlam, H. F., Alenezi, A., Alassafi, M. O., & Wills, G. B. (2018). Blockchain with Internet of Things : Benefits , Challenges , and Future Directions. *International Journal of Intelligent Systems and Applications(IJISA)*.

Md Sadek Ferdous, Raid Khalid Hussein, Madini O. Alassafi, Abdulrahman Alharthi, R. J. W. and G. W. (2016). TAXONOMY FOR CLOUD OF THINGS. *Internet of Things and Big Data Analysis: Recent Trends and Challenges - United Scholars Publications*, 1–27.

Acknowledgements

All my thanks go to Almighty Allah for the help, favours, mercies and blessings he has given me; these have enabled me to accomplish the present work. I would like to express my deepest gratitude to both of my supervisors, Dr Gary Wills and Dr Robert J Walters, for their support, guidance and feedback throughout this research study. They have always been wonderful supervisors; encouraging and helpful. Words just fail to express my heartfelt gratitude and appreciation – thank you both so much.

Likewise, to my supervisors, I would like to acknowledge the intellectual atmosphere and equipment provided by the Electronics and Computer Science Department at the University of Southampton during my study. I also wish to extend my sincere gratitude to the organisations and individuals who have been involved in and cooperated with this study by answering survey questionnaires and participating in various other ways. Their cooperation is very much appreciated in helping to achieve the objectives of this study. Thank you for always being supportive, and being there whenever needed.

It is my hope that this research can benefit organisations in the Kingdom of Saudi Arabia, and so I must sincerely acknowledge the awards of the King Abdul-Aziz University scholarship and the Saudi Arabian Cultural Bureau in London (SACB) for allowing the research to be funded and undertaken.

A special thank you is also dedicated to my friends and colleagues at the University of Southampton and in Saudi Arabia, especially Abdulrahman Alharthi, Ahmed Alenezi and Abdullah Alzahrani, for their guidance, collaboration in scientific publications, and moral support during calamities; I am very proud to have them as friends.

Also, a big thanks goes to my brothers Ali Alassafi, Dr. Abdulrahman Altalhi, and Hadi Oqaibi for their usual help and support. I really appreciate their help and encouragements.

My sincere thanks also go to my mother, father, brothers and my sisters, for their inspiration and encouragement, and for motivating me to attain my goal. I am grateful to my mother for her encouragement and prayers during my PhD journey.

A big thank you also goes to my wife (Galliah) and my sons (Faisal and Hussam) for their patience and for always energising me with their indispensable love and providing moral support throughout my life; they have reduced the pressure of this PhD during what has been an extremely stressful time. Again, my sincere thanks to my wife – I really cannot find the appropriate words to express my genuine gratitude for her assistance, love, immense patience, and for sacrificing her social life in coming with me to the UK and providing moral support throughout the PhD study.

Abbreviations

AH – Account or Service Hijacking

AS – Advanced Security Mechanism

CE – Cutting-edge Cloud Security Marketing

CFI – Comparative fit Index

CIA – Confidentiality, Integrity, and Availability

CPNI – Centre for the Protection of National Infrastructure

CR – Failure of Compliance with Regulations

CS – Cloud Security Auditing

CSA – Cloud Security Alliance

CSE – Failure of Client-side Encryption

CVR – Content Validity Ratio

DL – Data Leakage

DO – Data Ownership

ENISA – European Network and Information Security Agency

ERGO – Ethics Research Governance Online

GFI – Goodness of Fit Index

GoF – Goodness of fit

IaaS – Infrastructure as a Service

ICT – Information and Communication Technology

II – Insecure Interfaces

IoT – Internet of Things

IT – Information Technology

KMO – (Kaiser-Meyer-Olkin) Strength of the Relationships among the Variables measured

KSA – Kingdom of Saudi Arabia

MI – Malicious Insider

NIST – National Institute of Standards and Technology

OWASP – Organisation of the Open Web Application Security Project

PaaS – Platform as a Service

PR – Privacy

RC – Resource Concentration

RMR – Root Mean Square Residual

RMSEA – Root Mean Square Error of Approximation

SaaS – Software as a Service

SC – Security Culture

SDI – Service and Data Integration

SLA – Service Level Agreement (SLA) Audit Enforcement

SLA – Service Level Agreements

SRMR – Standardised Root Mean Square Residual

SS – Smart Scalable Security Benefits

SSI – Standardised Security Interfaces

ST – Shared Technology

TR – Trust

Definitions

Reliability – Extent to which a variable or set of variables is consistent in what it is intended to measure

Goodness of fit – Measure indicating how well a specified model reproduces the observed covariance matrix among the indicator variables

Government Organisations of Saudi Arabia – Including, Miniseries, Telecommunication organisations, State Universities, Research Institutes and Education Facilities

Exploratory Analysis – Analysis defining possible relationships in only the most general form and then allowing the multivariate technique to make known relationships

Eigenvalues – This method is used in deciding how many factors to extract in the overall factor analysis and is most commonly reported in factor analyses

Confirmatory Analysis – Use of multivariate technique to test (confirm) a perspective relationship

Correlation matrix – Table showing the intercorrelations among all variables

Cronbach's Alpha – Measure of reliability that ranges from 0 to 1

Chapter 1: Introduction

Cloud computing defines distributed computing which is linked through a network and which affords utility services to the end user (Mauch et al., 2013). It represents a way of providing computing resources based on various technology services, such as distributed systems, cluster computing, and web-based services (Buyya et al., 2009). In an economic recession, cloud computing technology services can play a considerable role in public organisations and private sector companies, since they reduce the cost of using Information Technology (IT) services in addition to offering certain other features (Alsanea and Barth, 2014).

Cloud Computing can be defined as a paradigm that has developed from previous computing paradigms. There are traditionally six different stages of development for computing (Zhang and Zhou, 2009), as illustrated in Figure 1-1. The first stage of computing development was mainframe computing, when a number of customers shared a CPU using a number of terminals. The second stage of the computing development was personal computing (PC), when every user used their own stand-alone PC. While in stage three of computing development, personal computers are networked together in a local area network. The fourth stage of computing development was the Internet, a network of networks.

In the fifth stage of computing movements, several high performance computing resources collaborate for a particular purposes; this stage is grid computing. Cloud computing is the sixth stage of computing movements, which is a development of computing resources on the internet as services, (Azeemi et al., 2013).

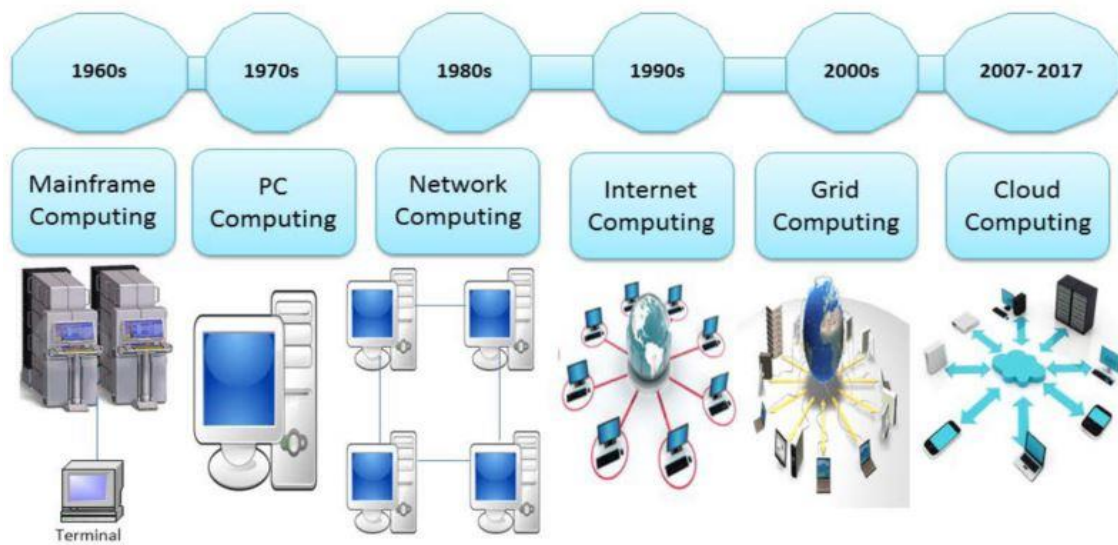


Figure 1-1: Computing Paradigm Developments (1960s - 2017)

The main objective of cloud computing technology is to lower companies' IT costs and offer organisations the chance to take control of their data centres. Several developed countries have begun to recognise the benefits of using cloud computing in government such as the United States, Australia and China which are considered developed countries (Bannerman, 2010). While the adoption of cloud computing services can provide many advantages for government services, few European countries have developed governmental cloud strategy plans (Elena and Johnson, 2015). The security concerns related to the cloud hinder many organisations' attempts to adopt cloud services (Sabahi, 2011). Such security concerns include physical security and simple access to facilities and equipment (Pearson, 2013). Furthermore, the security element has the potential to influence the acceptance of cloud computing across most of the world. In the KSA, the government has acknowledged the importance of cloud-based services and has laid out plans to establish government cloud services and other forms of cutting-edge technology, such as smart cities and IoTs sensing (Alsanea and Barth, 2014). KSA government organisations spent approximately £4 billion in 2010, and it is expected that whole spending for the subsequent years may have increased by as much as 10.2% (Alsanea and Barth, 2014). This specifies that, in the KSA, there is a negative attitude to

adopt and implement advanced technology. A number of studies have been conducted to investigate the effect of the social and management features that facilitate or pose challenges to cloud adoption in the KSA (Alsanea and Barth, 2014). Moreover, little is known about the security factors that influence cloud computing adoption services across the world (Elena and Johnson, 2015a). According to ICorps IT Consulting Technologies, by 2020 it is predictable that the rate of the cloud computing market will exceed \$270 billion. This forecast indicates that the cloud computing production is on the up and that the number of cloud customers around the world is increasing. Said increase in the use of cloud computing technology is directly related to the various benefits it offers, such as lower maintenance cost, low initial investment, and very high computation power (Kumar, 2010). It is clear that cloud adoption in the KSA is influenced by security risks and benefits awareness; in light of this, and in order to understand the influence of security on cloud computing adoption, the present research investigates the security risks, security social factors and security benefits associated with the adoption of cloud computing in Saudi government organisations.

1.1 Background of Saudi Arabia Context

This section delivers an overview of the Kingdom of Saudi Arabia (KSA), which is home to the largest petroleum companies in the Middle East, and has an estimated population of over 30 million. KSA is located in the southwest of Asia, and with Arabic listed as its official language, it is considered the largest Arab state in Western Asia (Alnatheer and Nelson, 2009). Saudi Arabia's resources are based on natural wealth, including petroleum, natural gas, iron ore, gold, and copper (Alateyah et al., 2013).

More and more governments around the world are presenting e-government as a means of decreasing costs, developing services, saving time and rising success and effectiveness in the public region. Consequently, e-government has been determined as one of the top priority for the KSA government and all its organisations (Alshehri and Drew, 2010). However, the adoption of any technology by the government organisation is experiencing a lot of concerns and obstacles such as technological, cultural,

organizational, and social problems which need be take into consideration when government plans its implementation (Alnatheer and Nelson, 2009). The ruling family of the Kingdom of Saudi Arabia oversees the government organisations. According to the Economist's 2010 Democracy indicator, the KSA government was the seventh most authoritarian government from among the 167 countries rated (Economist Intelligence Unit, 2010).

The Kingdom of Saudi Arabia has the largest information communication and technology market in the Middle East, in terms of both capital volume and spending. In addition, the vision of the KSA is to implement and promote controlled communication and IT systems to realise an IT community and a digital economy (Alarifi et al., 2012).

The KSA is one of the biggest market for Information and Communication Technology (ICT) in the Middle East. However, although the KSA government supports the ICT development across the country and has established a strategy for the next 20 years, ICT in KSA is considered to be in the developmental stage. The KSA government has initiated proceedings designed to improve business operations and disseminate the notion of e-services in different government organisation so as to achieve the vision 2030 (Alateyah et al., 2013).

1.2 Motivation & Research Questions

According to the World Bank, World Development Indicators, 2015, the Kingdom of Saudi Arabia (KSA) is the 19th largest economy in the world and is driven by the exportation of crude oil. The KSA is pushing itself in order to achieve strong economic expansion and move away from its oil-based economy (Alshahrani and Alsadiq, 2014).

When it comes to expanding the economic opportunities in the KSA, information and communication technology plays a very significant role in promoting the Saudi government's 2030 vision initiative, the aim of which is to diversify the country's economic income and technology (Alsanea and Barth, 2014). With organisations around the world looking towards third-party IT platforms such as mobile, big data, cloud computing, social media, etc., the KSA has realised that mobility and cloud computing

technology are important and may represent the most crucial future investment area of ICT technology (Kumar, 2010).

Despite the strong IT market and the allocated budget of adopting technologies, Saudi government organisations are still in the early stages of adopting the cloud, and there is a lack of research concerning the reasons behind the slow pace of this advancement toward the cloud (Alateyah et al., 2013).

In light of this, the main research goal here is to investigate the relevant security factors in order to develop an appropriate security framework that can help KSA government organisations to adopt cloud computing. In addition to this, another goal of this research is to develop and validate a cloud security adoption model for Saudi government organisations.

To achieve these goals, the research process is broken down into two main stages, as presented in Figure 1-2:

1. The framework development and confirmation.
2. Based on the confirmed framework in the previous stage, an instrument is developed and validated (validate the model to explore and confirm the significance of the relationships between the security factors by using the structural equation modelling technique).

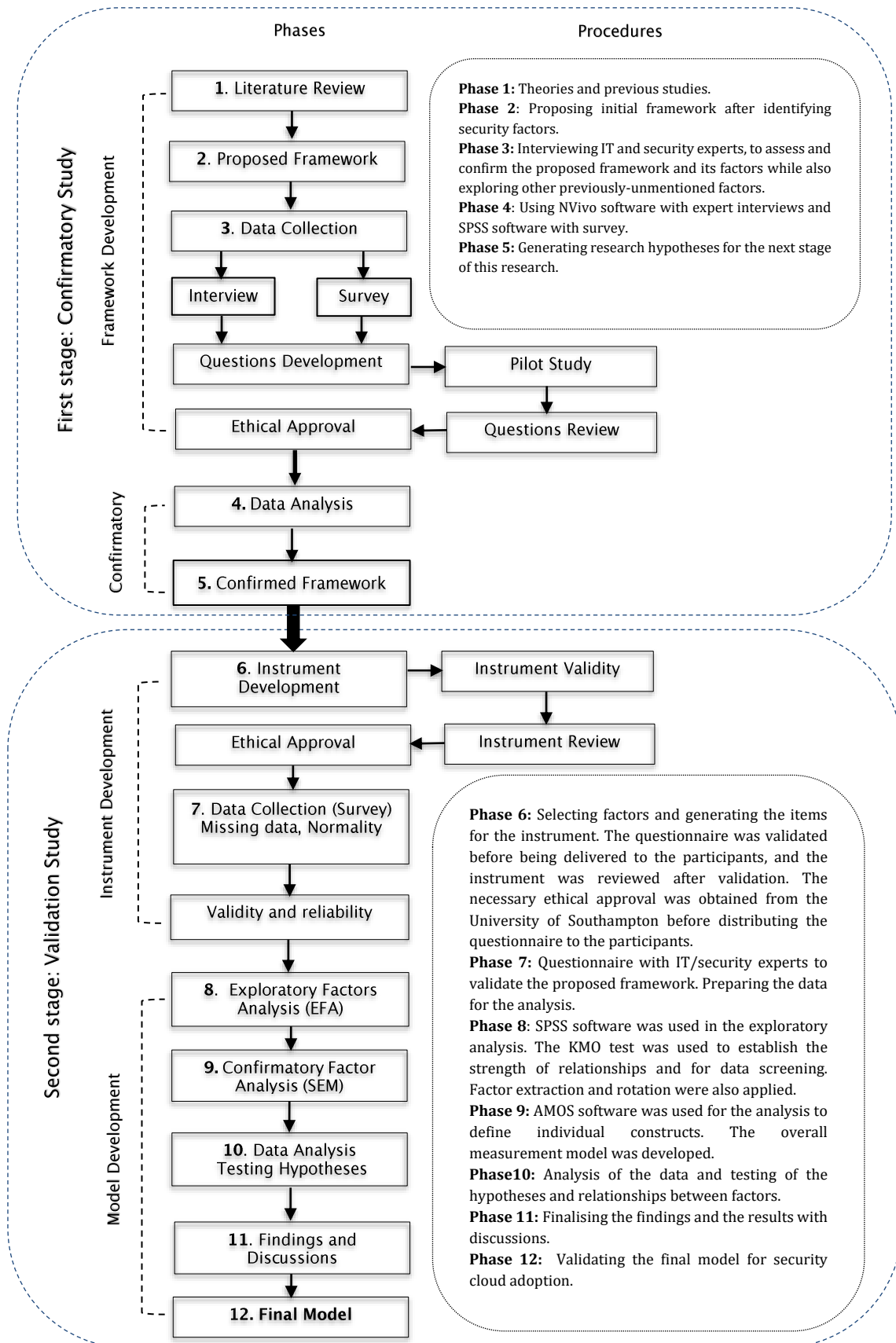


Figure 1-2: Summary of the Research Stages and Procedures

The first stage of this research was the development in order of an appropriate security framework for cloud computing adoption. The main questions and sub-questions to be answered are as follows:

RQ: ‘What is an appropriate framework with which to determine the influence of security factors on the adoption of cloud computing in the Saudi government organisations context?’

Q1: What are the security risk factors which affect cloud computing adoption?

Q2: What are the security benefits factors which affect cloud computing adoption?

Q3: What are the security social factors which affect cloud computing adoption?

The framework is constructed by exploring existing security frameworks which have been identified in previous research and recommended by industries. Subsequently, the resulting security factors can be used to facilitate the adoption, by KSA government organisations, of cloud computing services. After confirming the framework, the second stage of this research focuses on answering the follow research questions, Q4, Q5, and Q6, which are as follows:

Q4: What is a suitable instrument with which to evaluate security factors in the cloud adoption framework and how can the instrument be validated?

Q5: What are the relationship(s) among the security factors identified from the factor analysis and structural equation modelling?

Q6: Which relationship(s) between security factors will affect the desire of Saudi government organisations to adopt cloud computing services?

During this second stage, an instrument was developed and validated. The development of the model started with constructing an instrument based on the confirmed

framework in the confirmatory study. The instrument was applied in Saudi government organisations to establish which security-related factors influence these organisations' decision to adopt the cloud.

After applying the instrument to the KSA context, the instrument was evaluated using a statistical model. Hence, the research outcome contribution is important due to the following reasons:

- It helps KSA government organisations to identify the security factors which could potentially influence their adoption of cloud computing.
- It fills the gaps in existing research related to the influence of security factors on the adoption of cloud computing in KSA government organisations.
- It provides empirical data that can be beneficial to both cloud providers and researchers, and which may be used as a guide for cloud implementation projects in the context.

1.3 Thesis Structure

The remainder of this thesis is structured as follows, the flow and chapter contents are presented in Figure 1-3:

Chapter 2: This chapter presents a literature review comprising an overview of cloud computing paradigm principles and a critical review of work in the field of cloud adoption; discussion also focuses on the status of cloud adoption in different countries in general, and in the KSA in particular. Moreover, this chapter includes an exploration of security in cloud computing, security principles, cloud security benefits and cloud security risk factors; all of these factors have been highlighted in the literature according to different organisation industry standards. The main aim of this chapter is to pinpoint the most common factors affecting the adoption of cloud computing. Finally, this chapter recognises the study gaps.

Chapter 3: The purpose of this chapter is to present the initial proposed framework for security cloud adoption and to identify the factors that may influence government organisations' decision of adopting cloud computing services for the present research. This involves the phases and work carried out to develop and build the security cloud adoption framework in this research.

Chapter 4: The fourth chapter provides details on the research methods that applied in the first stage of this work (confirmatory study), as well as those used in the initial research. Qualitative and quantitative methods were employed, as both were deemed suitable for confirming the framework. Moreover, this chapter deliberates the calculation of the sample size and the approaches taken to designing the questions.

Chapter 5: This chapter presents the results and discussions of the first stage of the present research (confirmatory study). Moreover, this chapter illustrates the results of the mixed method research conducted by security experts in the KSA; the aim of this is to confirm the framework and identify any factors not alluded to during the expert interviews and not mentioned in the questionnaires. The findings from the expert reviews and questionnaires are analysed and discussed in order to refine and confirm the influential factors. This chapter also delivers an in-depth argument of these findings and the suggestions from the experts surveyed in this study.

Chapter 6: This chapter discusses the research methods applied in the second stage of this research to validate the proposed framework and test the study hypothesis. It begins with a brief discussion of the research philosophy and approach which are best suited to this research. It presents the research strategy applied in the second stage of this research, as well as the approaches taken to designing and developing the instrument. This chapter also describes the sample size and population which were considered suitable for this research, and the tests used for proving the validity of the instrument and reliability. Lastly, it clarifies the procedures of the factor analysis and Structural Equation Modelling (SEM) used for data analysis in the second stage of the research; this is followed by ethics approval consideration.

Chapter 7: This chapter presents the validation results and discussions of the instrument, including possible reasons for each finding pertaining to the relationships between factors in the proposed model. The development instrument is used to evaluate and validate the security cloud adoption model of this research. The instrument validation process went through a pre-test stage to ensure the validity of the content. After the pre-test stage, the validation parts were carry out to establish the reliability and validity of each factor in the instrument, and how it relates to the other factors. Correlation was applied to identify the relationships between the latent variables.

Chapter 8: This chapter discusses the model validation, which uses factor analysis and SEM, and was applied during the second stage of this research. Firstly, the missing data value from the collected data is deliberated, following which said data is analysed in terms of its demographic information. The reliability and validity of the instrument are presented in detail. The chapter presents the results of factor analysis, which consists of the initial considerations, assessment of appropriateness of data, and data screening results. The results of the factor extraction and rotation, which were applied during the factor analysis, are also presented in detail. The chapter then discusses the results yielded by the assessment of the proposed model over Structural Equation Modelling (SEM), which is utilised in two stages: first by measurement and then by the structural model. The chapter also provides an assessment of the proposed hypotheses. Finally, it deliberates, in detail, the impact of security risk factors, security social factors and security benefits factors on government organisations' willingness to adopt cloud services, along with the possible reasons for each outcome.

Chapter 9: This last chapter provides an overview of the research. The Conclusions and Future Work section addresses the main concept of the research. This chapter also highlights the contributions of the study and the limitations of the study. Finally, suggested directions for future work are included in this chapter.

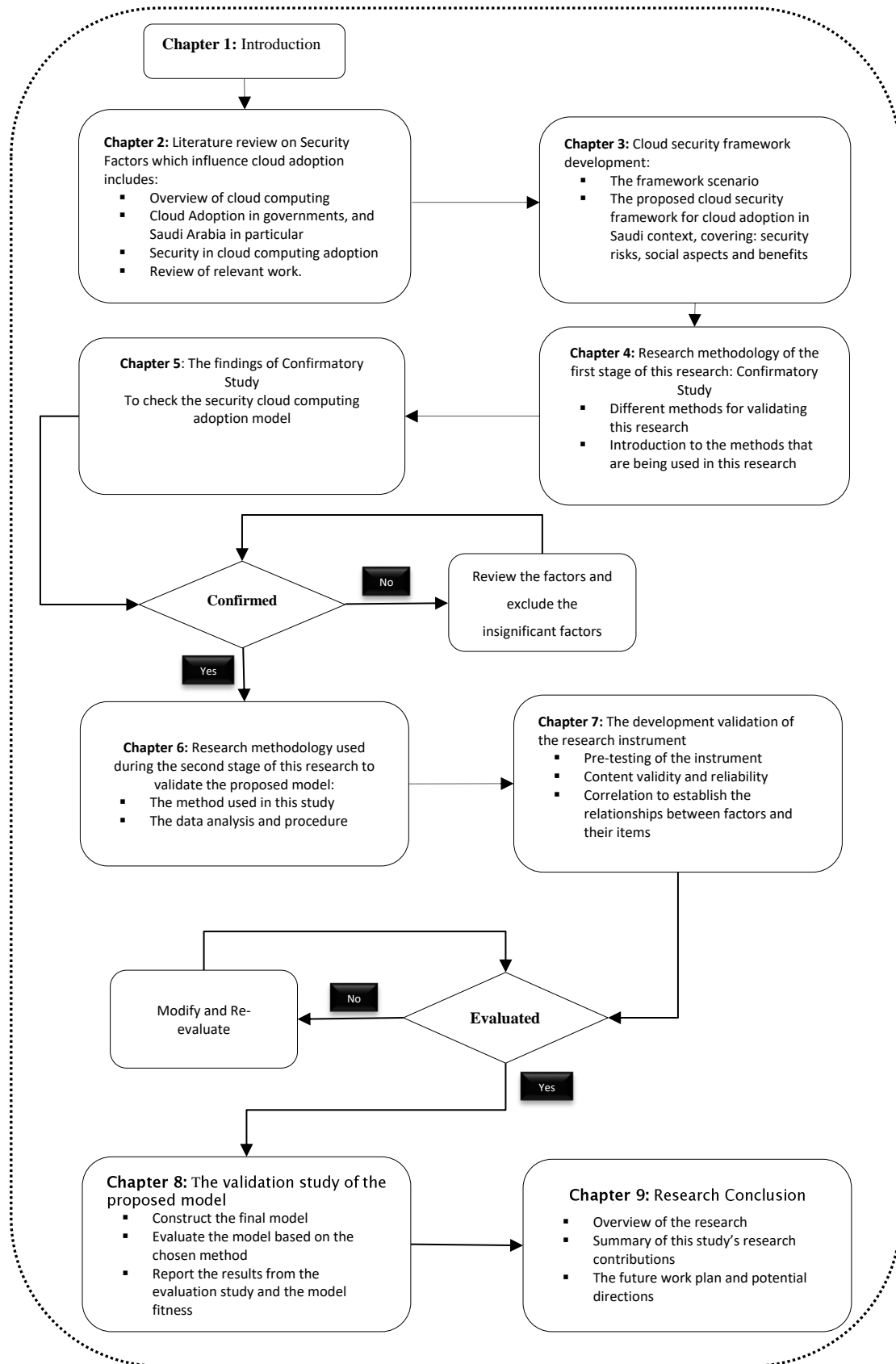


Figure 1-3: The Summary of the Research Flow and Chapters' Content

1.4 Chapter Summary

This chapter presented a picture of the research situation and the nature of the problem being addressed, following which a general overview of the Saudi Arabia context was provided. In addition to this, the chapter placed emphasis on the adoption status of cloud computing in KSA's government organisations and detailed the relevant research methodologies available in the literature. Subsequent discussion focused on the research questions, objectives and thesis structure, while the motivation which drives this study was also discussed. Finally, an overview of the thesis' structure was provided, which involved outlining the content discussed in subsequent chapters. With all of this in mind, the following chapter will focus on the context of this research, the research background, and the status of cloud adoption in developing and developed countries.

Chapter 2: Background Literature

With Chapter 1 having explained the research motivation, research questions and research context, this chapter provides the context of the present research. It offers an overview of the research background of conceptual cloud computing while also providing a review of important factors including security risk, social aspects, and benefits, all of which affect the implementation of cloud-based services by Saudi government organisations. In addition to this, the chapter also focuses on several relevant works related to the present research. In concluding, the chapter provides an example which illustrates the status of cloud adoption in developing and developed countries, with particular emphasis on the government context of these countries.

2.1 Overview of Cloud Computing

By adopting cloud computing services, government organisations can deploy their application systems over a group of independently-managed resources. However, the majority of such organisations count on their own custom needs, which must be considered if they decide to use cloud-based systems (Alharthi et al., 2016). As with any contemporary innovation, cloud computing usage and users' acceptance need to be understood, as users are key players in promoting new innovations. As a cloud computing model, many industry white papers and academics researchers have devoted a considerable amount of effort to defining and illustrating the notion of cloud computing.

There are many definitions of cloud computing. The definition used in this work is that put forth by the National Institute of Standards and Technology (NIST): *"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction"* (Catteddu and Hogben, 2009). The NIST has broken down the components of cloud computing into

five essential features, three cloud service models, and four cloud deployment models. Figure 2-1 illustrates the NIST conceptual view of cloud computing.

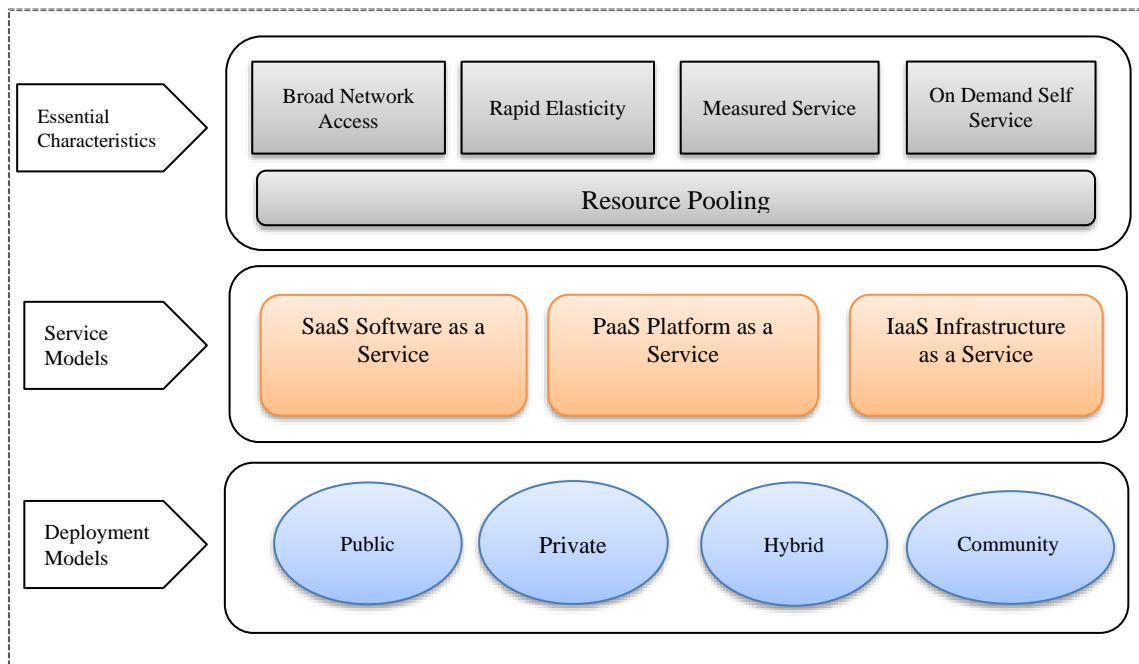


Figure 2-1: Conceptual View of Cloud Computing (NIST, 2011).

2.1.1 Essential Characteristics of Cloud Computing

The five essential characteristics of cloud computing are as follows (Mell and Grance, 2011):

- **On-Demand Self-Service:** A consumer can gain computing capabilities such as servers, networking, and storage as needed automatically, without the need for human interaction with a service provider.
- **Resource Pooling:** The providers' computing resources are pooled to serve numerous consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned, and reassigned, according to consumer demand.
- **Broad Network Access:** Capabilities are available over the network and accessed through standard mechanisms that promote their use by mixing thin- or thick-client platforms.
- **Rapid Elasticity:** Capabilities can be changed to quickly scale up, and can be rapidly released to scale down.

- **Measured Service:** Resource usage can be monitored, controlled and reported, thereby providing transparency for both the provider and consumer of the service.

2.1.2 Cloud Computing Service Models

Cloud service models define exactly how the cloud computing services available to the clients are organised. There are three different categories of service provided by cloud computing (Michael, 2010).

The **Infrastructure as a Service (IaaS)** model supplies infrastructure components to customers. These components may be virtual machines, storage facilities, networks, firewalls, load balancers, operating systems, databases, and so on. The consumer is able to deploy these components in their infrastructure. Examples of the IaaS model include Amazon Web Services and Dropbox (Badger et al., 2014).

The **Platform as a Service (PaaS)** model delivers a pre-built application platform to the customer. The PaaS automatically scales and supplies the demand for infrastructure components dependent on varying application requirements. PaaS solutions supply an API, which has a set of tasks for platform management and for development. The Google App Engine is a popular PaaS provider, while Amazon Web Services also supplies some PaaS solutions (Badger et al., 2014).

The **Software as a Service (SaaS)** model comprises software which is provided by a third-party developer, is available on demand, generally through the Internet, and is remotely configurable. Examples of the SaaS model are Salesforce CRM and Google Docs (Dupre, 2009).

2.1.3 Cloud Deployment Models

Over recent times, the majority of cloud users have accepted the following four cloud deployment models:

- **Public Clouds:** Provided for the public under a utility-based pay-per-use consumption model, public clouds may be owned, managed and operated by a business, academic institution, or government organisation (NIST, 2011). Any user that is aware of the service location can access the infrastructure. Examples include Microsoft's Azure Service Platform and Amazon's AWS (Badger et al., 2014).
- **Private Clouds:** The cloud infrastructure is provided for exclusive use by a single organisation comprising multiple consumers (e.g., business units). A Private Cloud is built to be operated and managed by a particular organisation which only uses it internally to support its business operations. Public, private, and government organisations across the world are adopting this model to exploit the benefits of the cloud, namely flexibility, cost reduction, and agility (Avram, 2014). Examples include Amazon Virtual Private Cloud and eBay.
- **Community Clouds:** The goal of this deployment model is to provide free or low-cost services to organisations with common interests (Chandra and Weissman, 2009).
- **Hybrid Clouds:** Merging two or more clouds may accomplish maximum benefits while simultaneously reducing cost. Thus, an internal cloud can be employed within an enterprise to protect confidential data, while a community or public cloud can be used to attain cost reduction (Gong et al., 2010). While few hybrid clouds are actually in use, initiatives from companies such as IBM and Juniper do exist (Schubert et al., 2010).

2.1.4 Fundamental Elements of Cloud Computing for Government Organisations

Wyld et al. (2009) concluded that the important proposition of cloud computing has many features for governments, due to the dynamic nature of IT demands and the exciting economic situations faced by various governments. These elements are illustrated in Figure 2-2.

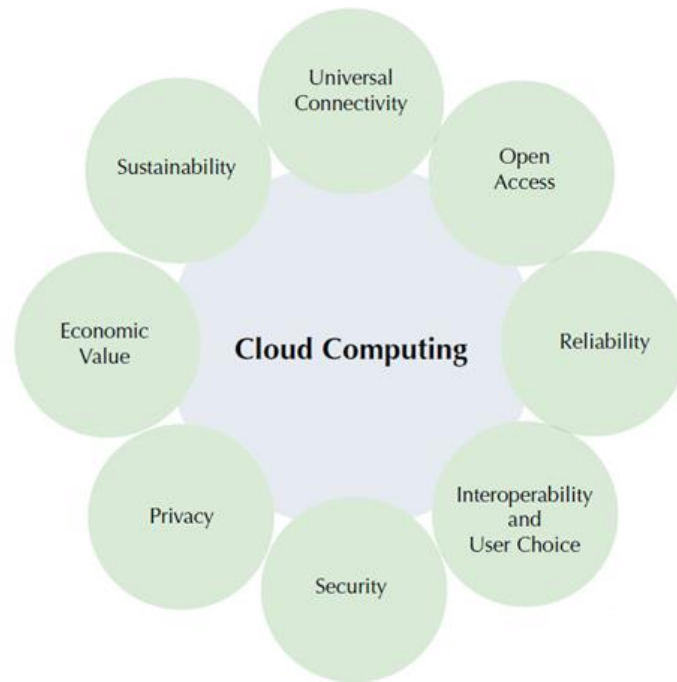


Figure 2-2: Fundamental Elements of Cloud Computing for Government (Wyld and Robert, 2009)

These eight elements are dynamic in qualifying the cloud computing government organisations, and it is important for any organisations to consider it:

- **Universal Connectivity:** a user's requirement has nearly global contact with the Internet.
- **Open Access:** a user's requirement has fair, non-preferential contact with the Internet.
- **Reliability:** provides IT system and clarification architects, developers, and engineers with the knowledge needed to consider the impact of virtualisation and cloud computing on service reliability and availability.
- **Interoperability and User Choice:** users have the ability to shift through the cloud platform.
- **Security:** users' data must be safe.

- **Privacy:** users' privileges to their data must be clearly defined and secured.
- **Economic value:** the cloud option brings about tangible savings and benefits.
- **Sustainability:** the cloud requirement increases energy efficiency, and decreases environmental influence.

2.1.5 Advantages and Disadvantages of Using Cloud Computing

The following section describes the advantages and disadvantages of using cloud computing in government organisations, and the features of cloud services throughout the IT provision paradigm. Any analysis focusing on the use of cloud computing by governments, companies, education institutes, or even private sectors, must address the advantages and disadvantages of the service before embracing it (Miller, 2009). Such organisations will enjoy the following advantages and disadvantages, as described in Table 2-1:

Table 2-1: Advantages and Disadvantages of Cloud Computing (Miller, 2009)

Advantages	Disadvantages
Cost saving	Vender lock-in.
Quick deployment	Limited control.
Less investment in infrastructure	Security issues
Hardware and software maintenance is very low	Requires Internet for access
Unlimited storage capacity	Features might be limited
Lower IT operating costs	Stored data might not be secure
Increased computing power	Not being able to monitor or control data movement
Instant software update	Limited knowledge and control

2.1.6 Cloud Computing Adoption in Government Organisations

Governments across the world are starting to make a dynamic shift to cloud computing to increase efficiency (Badger et al., 2011). In this study, cloud adoption is referred to as the process of accepting and embracing cloud services within the IT infrastructure in government organisations. It must also be stated that cloud adoption is considered by organisations to be an IT solution that can be used to reduce cost and recognise the scalability of data capabilities. Moreover, cloud adoption may satisfy an agency's IT needs to varying degrees, depending on the depth of adoption. It is clear that today's

ever-growing computing environment is shifting towards cloud services. According to some cloud adoption studies, the main appeals of using the cloud are falling IT costs as a result of collective productivity, availability, reliability, and flexibility, as well as reduced response times (Alharthi et al., 2015).

Cloud adoption has several benefits for organisations, government institutions, companies and small or large enterprises. One of the most notable benefits of cloud adoption is saving money; these lower costs result from the fact that cloud computing adoption provides organisations with an outsourcing model which allows them to access resources and pay as they use these services according to a measured model. Besides cost benefits, cloud adoption offers certain additional advantages for public services. The leading advantages of using cloud computing for governments and public sectors include: Pay for only what they use, Scalability, Availability, Low maintenance and Easy implementation (Winkler, 2011).

2.1.7 The Status of Cloud Adoption in Developed and Developing Countries

In 2011, the UK government formulated cloud strategy plans to endorse the adoption of the cloud paradigm and thus enhance its IT services in terms of cost efficiency, interoperability, and flexibility (Elena and Johnson, 2015a). The British government employed a representative and rational technique in order to implement the compulsory measures needed to start the process of integrating cloud computing processes into its operations. In light of this, the UK government is considered one of very few developed countries to have initiated the planning of national strategies and the use of private and community deployment models (Ko et al., 2013).

Subsequently, with other governments around the world now starting to understand the benefits and cost-saving potential of cloud computing, the effective technology offered by this service is being steadily incorporated into government processes. The US government is one of the largest user when it comes to embracing cloud services in its government organisations. The cloud initiative was established to adopt cloud

computing platforms and services in order to consolidate and promote public electronic services (Ko et al., 2013).

Moreover, while the Chinese government is considered one of the world's economic heavyweights, it has yet to formulate a national cloud computing strategy. On the other hand, the Chinese government has started to recognise the benefits of cloud computing and has subsequently begun the process of cloud implementation with IBM to develop a regional cloud services infrastructure (Alsanea and Barth, 2014). Added to this, in Australia, the government has started to transfer the majority of its systems' data to the cloud (Wyld and Robert Maurin, 2009).

In developing countries, such as Thailand, the governments are planning to adopt the cloud in order to add software as a service initiative. Moreover, the Thai government previously developed a national platform for cloud-based and email services; this particular government holds the view that such consolidation will increase service assistance for government organisations, while concurrently cutting down on its general IT costs significantly (Wyld, 2010).

2.1.8 Cloud Computing Adoption Status in Saudi Government Organisations

In terms of expenditure on IT services, the KSA remains one of the top spenders in the Middle East and Africa region. Much of this progression is determined by spending on public cloud services, such as infrastructure as a service and software as a service (Alharbi et al., 2015). The Saudi government has set itself the target of making the country one of the world's top ten destinations in terms of investment competitiveness.

Moreover, the Saudi government's objective is to encourage public services, achieve success for society, and increase the production of all sectors (Alnatheer and Nelson, 2009). The KSA has a strong desire for the public cloud to be managed in the country itself, rather than being based in a foreign country; however, at present, this is a difficult task due to the lack of infrastructure, connectivity and services (Alkhater et al., 2014).

Government cloud computing initiatives provide government organisations with ready-to-use services which are highly efficient, reliable and secure with respect to

infrastructure, platform, and software (Alshahrani and Alsadiq, 2014). With cloud computing now becoming the new IT provision paradigm, it is also expected to set future trends in the domain of information and communication technology. In the KSA, the government has acknowledged the importance of cloud-based services and has thus started to lay out plans to establish government cloud services, as well as other cutting-edge technologies, including smart cities and IoTs sensing.

Moreover, the KSA has begun investing and applying the cloud to the ICT infrastructure of government organisations, such as the ministry of interior and higher education institutions; this is being done in order to improve these organisations' IT services and standardise their means of communication (Alharthi et al., 2016).

The use of cloud computing in the KSA is still in the early stages. On the other hand, however, increasing attention to cloud adoption has been noticed in the information technology organisations, and particularly all government organisations in general in the KSA (Alfifi et al., 2015).

2.2 Fundamentals of Cloud Computing Security

Security is considered one of the most serious aspects of everyday computing, and this is no different for cloud computing when compared to the sensitivity and significance of data stored in the cloud services (Jasti et al., 2010). In order to shed some light on the security underlying cloud computing, it is certainly worth referring to the definition of cloud security itself. According to the Cloud Security Alliance (CSA), cloud security comprises a *“set of control-based technologies and policies designed to follow regulatory compliance rules and protect information, data applications and infrastructure associated with cloud computing use”*. In addition to the previous definition, cloud computing security can be defined as a broad set of rules, technologies, and controls organised to protect data, applications, and the supplementary infrastructure of cloud computing. Cloud Security Alliance et al. (2013) indicates that cloud security controls are not different from IT environment security. On the other hand, while cloud computing

works with service models such as the operational models and the technologies used to assist cloud services, cloud computing could possibly pose several risks to an organisation when compared with normal IT solutions. Any organisation willing to adopt cloud computing requires professionals with security skills; this is due to the fact that security management is one of the most important elements of the cloud (KPMG, 2011). The full utilisation of cloud-based services depends on the security of information related to the organisation and its employees, which is the biggest concern (Chang and Ramachandran, 2015). Moreover, security concerns are considered the primary obstacles standing in the way of a wide adoption of the cloud in government organisations (Chang and Ramachandran, 2015).

Security is defined in relation to three concepts: confidentiality, availability, and integrity (Cherdantseva and Hilton, 2013). Table 2-2 presents the concepts of CIA. These concepts are crucial to the topic of security analysis as a whole, especially when accessing a user's history of encrypted data across the Internet (Cherdantseva and Hilton, 2013).

Table 2-2: Security Concepts (CIA) (Cherdantseva and Hilton, 2013).

Security Concepts	Definition
Confidentiality	A system should ensure that only authorised users can access information.
Integrity	A system should ensure completeness, accuracy, and absence of unauthorised modifications in all its components.
Availability	A system should ensure that all of its components are available and operational when authorised users require them.

When it comes to the adoption of cloud computing, security is one of the main concerns; this is due to the fact that comprehensive security can persuade organisations to adopt the service, while it can also encourage them to pause agreements to use or accept said service (Paquette et al., 2010). Moreover, each provider engaged in cloud computing services will have to contend with security concerns expressed by the others in relation to trust, service risks or legal problems (Cherdantseva and Hilton, 2013). A major concern regarding the adoption of the cloud for data handling is security and privacy. It is very important for the cloud service provider to guarantee the data's integrity, privacy, and protection. For this purpose, several service providers are now using different

policies and mechanisms that depend upon the nature, type, and size of data (Yahya et al., 2014). One of the key questions which arises while using the cloud for data storage is whether to use a third-party cloud service or create an internal organisational cloud. The data are, on occasions, too sensitive to be stored on a public cloud; examples of such data include national security data or highly confidential future product details etc. This type of data can be extremely sensitive, and the consequences of exposing it on a public cloud can be serious. In such cases, it is highly recommended to store data using an internal organisational cloud. This approach can help in securing data by imposing data usage policy on premises. However, this still fails to ensure full data security and privacy, since many organisations are not qualified enough to add all layers of protection to the sensitive data (Albugmi, 2016).

2.2.1 Cloud Computing Security Benefits

Most considerably, the cloud computing environment suffers with the understanding of perimeter security. Perimeter security comprises a set of physical and programmatic security policies that supply levels of protection on a fictitious borderline against the remote malicious actions (Heiser and Nicolett, 2008). Organisations around the world are facing the problem of protecting individuals' private information. In reference to this point, it is not clear whether adopting cloud computing will provide increased security efficiency for enhancing information protection. Despite this uncertainty, cloud services do offer security benefits, including the ability to keep applications securely anywhere in the cloud computing infrastructures, whether inside the network or on the Internet (Che et al., 2011).

Security is a priority concern for many government organisations. In comparison with traditional environments, organisations will place more emphasis on obtaining selections; this is the basis of their ethos, as it stands for confidentiality, integrity, and resilience, as well as the security offered by a provider. Most cloud providers have the commercial resources to reproduce content in multiple locations by default. Moreover,

the greatest security benefit offered by cloud computing is the safe and secure transmission of data (Che et al., 2011).

According to ENISA (European Network and Information Security Agency), the top security benefits of cloud computing include (Dupre, 2009):

- Security and the benefits of scale
- Security as a market differentiator
- Timelier, security effective and efficient updates and defaults
- Secure, rapid, and smart scaling of resources
- Standardised interfaces for managing security services
- Security audit and evidence gathering
- Security audit and SLA force better risk management
- Security benefits of resource concentration

2.2.2 Cloud Computing Security Risks

Despite all the previously-mentioned benefits of cloud adoption, there are certain risks that hinder governments' attempts to adopt cloud computing. Security risks represent the major obstacle standing in the way of successful cloud adoption; this is because information always comes with security and risk problems. According to the CSA organisation, the security of cloud computing is the biggest concern for organisations (von Solms and van Niekerk, 2013). The security risks linked with each cloud delivery model are different and are dependent on a varied collection of factors, including the sensitivity of information possession, cloud architectures, and the complexity of security control in a specific cloud environment (Sen, 2013). The majority of these risks are described in the following taxonomy:

- **Time Risk:** considered one of the greatest risks affecting the decision to leverage cloud computing services, time risks include time to recognise, the situations and environments in which cloud computing is used, compliance with data protection regulations, time to explore and implement a new solution, and time

to know and comply with the service level agreement terms (Elena and Johnson, 2015a).

- **Performance Risk:** consumers always want to have confidence in and transparency about the performance of the cloud system and how it has achieved such success. This is because the cloud offers a dynamic service, which meets performance needs and offers low operating costs (Radack, 2012).
- **Social or Reputational Risk:** this is considered one of the most technical risks, as it revolves around meeting customer demands. When using cloud services, social risk is very high because of the potential damage and loss of standing that may result from the leakage of particular data and the unavailability of the cloud services (Chang et al., 2013).
- **Financial Risk:** this category includes prospective costs from reputational aspects caused by security data breaches. Financial risk is an important security risk related to cloud services, because these cloud services need to achieve qualifications and demonstrate high levels of performance before spending money on new IT systems (Gentzoglanis, 2011).
- **Security Risks:** the most recent cloud adoption studies showed that security is the most important factor to consider when adopting cloud computing services in government organisations. It is typically ranked as the top cloud computing adoption concern (Bannerman, 2010; Elena and Johnson, 2015b).

With regard to the security risks, there are several challenges associated with the adoption of cloud computing which must be addressed (Sen, 2013). Prior to the adoption of cloud services, every organisation should be ready for, and aware of, the multiple dimensions of security risks and benefits (Weng, 2014).

A number of top security risks associated with cloud computing have been identified by organisations, such as: the European Network and Information Security Agency (ENISA), the Centre for the Protection of National Infrastructure (CPNI) and the Organisation of the Open Web Application Security Project (OWASP). These risks include: *Insecure Interfaces, shared technology, Account or Service Hijacking, Malicious Insiders, Failure*

to Comply with Regulations, Data Ownership, Service and Data Integration, and Data Leakage.

The characteristics of cloud computing mean that many users are concerned about the potential security risks, because of the shared resources in the cloud. Implementing cloud computing in any organisation means that all of the data are shifted to the cloud, which increases the risk of threats from attackers (Sen, 2013). As such, before implementing cloud computing, it is vital to research potential security risks in the organisation. The top cloud security risks, as stated by organisation industries (ENISA, CSA, CPNI, and OWASP) are in Table 2-3:

Table 2-3: Top Cloud Security Risks by Organisation Industries.

European Network and Information Security Agency (ENISA)	Cloud Security Alliance (CSA)	Centre for the Protection of National Infrastructure (CPNI)	Organisation of the Open Web Application Security Project (OWASP)
Loss of government, Lock-in, Isolation failure, Compliance risks, Management interface compromise, Data protection, Insecure or incomplete data deletion, Malicious insider, Customer's security expectations and Availability chain.	Data breaches, Data loss, Account hijacking, Insecure APIs, Denial of service, Malicious insiders, Abuse of cloud services, Insufficient due diligence, and Shared technology issues.	Insider user threats, External attacker threats, Data leakage, Data segregation, User access, Data quality, Change management, Denial of service threat, Physical disruption, and Exploiting weak recovery procedures.	Accountability and data ownership, User identity federation, Regulatory compliance, User privacy and secondary usage of data, Service and data integration, Multi-tenancy and physical security, Incidence, Infrastructure security and non-production.

Having identified the above-mentioned top security risks, it is now important to present a list of the top cloud security risk factors as stated by organisation industries. This makes it possible to identify the factors that are agreed upon or covered by most of the organisation industries by removing the duplicates of these factors, as in the summary section illustrated in Table 2-4.

Table 2-4: Summary of the Top Security Risk Factors Studied.

Top Security Risks	ENISA (Catteddu and Hogben, 2009)	CSA (Cloud Security Alliance, 2013)	OWASP (Council, 2012)	CPNI (Deloitte, 2010)	Covered by three or more of the Organisation Industries
Insecure and application programming interfaces (APIs) ¹	√	√	√	√	√
Abuse and nefarious use of cloud computing		√		√	
Account or Service Hijacking ¹	√	√	√		√
Malicious insiders ¹	√	√	√	√	√
Composite service's risk		√		√	
Data ownership (governance) and accountability ¹	√	√	√		√
Service and data integration/protection ¹	√	√	√		√
Lack of update/patching		√			
Data leakage ¹	√	√	√		√
Multi-tenancy and physical security	√	√			
Denial of service threat			√	√	
Unknown risk profile		√	√		
User identity federation		√	√		
Shared technology (multi-tenancy/isolation) risk ¹	√	√	√	√	√
Isolation failure			√	√	
Insufficient due diligence	√	√			
Non-production environment exposure	√				
Lock-in	√	√			
Failure to comply with regulations ¹	√	√		√	√

¹ Common Security Risks Related to Cloud Computing Services.

2.3 Security Social Factors and Saudi Government Organisations

Security, whether social or cultural, often has a significant influence when it comes to which organisations attempt to implement technology transfer. Of key importance are a society's own concepts, principles, and beliefs about how technology will be applied in developing countries. Social security factors are extremely important and should be taken into consideration when government organisations adopt cloud computing. In this field, many studies have found that social and culture security have a huge influence on the use of online services and the adoption of new technology (Walsham et al., 1988; Weerakkody, 2008, Straub et al., 2003).

For instance, in governments, security social influences can slow down the diffusion of an innovation by enforcing laws and regulations; in contrast, they can also speed up the diffusion of an innovation by offering subsidies and incentives (Straub et al., 2003). In social sciences, social influence is defined as change in a being's beliefs, feelings, attitudes, or behaviours resulting from interaction with another group. In the context of cloud security adoption, the security social factors are related to the perceived benefits and risks of cloud services adoption and the intention to share, communicate, and create real-world relationships with the cloud providers and tenants (Elena and Johnson, 2015a).

Arab culture and history constitute a complex system comprised of conflicting forces; this system looks to exert a stronger social influence on the Arab society in comparison to Western culture; this is achieved by expanding and enforcing a specific social model and common beliefs (Hill and Loch, 1998).

From the cloud adoption perspective, this research will focus on the security social factors that influence the adoption of cloud computing in Saudi government organisations. These factors are linked to the security aspect and are associated with Saudi organisations' behaviour and attitudes towards the adoption of cloud computing. These social factors also pertain to issues of trust, security culture, and privacy.

- **Trust**

Trust is a big concern for government organisations looking to adopt cloud computing, and is the sole reason why there exists a lack transparency and control over data in cloud computing (Khan and Malluhi, 2010). Difficulties related to trust in cloud computing consist of trusting the service itself and trusting the supplier of internal procedures to supply a reliable level of confidentiality, integrity and authentication when it comes to the services and the stored data.

Moreover, the issue lies not only with trusting the cloud provider, but also the possibility that the technology itself may be untrustworthy and incapable of offering a good service that meets the organisations' due diligence without disruption or loss of data (Khan and Malluhi, 2010).

- **Security Culture**

Security culture can support and enhance the performance of most organisations; this means that information security can constitute a normal part of all employees' daily activities. Security culture helps organisations to execute information security policies and covers various factors, e.g., social, cultural, and ethical. All of these help to develop the security-relevant behaviour of an organisation's structures, and such behaviour remains a subculture of organisational culture (Alnatheer and Nelson, 2009).

- **Privacy**

Privacy is related to the confidentiality of data and the fact that data should only be accessed by certified users. Privacy is considered a major concern for any organisation willing to adopt cloud computing; this is because it is almost impossible to have complete control over information that is stored on cloud-based servers (Sen, 2013).

2.4 Review and Discussion of Related Work

In this section, existing related work and approaches to security in cloud computing will be discussed and summarised. When deciding whether to use cloud-based systems, the majority of Saudi government organisations place primary emphasis on their own custom needs (Alharthi et al., 2015). As with any innovation, cloud computing usage and

user acceptance must be understood, as users are key players in promoting innovation. When it comes to adopting such technology, these organisations are hesitant to embrace it, due to the security factors. Security has been identified as the main challenge which organisations must consider before adopting the cloud and is typically ranked as the top concern in cloud computing adoption (Bannerman, 2010).

Zhou et al. (2010) analysed the barriers which users may encounter when deciding whether or not to adopt cloud computing systems. However, they encountered a lack of evidence related to the security risks and benefits tailored to the user side. Paquette et al. (2010) examined the current level of cloud adoption, its use by governments, and the risks, both tangible and intangible, associated with its use. With this said, however, the authors did not address security risks and benefits.

Che et al. (2011) highlighted the security risks of cloud computing, but only investigated security strategies. Moreover, Sun et al. (2011) placed emphasis on the major security, privacy and trust issues in current cloud computing environments, and guided the users to identify the tangible and intangible threats related to them; they failed, however, to provide an empirical investigation.

Along similar lines, both Alkhater et al. (2014) and Alsanea and Barth (2014) investigated the managerial, technological and environmental factors influencing cloud adoption in the KSA. However, they did not address the security risks or provide an in-depth analysis of said risks.

Furthermore, Subashini and Kavitha (2011) suggested a few security elements related to cloud computing and its vital role as an integral part of the SaaS development and deployment process. However, the researchers failed to address the security risks, benefits and social related factors.

Klems et al. (2009) suggested a framework with which to evaluate the cost risks of utilising IT infrastructure based the cloud. They associated it with predictable IT methods, like a grid computing service or the cost of setting up in-house IT infrastructure. They considered the costs in their framework as indirect and direct costs.

IT infrastructure resources are a sample of direct costs, while an indirect cost is suffered due to failure to come across business aims and nominate training courses with the new technology. However, their work was in the development stage, and consequently the outcomes are not provided. In addition, their study did not consider the aspect of security as part of the cloud implementation framework.

Gangwar et al. (2015) combined the TOE framework and the TAM model to identify organisational, technological and environmental factors that have a direct influence on cloud computing adoption at the organisation level. However, this study did not include any factors related to security.

Alharbi (2017) proposed an extended UTAUT model to investigate the factors that influence users' intention to employ cloud services. Although this study included trust as a factor that influences cloud adoption, other security factors were omitted. Moreover, this study did not focus on government organisations.

Alturki et al. (2017) briefly explained the framework and actions that can help the community, customers and small vendors to use cloud services. He also identified challenges and applications in private and public organisations in Saudi Arabia. However, this study did not provide in-depth analysis, nor did it identify the security factors.

After reviewing these previous studies, it is clear, to the best knowledge of the researcher, that no formal studies have examined the security factors that affect cloud adoption in Saudi government organisations. This is the research gap that the present research intends to fill. With all of this in mind, this study aims to bridge the gap in the literature by conducting an in-depth analysis and investigation of the security risks, social aspects, and benefits factors that affect the adoption of cloud computing in KSA government organisations. The investigation begins with a review of the literature, the purpose of which is to paint a comprehensive picture of cloud adoption security-related factors in the global context. Following this, the synthesised factors based on the literature survey are confirmed by conducting interviews and surveys with security

experts and specialists working in government organisations in Saudi Arabia. The summaries and reviews of the work related to this research are presented in

Table 2-5:

Table 2-5: Summary of Review and Discussion of the Related Work

Study	Type of Contribution	Security	Saudi Context	Evaluation
Zhou et al. (2010)	Identified factors	NO	NO	This study explored the security and privacy concerns resulting from a certain degree of cloud computing use.
Paquette et al. (2010)	Identified factors	NO	NO	This study identified different issues which arise when government organisations utilise cloud computing.
Che et al. (2011)	Identified factors	Yes	NO	This study proposed strategies and security models that can be utilised to address existing security issues.
Sun et al. (2011)	Identified factors	NO	NO	The security risk classification was not considered.
Alsanea and Barth (2014)	TOE (Technology, Organization, Environment) Model	NO	Yes	This study only examined a range of factors affecting cloud computing adoption by governments in general. It failed to consider the security risks.
Subashini and Kavitha (2011)	Identified factors	NO	NO	This study conducted an investigation into cloud computing security issues linked to the cloud computing service delivery model (SPI model). The sole focus was on the SaaS model, and so the risks were not addressed.
Klems et al. (2009)	Identified factors	NO	NO	This study offered a framework to evaluate the costs of using IT infrastructure in the cloud, but did not reflect the feature of security.
Alkhater et al. (2014)	Identified factors by using models	NO	Yes	This study investigated factors that impact an organisation's decision. The security risks and benefits classifications were not considered.
Gangwar et al. (2015)	Combined TOE framework and TAM model	NO	NO	This study combined the TOE framework and the TAM model to identify organisational, technological and environmental factors that have a direct influence on cloud computing adoption. It failed to consider the security factors.

Alharbi (2017)	Proposed extended UTAUT model	NO	Yes	This study revealed that performance expectancy, trust and facilitating conditions influence users' intention to use cloud computing. This study did not focus on government organisations, while other security factors were also missing.
Alturki et al. (2017)	Developed a framework	NO	Yes	This study identified challenges and applications in private and public organisations in Saudi Arabia. However, this study did not provide in-depth analysis, nor did it identify the security factors.

2.5 Summary

This chapter began by examining the contextual of cloud computing, in order to recognise its perceptions and important characteristics. Cloud computing offering online resources based on customers' needs. Moreover, it agrees users to pay only for the service that they use. This chapter also illustrated the key advantages that drive government organisations to adopt cloud services, e.g., cost reduction and flexibility. Furthermore, this chapter demonstrated the benefits of cloud adoption and discussed some of the important security social factors that influence the adoption of cloud computing services in the KSA. This was followed by a summary of the status of cloud adoption in different developed and developing countries, with reference to the KSA context.

Moreover, a review of previous studies in this field was put forth in order to clarify the state of cloud computing adoption in developed and developing countries. Particular emphasis was placed on the security factors that hinder the attempts of governments, and even private sector organisations, to adopt the cloud. In summary, this chapter examined the most important CIA security aspects and clarified some of the top security risk factors that affect organisations' adoption of the cloud. The chapter then explored the existing cloud computing literature and provided an overview of the applications of this technology in several government organisations. Finally, discussion focused on the security factors that play an important role in the adoption of cloud computing. The cloud security framework will be proposed in the next chapter.

Chapter 3: Cloud Security Framework for Saudi Government Organisations

Before embarking on this chapter, it is important to note that the previous chapter examined the cloud security benefits, security social factors, and security risk factors that can affect the cloud adoption decision-making process. Following on from this, the present chapter proposes a cloud security framework which can be used to investigate the security factors that influence cloud adoption by KSA government organisations.

3.1 The Framework Development and Confirmation Process

As discussed in the previous chapter, and after reviewing these previous studies, it is clear, to the best knowledge of the researcher, that no formal studies have examined the security factors that affect cloud adoption in Saudi government organisations. This is the research gap that the present research intends to fill. With all of this in mind, this study aims to bridge the gap in the literature by conducting an in-depth analysis and investigation of the security risks, social aspects, and benefits factors that affect the adoption of cloud computing in KSA government organisations.

The investigation begins with a review of the literature, the purpose of which is to paint a comprehensive picture of cloud adoption security-related factors in the global context. Following this, the synthesised factors based on the literature survey are confirmed by conducting interviews and surveys with security experts and specialists working in government organisations in Saudi Arabia.

The purpose of the framework proposed in this research is to investigate the security factors that influence the adoption of cloud computing by Saudi government organisations. The development of this framework consists of two phases, as shown in Figure 3-1.

- **Phase 1**

The first phase covered identifying and reviewing published studies, specifically those concerning security frameworks, which have explored cloud computing adoption. It should be noted that the classification of factors, namely security risks, social security, and security benefits, is based on the literature. The first phase consists of four stages.

Stage 1: this stage began with the listing of security risks that have been highlighted by previous literature on cloud security frameworks and industrial security standards, such as ENISA, CSA, CPNI, and OWASP. The aim of this stage was to survey widely-recognised security risks factors in order to identify which of them may, and may not, influence cloud adoption. This included identifying and reviewing published studies related specifically to cloud security frameworks used to explore cloud computing adoption.

Stage 2: during this stage, emphasis was placed on reviewing the unique security advantages and services of cloud computing. The cloud security features were grouped based on different industry standards and cloud security-related studies.

Stage 3: this stage involved a literature review which was carried out in order to identify the security social factors that can hinder or facilitate Saudi government organisations' decisions regarding whether or not to adopt the cloud.

Stage 4: this stage was developed to filter and remove duplicated factors, as well as to synthesise and refactor those factors identified in the previous stages. The synthesising procedures used to reach a decision in this stage can be broken down as follows:

- The factors were filtered to identify overlapping and duplicated factors.
- The filtered factors were grouped under their main category.
- The factors were adopted in the framework if they were mentioned in three or more industrial standards.

- **Phase 2**

During this phase, a confirmatory study was conducted in order to paint a clearer picture of the cloud security adoption framework proposed in the previous phase. A triangulation method was applied. This was achieved by interviewing IT and security experts, and surveying security practitioners in different Saudi government organisations. A detailed explanation of the research methods employed in this study is provided in Chapter 4.

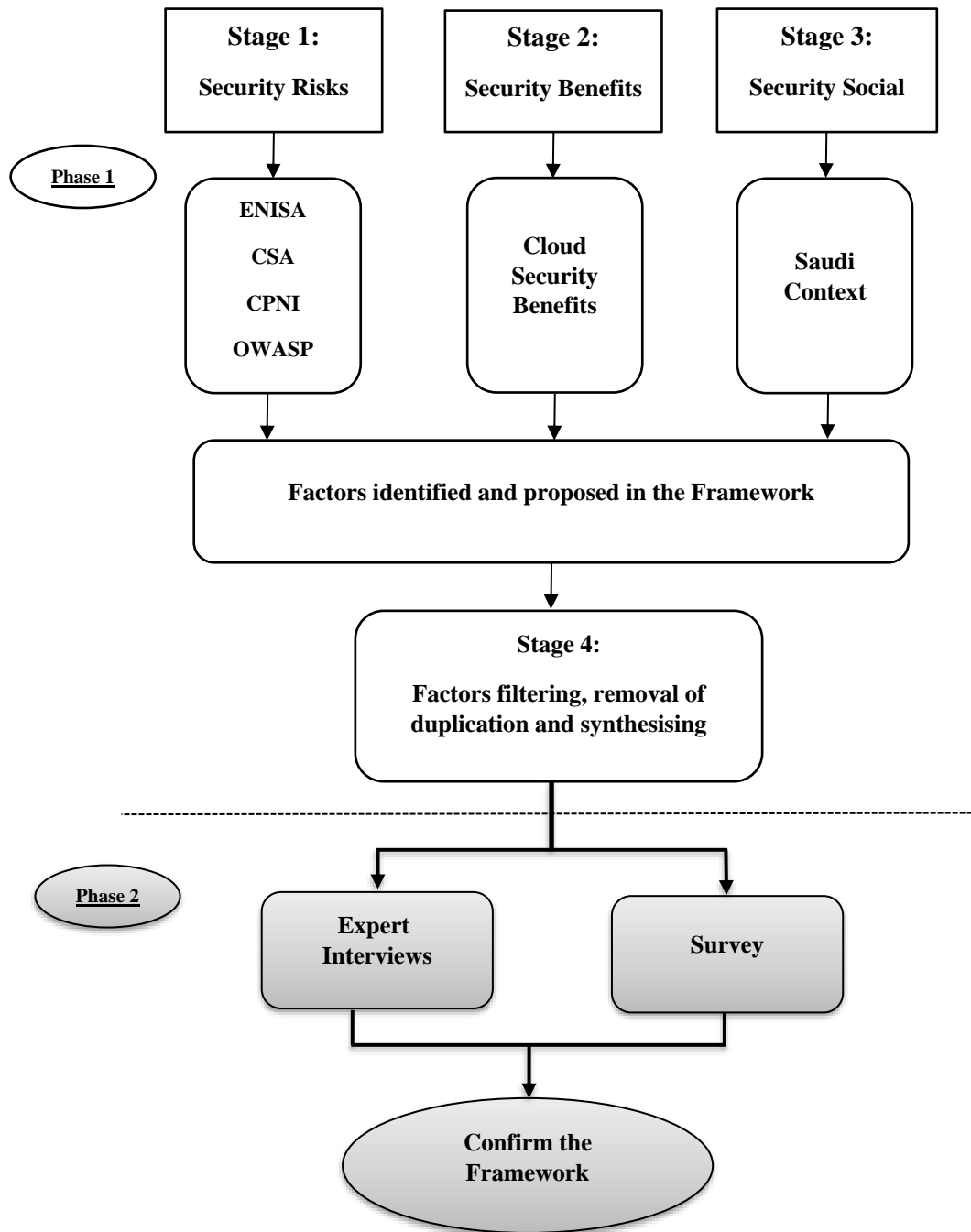


Figure 3-1: Process for Developing Proposed Framework

3.2 The Proposed Cloud Security Framework

The framework consists of three categories: cloud security risks, security social factors, and cloud security benefits, as shown in Figure 3-2. These categories are described in the following figure:

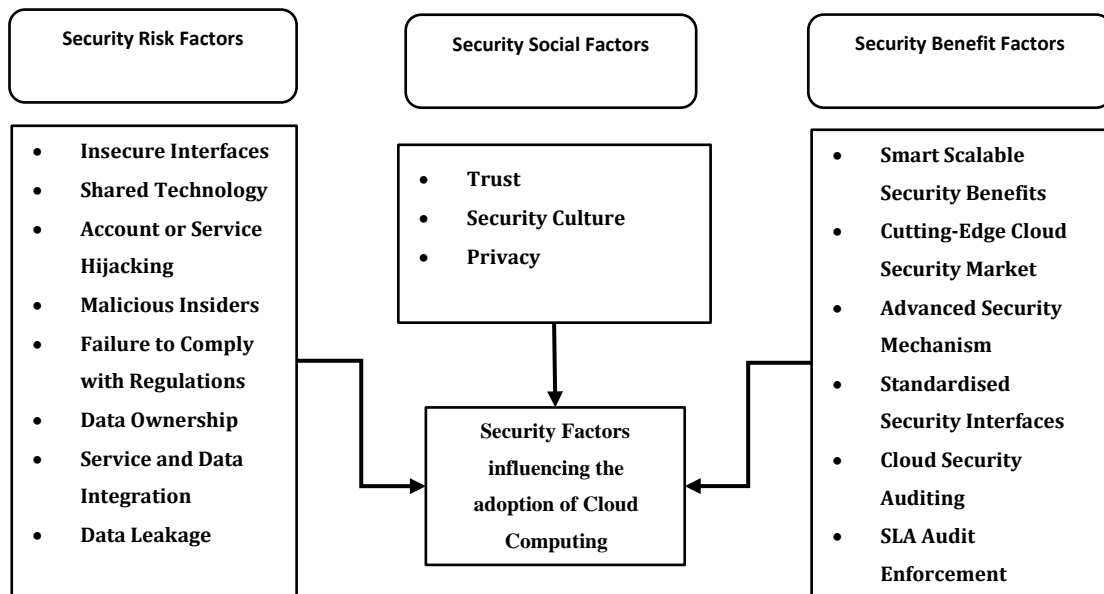


Figure 3-2: Proposed Framework, Including Security Factors that Influence the Adoption of Cloud Computing in Saudi Government Organisations

3.2.1 Security Risk Factors

The following cloud security risk factors are related to the set of cloud security risks identified based on the literature reviewed in Chapter 2:

- **Insecure Interfaces and Application Programming Interfaces (APIs):** consumers manage and react to cloud services by using interfaces and APIs. Providers must guarantee that security measures are implemented and taken into consideration when service models are being formulated. However, the users should understand, and be aware of, security risks when using these services (Cloud Security Alliance, 2013).

- **Shared Technology Risk:** the IaaS is constructed based on a shared infrastructure that is frequently thought to not accommodate a multi-tenant architecture, such as CPU caches and GPUs (Wei et al., 2009).
- **Account or Service Hijacking:** according to the Cloud Security Alliance, service traffic hijacking is recognised as the highest cloud computing security risk. It is regularly associated with stolen identifications and is considered to be one of two influential factors that affect authentication techniques (Cloud Security Alliance, 2013).
- **Malicious Insiders:** these pose a risk to organisations, because a malicious insider could be a company's current or previous operation provider. On the other hand, a malicious insider could have authorised access to an organisation's system or to potentially sensitive data. However, it is important for government organisations to understand what providers are doing to identify and tackle the malicious insider risk (Jasti et al., 2010).
- **Failure to Comply with Regulations:** compliance with regulations is one of the most important risk factors and one which the government should be aware of before adopting the cloud, even when it is held through a service provider (Brodkin, 2008). Complying with regulations is an influential factor which can facilitate the secure transference of information to the cloud. This risk derives from the fact that there are no governmental regulations or directions which can support a business in the event of a data breach. The lack of IT standards is a big problem, which could potentially hinder cloud computing adoption decisions (Mather et al., 2009).
- **Data Ownership (Governance) and Accountability:** this factor is a critical security risk which government organisations must consider carefully and quantify, since these organisations must logically and actually defend the data they own (Babu et al., 2010).
- **Service and Data Integration/Protection:** all organisations must be sure that their own data is protected while it is moving between the end user and the cloud data centre. However, the Service and Data Integration is greater for

organisations which use a cloud computing model, because unsecured data is more liable to be intercepted during transmission (Dupre, 2009).

- **Data Leakage:** according to CPNI, data leakage relates to the weakness of security access rights, which means that more domains are penetrated. This factor also pertains to the weakness of the physical transport system used for cloud data and backups (Deloitte, 2010).

3.2.2 Security Social Factors

Security social factors are related to organisations' security behavior and attitudes toward the use of cloud computing in terms of security from the cloud adoption perspective. These factors have been highlighted by research studies in the literature, and are discussed below:

- **Trust:** has an indirect influence on knowledge sharing, which leads to increased sharing through technology in cloud computing. More specifically, trust has an effect on knowledge sharing when staff believe that other team members are honest, fair and follow the key principles (Khan and Malluhi, 2010). Security plays a central role in preventing service failures and cultivating trust in cloud computing. In particular, cloud service providers must secure the virtual environment, as this enables them to run services for multiple clients and offer separate services for different clients (Khan and Malluhi, 2010).
- **Security Culture:** can support organisations and increase their effectiveness, thus meaning that information security can become a normal part of all employees' daily activities. Security culture also facilitates the execution of information security policies within organisations. Security culture comprises social, cultural, and ethical elements which make it possible to develop the security pertinent behaviour of the organisational organs and ensure that such behaviour remains a subculture of organisational culture (Isaca, 2009).
- **Privacy:** relates to the confidentiality of data and the notion that data can only be accessed by licenced users. Privacy is considered a major concern for any

organisation willing to adopt cloud computing; this is because it is almost impossible to have complete control over information that is stored on cloud-based servers (Khan and Malluhi, 2010).

3.2.3 Security Benefits Factors

This category comprises the cloud computing security features that affect cloud adoption decision making in organisations. The features examined were highlighted by organisation industries and research studies in the literature. The cloud security features are further elaborated on below:

- **Smart Scalable Security Benefits:** this factor is defined as the ability to extend security features to multiple locations, edges networks, timelessness of response, and threat management. The list of cloud resources that can be rapidly scaled on demand already includes: storage, CPU time, memory, web service requests, virtual machine instances, and level of granular control over resource consumption, the latter of which is increasing as technologies mature (Catteddu and Hogben, 2009).
- **Cutting-Edge Cloud Security Marketing:** cloud providers such as Amazon and Google are considered to be the largest hardware and software providers in the world. Therefore, cloud customers can benefit from up-to-date, high-standard security techniques which allow them to secure their assets (Catteddu and Hogben, 2009).
- **Advanced Security Mechanism:** a cloud provider can provide the customer with centralised security in the form of service patches and updates. This is more efficient than traditional organisation security capability (Kanday, 2012).
- **Standardised Security Interfaces:** security management interfaces can make it easier for consumers to change from one provider to another in a short period with saving cost (Cloud Security Alliance, 2013).
- **Cloud Security Auditing:** auditing in the cloud can be better organised, and people can pay as they go for auditing and gathering of audit log requirements (Catteddu and Hogben, 2009).

- **SLA Audit Enforcement:** cloud customers can benefit from a set of audit management requirements and the provider should comply with those audit demands stated in the service level agreements (SLA) (Ahn et al., 2014).
- **Resource Concentration:** costumers can benefit from access control, comprehensive security policy, patch and data management, and maintenance processes; in this way, they can harness a pool of security resources (Che et al., 2011).

3.3 Summary

This chapter summarised the development of a framework and proposed security factors that affect cloud adoption in KSA government organisations. The development of this framework was divided into two phases: Phase 1 involved gathering the framework factors, while Phase 2 included a confirmatory study that was carried out to confirm the framework. This chapter also explained how to identify and synthesise the security factors that hinder governments' attempts to adopt cloud computing. Three categories were proposed in this framework: cloud security risk factors, security benefits, and security social factors. Each category in the framework comprises various factors, all of which have been explained thoroughly. The following chapter describes the methods used in the first stage of this research.

Chapter 4: Research Methodology Used in the First Stage for the Confirmatory Study

The previous chapter examined the proposed cloud security framework to identify those security factors which influence cloud adoption. Following on from this, the present chapter describes the research methodology and the research designs used to explore and confirm the framework's factors in the first stage of this research. The chapter is organised into two main sections. Section 4.1 presents a general discussion of qualitative, quantitative, and mixed methods, as well as triangulation techniques. Following this, Section 4.2 focuses on the research methods applied in this study. A summary of the research methodology process for the confirmatory study of this research is illustrated in Figure 4-1.

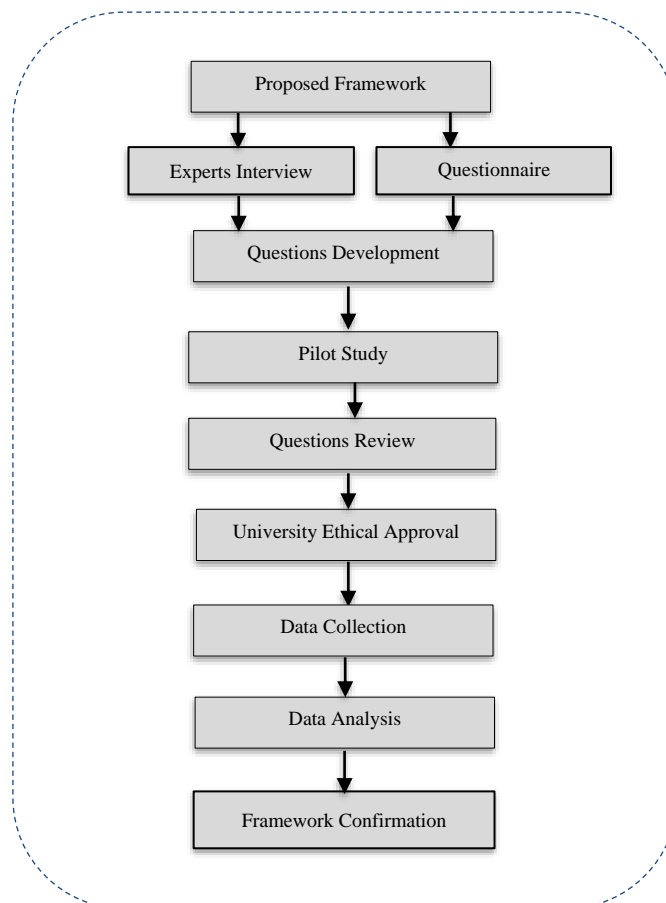


Figure 4-1: Research Methodology Process for Confirming the Framework

4.1 Background of Research Methods

Qualitative methods are exploratory in nature and are used to identify the perceptions of target viewers with reference to specific subjects (Creswell, 2003). This helps in understanding a specific condition, as it provides insights into problems which could potentially be studied in the future. A qualitative method is useful when dealing with secondary data, such as a literature review. However, such methods are insufficient when it comes to gaining an in-depth insight into a subject (Fink, 2003).

With qualitative methods, a large amount of data is generated, although it is not always clear what parts of the data are relevant to the research. A commonly-used technique for analysing qualitative data is coding (Creswell, 2003). Coding involves attaching labels to sets of data so that they can be easily identified. Data is commonly coded in accordance with the main ideas or subjects to be addressed in the research. These codes may be specified prior to data collection or generated as the analysis proceeds; moreover, the codes may be revised and improved as the researcher is exposed to the data and his/her perceptions are broadened. Tools such as Nvivo software may be used to help researchers analyse and keep track of the data (Creswell, 2003).

The second type of research approach is the quantitative method. This is used to measure numerical data into practical statistics by practicing a number of simple measurements or sample participants (Katsirikou, 2010). One method for collecting quantitative data involves finding answers from a set of related questions in a survey. The data gathered is analysed using statistical methods and the outcomes found are generalised to the population (Myers, 1997). One key difference between quantitative and qualitative methods is that qualitative research is concerned with meaning, while quantitative research is concerned with measurement (Saunders et al., 2009).

A mixed method approach is one which uses both quantitative and qualitative methods, and thus includes open-ended as well as closed-ended questions (Creswell, 2003). This helps the investigator to develop a better understanding of the implications resulting from the quantitative data, and the reasons behind these implications (Mack and Natasha, 2005).

The aim of mixing data collection methods is to give the investigator a clearer, wider picture (Caracelli and Greene, 1993). Employing the mixed method approach means that the researcher is making an active choice to increase the depth and improve the logical power of the study (Driscoll et al., 2007). Utilising this tactic can yield more results with a higher level of accuracy.

4.1.1 Triangulation

Triangulation is a technique used to simplify and validate data through the cross verification of two or more sources (Morse, 1991); the technique can be used in both quantitative and qualitative research. Triangulation is divided into four types: data triangulation, investigator triangulation, theory triangulation and methodological triangulation. In order to improve the framework and increase the accuracy of the study, the key findings of this research are subjected to the methodological triangulation method. Triangulation involves the use of two methods – usually one qualitative and one quantitative – to address the same research problem.

Methodological triangulation can be categorised as simultaneous or sequential:

- **Simultaneous Triangulation:** refers to the use of qualitative and quantitative methods at the same time. In this example, there is limited interaction between the two datasets during the data collection, although the results complement each another at the end of the research.
- **Sequential Triangulation:** is used if the findings of one method are essential to the planning of the next method. The qualitative approach is used before the quantitative method, or vice versa (Morse, 1991).

The confirmatory study follows simultaneous triangulation, whereby each element of the triangulation method should be applied individually at the same time (Mack and Natasha, 2005); the results of each phase are then cross compared to confirm the framework. The triangulation method abstract is illustrated in Figure 4-2.

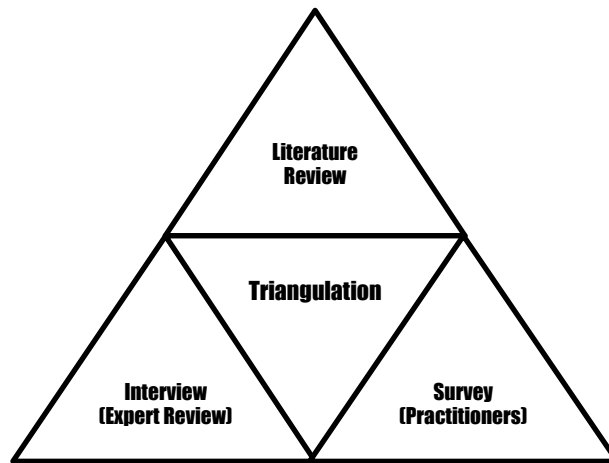


Figure 4-2: Methodological Triangulation Framework Validation

4.1.2 Expert Interviews

The interview is one of the most commonly-used tools when it comes to collecting qualitative data, and can also be employed in conjunction with quantitative research methods (Anderson, 2010). By utilising the interview research method, an investigator can discover additional information related to the subject of study. The flexibility of communication between the researcher and participants during an interview can help the participants to understand the questions. Interviews can take place via telephone, face to face, or online (Kurniawan, 2004), and can also be broken down into four types (Sharp et al., 2011):

1. **Structured Interviews:** the interviewer usually employs the same questions, which are closed-ended in nature. These questions are short and straight to the point.
2. **Unstructured Interviews:** these interviews involve a set of open-ended questions. This method is in stark contrast with fully-structured interviews, and allows the investigator to discover other detailed and important information related to the area (Britten, 1995).
3. **Semi-structured Interviews:** these types of interviews include both closed-ended and open-ended questions, and can be structured as well as unstructured. Questions are determined before the interview, and the investigator can clarify any details about the questions during the interview.

4. **Focus Groups:** a focus group is defined as a conversation within a group about a specific topic. The group generally contains 3 to 10 persons, and one of the group participants directs the conversation. When dealing with such experts, the quantitative, qualitative and mixed method approaches can all be used at different stages of the study (Lake and Tessmer, 1993). The experts are able to express their attitudes or put forth any ideas that may help to develop the research.

The expert review method offers the researcher a chance to reach persons who have varying degrees of involvement in the study rather than just beginners; this, in turn, means that more information can be gathered, thus improving the validity of the study (Olson, 2010).

4.1.3 Expert Interviews Sample Size

When conducting interviews, it is crucial to gather an appropriate number of experts, as this will help in achieving substantial results. With regard to this point, determining the minimum sample size is essential when it comes to producing consistent results (Bhattacharjee, 2012). In terms of the number of experts, according to Grant et al. (1997), there is no agreed-upon number of experts for an interview in a content validity study. However, most researchers recommend a panel consisting of 3 to 20 experts.

In expert sampling, participants are selected based on their knowledge in the field of study (Bhattacharjee, 2012). With this type of sampling, size depends on saturation (Guest et al., 2006). Saturation is reached when no new knowledge can be gathered. In reference to this point, Guest et al. (2006) suggested that saturation is usually reached after 12 interviews.

4.1.4 Questionnaire

The questionnaire is one of the most commonly-used tools for collecting quantitative data (Recker, 2012). It can also be used to collect qualitative data when open-ended

questions are involved. This method is constructive because it is a recognised technique for obtaining data related to, for example, participants' attitudes. Moreover, it can also be used to capture data pertaining to a large population, as such populations cannot be assessed directly; finally, it allows respondents to answer the questions in their own time (Bhattacharjee, 2012). A questionnaire is used to collect information and thus capture knowledge, attitudes, and behaviours. In research where a questionnaire is employed as a data collection tool, participants are asked to answer different predetermined questions.

One of the most significant benefits of applying a questionnaire as a research part is that it allows the investigator to collect a large quantity of data in a period time across the world, and in a relatively cost-effective way (Oppenheim, 2000). In terms of the questionnaire design, there are two styles: self-administered and interview-administered. A self-administered survey requires respondents to take responsibility for reading and answering the questions, while an interview-administered survey is either conducted in person or over the telephone (Saunders et al., 2009; Zikmund, 2012).

4.2 Research Methods Used in the Confirmatory Study

The aim of this study is to explore and confirm which security factors in the framework influence cloud adoption in Saudi government organisations. In order to achieve this, simultaneous methodological triangulation was implemented. This involved linking and comparing data that emerged from a detailed literature review, an expert review, and a questionnaire survey. As can be seen in Figure 4-3, during the first phase, data was collected from secondary research by reviewing related literature in order to build the proposed framework in Chapter 3.

During the second phase, interviews were conducted with experts in order to review and confirm the framework. This phase included both open-ended and closed-ended questions. The open-ended questions were used to identify and explain the reasons behind the experts' answers to the closed-ended questions, and to accommodate suggestions of new factors that had not been included in the framework.

The third phase involved distributing an online questionnaire to IT and security experts who had experience in this field in different Saudi government organisations. The questionnaire included closed-ended questions, the purpose of which was to confirm the factors mentioned.

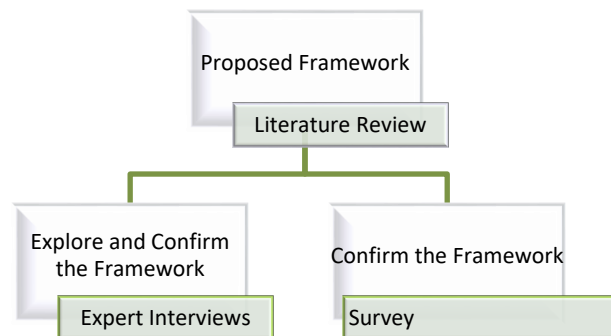


Figure 4-3: Methodological Triangulation for Confirming the Framework

This research applied a mixed method approach, including interviews with experts in the field; the reason for this was to improve and confirm the proposed framework for cloud security adoption in Saudi government organisations and to explore additional factors not already mentioned in the framework. The mixed method approach was selected in order to support the results of the research by validating the findings through triangulation.

In contrast, the questionnaire was selected in order to generalise from a sample to the total population. The questionnaire was aimed using quantitative methods and was employed to collect data from IT and security practitioners (defined as employees who have worked in an IT project) as well as security experts in different departments and locations within the KSA government. The participating experts worked in ministries, research institutes, state universities, education facilities and telecommunication organisations; the aim of the questionnaire was to explore and confirm the proposed cloud security framework.

4.2.1 Design of Expert Interviews

This research included interviews with 12 security experts from the KSA government. The experts targeted in this research were individuals who work on IT projects and security experts in different Saudi government organisations. This method was embraced and, as mentioned above, 12 interviews were conducted with security experts and IT project workers from different departments and locations within the KSA government, including ministries, research institutes, state universities, education facilities and telecommunication organisations. A participant was considered an expert if they had at least three years' experience working on IT projects and three years' experience in the security or cloud field in a Saudi government organisation. The research was conducted in different cities across the KSA (Riyadh, Jeddah, and Madinah), as illustrated in Table 4-1.

Table 4-1: Summary of the Interviewees with Their Position and Years of Experience

Experts	Job Description	Years of experience	Government Organisation	Type of organisation	City
A	Security expert	6+ years	Saudi Food and Drug Authority	Authority	Riyadh
B	Head of the Networking Department	8+ years			
C	Chief Information Officer	3+ years	Ministry of Education	Ministry	Madinah
D	Security Expert	11+ years			
E	Data Management	3+ years	Ministry of Health	Ministry	Jeddah
F	System Administrator	7+ years			
G	Data Security Expert	4+ years	King Abdul-Aziz University	State university	Jeddah
H	Security Expert	5+ years	Ministry of Labour Saudi	Ministry	Riyadh
I	President of the IT Department	16+ years			
J	IT Project & Cloud	10+ years	Saudi Interior Ministry	Ministry	Jeddah
K	Security Expert	6+ years			
L	Cloud System Admin	3+ years			

The purposes of these interviews were:

- To review the factors identified in the literature review based on previously-conducted studies in order to improve the framework.
- To identify additional factors from the context of Saudi government organisations that had not been mentioned previously in the literature.

This research used semi-structured interviews, which included both open- and closed-ended questions. Furthermore, the various procedures involved in the interview method followed several stages:

- The experts were emailed and asked to specify a date, time, and place for the interview. The email also included a brief clarification of the topic and the aims of the research.
- The experts took part in a face-to-face interview with the researcher or were interviewed over the telephone.
- Before the interviews began, the participants were asked to read the participant information sheet and then sign the consent form.
- After participants were shown the framework, they were then given a chance to ask for clarification. This took approximately 10 to 15 minutes.
- Following this, around 18 closed-ended questions were put to the respondents, and they were then asked to refine the factors they had mentioned and to clarify the reasons for their answers.
- The final part of the interview involved open-ended questions that addressed ways in which the framework could be improved; these questions also sought to establish if the participants felt that there existed other factors that affected the adoption of the cloud in KSA government organisations, e.g., security risks, security social factors, and security benefits. This took around 20 minutes.
- The interviews were recorded and lasted, on average, approximately 35 to 40 minutes.

- In cases where the experts were located in the KSA and preferred to complete the interview over the phone, the consent form and the framework sheet, along with the information sheet, were sent to them by email before the interview.

4.2.2 Piloting Interviews with Experts

A pilot test is a chance to try out a survey well before it is used for any official purpose. A pilot test simulates the use of the instrument in its intended setting (Hox, 2008). In order to enhance the effectiveness of this research, a pilot session was carried out to test the interview questions. The test involved 10 people, 5 of whom were IT security experts from Saudi security groups, while 5 were researchers from the University of Southampton in computer science. The aim was to ensure that all questions were clear and understandable. The participants provided a number of comments, and the questions were edited according to said comments.

4.2.3 Questionnaire Design

In order to confirm the proposed framework, a self-administered type for questionnaire was considered for this initial research. The questionnaire was sent to different experienced staff from IT and security departments in Saudi government organisations, including ministries, research institutes, state universities, education facilities and telecommunication organisations. All of the respondents were working in different departments in Saudi government organisations and had at least two years' experience in the security and cloud fields. The questionnaire was posted online and sought to confirm the factors in the framework. A total of 32 experts from Saudi government organisations responded to the online survey. These experts were from different Saudi government organisations in various locations around the KSA. The decision was taken to manage the questionnaire online, as this method suited the needs of the respondents. Respondents were approached by email and asked to complete the online questionnaire. The email included a link to the questionnaire; if they agreed to answer the questions, they could open the link. The first page of the questionnaire explained more about the research and its goals and asked the participants if they agreed to take

part in the research. The page then stated that, if they agreed, they should check the box and press the button to proceed to the next page to answer the questions.

The questionnaire was divided into two parts. The first part asked the respondents four nominal questions, which were designed to confirm their suitability for the study. The second part consisted of questions that respondents could answer using a five-point Likert type scale (Bhattacharjee, 2012); the Likert ratings were as follows: strongly agree = 5, agree = 4, neutral = 3, disagree = 2, and strongly disagree = 1. In reference to this point, Revilla et al. (2014) suggested that, if researchers want to use scales, they should offer 5 answer categories rather than 7 or 11, because the latter yield data which is lower in quality. The purpose of the questions in this part was to confirm the security factors that affect decisions to adopt the cloud in Saudi government organisations. The University of Southampton's iSurvey application was used to generate the online survey.

4.2.3.1 Piloting Questionnaire

A pilot survey was used in order to establish if the respondents understood each of the questions and the instructions for completing the questionnaire itself. This included the wording and language of the questions and the instructions regarding where to mark the responses. Generally speaking, a questionnaire pilot requires 10 or more people (Hox, 2008). As such, the questionnaire was tested by 10 IT security experts taken from the IT division of the ministry of education, as well as from security groups in the KSA and the computer science research facilities of the University of Southampton and King Abdul-Aziz University. Prior to administering the online questionnaire, it was pre-tested by five computer science researchers at the University of Southampton.

4.2.3.2 Questionnaire Sample Size

Quantitative research involves the employment of random sampling, and this allows for the findings of the study to be generalised to the population (Bhattacharjee, 2012). Calculating random sample sizes is usually done mathematically, based on preselected parameters (Guest et al., 2006). Two types of errors are considered when calculating the minimum acceptable sample size (Tessmer, 2009): type1 or α errors, which occur when

rejecting a true null hypothesis, and type2 or β errors, which occur when a false null hypothesis is not rejected. By convention, α is set to 0.05 and $(1 - \beta)$ is set to 0.8 (Banerjee et al., 2009). Another parameter to be taken into consideration is effect size, which refers to the magnitude of the association between the predictor and outcome variables. Cohen (1988) defined three different effect sizes: small ($d=0.2$), medium ($d=0.5$) and large ($d=0.8$). In exploratory studies, effect size is usually set to large. In this research, G* Power software was used to calculate the minimum sample size (Bhattacharjee, 2012; Mack, Natasha, 2005). The calculation was performed using a t-test in order to find the differences between the means. This calculation is shown in Table 4-2 and, as can be seen, the minimum sample size was deemed to be 15.

Table 4-2: Sample Size According to G*Power Software

Statistical Test	Means: Difference from constant (One Sample T-Test)	
Tails	2	Input
Effect size (d)	0.8	Input
Error probability (α)	0.05	Input
Power ($1 - \beta$ error probability)	0.8	Input
Minimum sample size	15	Output

4.2.3.3 Method of Quantitative Analysis

When analysing the quantitative data, the statistical One Sample T-Test (2-tailed) was used. Therefore, it was decided that a test value of 3 on a five-point Likert-type scale was the criterion based on which the judgment should be made as to whether to exclude or include factors. The full Likert scale ranged from 5 (strongly agree) to 1 (disagree), with 3 being neutral. A Bonferroni correction was applied in order to control the false positive error by dividing the alpha ($\alpha = 0.05$) by the number of factors included in the questionnaire ($p\text{-value} = (\alpha/n)$). For this test, a statistical significance level alpha of $\alpha = 0.05$ was chosen. A factor was statistically significant if:

- The $p\text{-value} < 0.0020$ for the first category, namely Security Risk Factors, including 24 items; otherwise, it was not statistically significant.
- The $p\text{-value} < 0.0055$ for the second category, namely Security Social Factors, including 9 items; otherwise, it was not statistically significant.

- The p-value < 0.0027 for the third category, namely Security Benefit Factors, including 18 items; otherwise, it was not statistically significant.

Following a rigorous factors selection stage, it was assumed that all factors were potentially important and should be kept unless there was a strong reason to remove them (e.g., if experts disagreed regarding their importance).

4.2.3.4 Statistical Reliability Test

A statistical reliability assessment was applied to establish whether each of the items from the questionnaire was clear and understood similarly by each participant. Cronbach's alpha coefficient is one of some analysis tools that can be conducted to measure the reliability and accuracy of research measurements. A Cronbach's alpha analysis is capable to measure internal consistency; higher values specify greater correlation between answers, with a maximum possible value of 1. An alpha value of 0.5 was satisfactory (acceptable) to begin the reliability of the internal consistency of the questionnaire in this research (Cronbach and Shavelson, 2004).

4.2.3.5 Ethical Considerations

The participants had to give their knowledgeable consent before starting part in the survey; they could officially approve to take part after being informed about the risks and features of participation, the terms of their participation, and their rights as study subjects (Fink, 2003). During the data collection process, a consent form with sufficient information (participation information) was given to the interviewees to sign; this ensured that they agreed to participate in the study. For the online respondents, they were also given printed sheet of participation information on the first page of the online questionnaire, which they had to check before they might begin responding to the survey.

The quantitative and qualitative methodologies used in this study was approved by the University of Southampton Ethics Committee. Ethics approval was approved under reference number ERGO/FPSE/20966 for both the interviews and the survey.

4.3 Summary

This chapter highlighted the methods used in this research and provided justifications for these selections. A mixed method approach was employed to review and confirm the proposed framework. This included the methodological triangulation of expert reviews, and a questionnaire survey. The expert reviews were based on semi-structured interviews with 12 IT and security experts from Saudi government organisations.

The aim of conducting interviews with the IT experts was to explore and review the proposed factors and identify additional factors related to Saudi government organisations. In order to confirm the security factors that affect cloud adoption, a survey was designed using closed-ended questions, which respondents answered on a five-point Likert-type scale.

A total of 32 IT and security experts from Saudi government organisations filled in the online survey. The findings from both the expert reviews and the questionnaire were used to explore and confirm the framework. Given what was discussed in this chapter, the next chapter will present the results of the interviews and questionnaire, following which these results will be discussed.

Chapter 5: Findings and Discussion for the Confirmatory Study

With the previous chapter having described the research methodology and the research designs in detail, this chapter discusses the results of the mixed method approach used in the first stage of the research. The aim of the interviews and questionnaire was to explore and confirm the factors of the cloud security adoption framework, as well as the reliability of the scale. This chapter also discusses the results of the questionnaire, which was completed by experts from different government organisations in the KSA. The present research relied on expert reviews, which made it possible to evaluate and identify influencing factors, as well as a survey, which was used to confirm the effects of these factors. The results of the questionnaire were analysed using SPSS software, while Nvivo software helped the researcher to analyse the interview findings.

5.1 Results of the Expert Review

The interviews conducted were semi-structured in nature. The data was collected from 12 security experts working in different departments of the Saudi government. The aim of this part was to review and explore the security factors recognised in the literature review and explore other factors that had not been mentioned in previous studies.

Initially, 16 experts were invited via email to participate in an interview. Only 14 responded, and two later chose not to participate. Interviews were conducted with the remaining 12 experts from different Saudi government organisations. All of the expert interviewees had minimum five years' experience working on IT and security projects and three years' experience in the security or cloud fields within Saudi government organisations. They were all capable of summarising and clarifying current security situations. Seven of the participants were working at organisations that had already adopted cloud computing, while five of them were not. The interviews were carried out in August and September of 2016. Some of the interviews were conducted via video conferencing and on the Internet by Skype, with the audio recorded using the QuickTime

recorder application. Some of the expert interviews done by face to face, and this audio was recorded using the Livescribe2 pen. A consent form was obtained from the interviewees before any recordings were made. All expert interviewees approved that their audio can be recorded for transcription purposes. A description of the IT and security experts interviewed, as well as their organisations, will be presented in the next section.

As information from closed-ended questions is considered quantitative approach in nature, questions were put to the 12 experts, who were asked to rate the importance of security factors when it comes to the adoption of cloud computing in Saudi government organisations. The responses to these survey were based on a five-point Likert-type scale, with 5 denoting “very important”, 4 denoting “important”, 3 denoting “may be important”, 2 denoting “not important”, and 1 denoting “not relevant”, as seen in Figure 5-1. SPSS was used to analyse the data. The statistical One Sample T-Test was employed to analyse the results of the quantitative investigation.

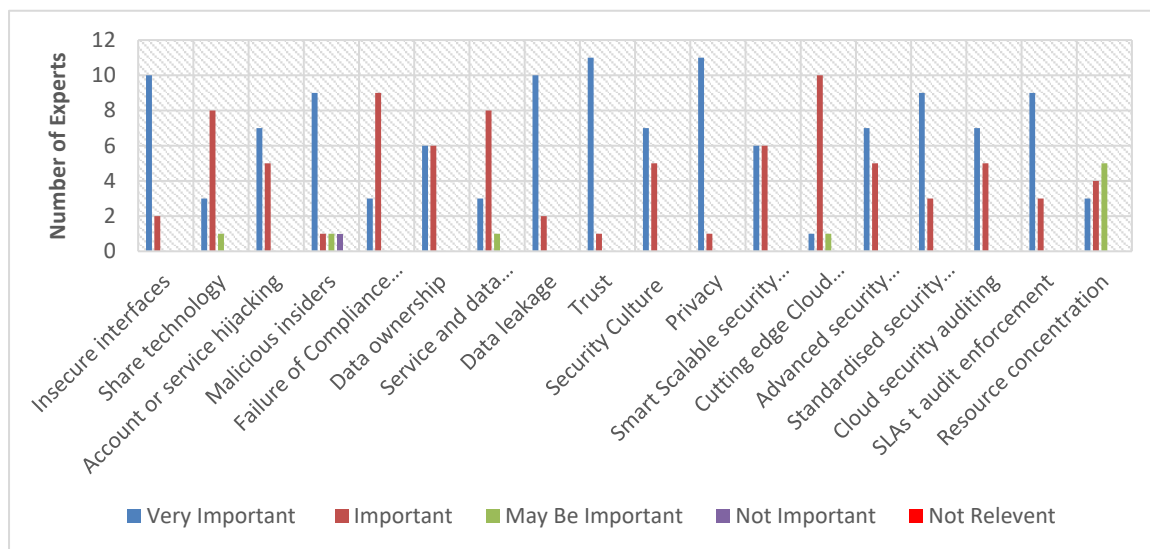


Figure 5-1: Rating of Each Factor by Experts

5.1.1 Descriptive and Frequency Analyses of the Framework Categories for the Interviews

Descriptive and frequency analyses were used to understand the responses regarding the 18 factors in the framework. These factors were split into three categories:

- **Security Risk Factors**

Table 5-1 presents the frequency of security risk factors. There are eight security risk factors that affect the adoption of cloud computing in Saudi government organisations. Of all the respondents, 83% stated that Insecure Interface was a 'very important' type of security risk which affects the adoption of cloud computing, while the other 17% of respondents felt that it was 'important'. The second security risk factor is Shared Technology. Approximately 67% of the respondents felt that this was 'important', while 25% of respondents saw it as 'very important', and 8% of the participants stated that it may not be among the important security risk factors in terms of affecting the adoption of cloud computing. With regard to the Account and Service Hijacking factor of security risk, 58% of the participants saw it as 'very important', and 42% of participants stated that it was an 'important' factor related to security risk. In terms of the fourth factor, namely Malicious Insiders, nearly 76% of the 12 experts concluded that this was 'very important', while 25% of participants viewed it as 'important', 'may be important' and 'not important' respectively, in terms of its effect on the adoption of cloud computing in Saudi government organisations. With regard to the Failure to Comply with Regulations factor, most (75%) of the participants felt that it was 'important', while the others (25%) rated it as 'very important'. The sixth factor, Data Ownership, was deemed by 50% of the experts to be 'very important', while the other 50% of the 12 participants saw it as 'important'. Approximately 67% of the respondents stated that the Data and Service Integration factor was an 'important' element of security risk, while 25% of the participants classed it as 'very important' and 8% as 'may be important'. Most (83%) of the participants concluded that the Data Leakage factor was a 'very important' element of security risk when it comes to the adoption of cloud computing in Saudi government organisations.

Table 5-1: Frequency (Security Risk Factors)

Variable	Ref	percentage					Total 100%
		Very important	Important	May be important	Not important	Not relevant	
Insecure Interfaces	II	83%	17%	0%	0%	0%	100%
Shared Technology	ST	25%	67%	8%	0%	0%	100%
Account or Service Hijacking	AH	58%	42%	0%	0%	0%	100%
Malicious Insiders	MI	76%	8%	8%	8%	0%	100%
Failure to Comply with Regulations	CR	25%	75%	0%	0%	0%	100%
Data Ownership	DO	50%	50%	0%	0%	0%	100%
Service and Data Integration	SDI	25%	67%	8%	0%	0%	100%
Data Leakage	DL	83%	17%	0%	0%	0%	100%

- **Security Social Factors**

The expert questionnaire addressed the importance of security social factors in relation to the adoption of the cloud service in Saudi government organisations. Table 5-2 presents the frequency of security social factors in terms of their influence on the adoption of cloud services in Saudi government organisations. A total of three security social factors were included in the questionnaire. Of the 12 participants, 92% found Trust to be a ‘very important’ security social factor when it comes to the adoption of cloud services in Saudi government organisations, while 8% of the respondents rated it as ‘important’. In terms of the Security Culture factor, 58% of participants stated that it is ‘very important’, and 42% of the participants deemed it to be an ‘important’ security social factor which influences the adoption of cloud services in Saudi government organisations. With regard to the last security social factor, Privacy, most (92%) of the participants viewed this as a ‘very important’ security social factor when it comes to the adoption of cloud services in Saudi government organisations.

Table 5-2: Frequency (Security Social Factors)

Variable	Ref	Percentage					Total 100%
		Very important	Important	May be important	Not important	Not relevant	
Trust	TR	92%	8%	0%	0%	0%	100%
Security Culture	SC	58%	42%	0%	0%	0%	100%
Privacy	PR	92%	8%	0%	0%	0%	100%

- **Security Benefit Factors**

The expert questionnaire was also implemented to gauge, according to the 12 experts, the importance of security benefits in relation to the decision to adopt cloud services in Saudi government organisations. Table 5-3 illustrates the frequency of security benefits in relation to the decision to adopt cloud services in Saudi government organisations. Of all the participants, 50% felt that the Smart Scalable Security factor was a 'very important' and beneficial factor, while 50% viewed it as an 'important' security benefit when it comes to the decision to adopt cloud services in Saudi government organisations. In relation to the Cutting-Edge Security Market factor, most (84%) of the participants felt that it was 'important', and the other 16% of participants saw it as 'very important' and 'may be important' in terms of security benefits. The third benefit factor is Advanced Security Mechanism. Of all the respondents, 58% regarded it as 'very important', and 42% felt that it is 'important' when it comes to decisions to adopt cloud services in Saudi government organisations. With regard to the Standardised Security Interfaces factor, 75% of participants rated it as 'very important', and 25% of participants felt that it was 'important' in terms of affecting the decision to adopt cloud services in Saudi government organisations. In reference to the fifth benefit factor, Cloud Security Auditing, 58% of the 12 respondents viewed it as 'very important', while 42% of participants saw it as 'important'. In terms of the Service Level Agreement Audit Enforcement factor, the majority (75%) of the participants rated it as 'very important', while the others (25%) felt that it was 'important' in relation to decisions to adopt cloud services in Saudi government organisations. Among the 12 participants, 25% regarded the Resource Concentration factor as 'very important', while 33% of respondents felt that it was 'important' and 42% of respondents agreed that it 'may be important' in relation to decisions to adopt cloud services in Saudi government organisations.

Table 5-3: Frequency (Security Benefit Factors)

Variable	Ref	Percentage					Total 100%
		Very Important	Important	May Be Important	Not Important	Not Relevant	
Smart Scalable Security benefits	SS	50%	50%	0%	0%	0%	100%
Cutting-Edge Security Market	CE	8%	84%	8%	0%	0%	100%
Advanced Security Mechanism	AS	58%	42%	0%	0%	0%	100%
Standardised Security Interfaces	SSI	75%	25%	0%	0%	0%	100%
Cloud Security Auditing	CS	58%	42%	0%	0%	0%	100%
SLA Audit Enforcement	SLA	75%	25%	0%	0%	0%	100%
Resource Concentration	RC	25%	33%	42%	0%	0%	100%

The results of the closed-ended questions included in the interviews are presented in Appendix A. The interviewees were asked to convey their attitude towards all of the proposed factors. The aim of the questions was to evaluate, according to the views of experts, the importance of the proposed security factors when it comes to the adoption of cloud services in Saudi government organisations. The experts' responses were collected and recorded using SPSS software, so as they could be statistically analysed. In terms of the experts' opinions, the results in Appendix A show that the means of all proposed factors were greater than the defined value, which was 3. Moreover, the analysis of responses to these questions showed that the factors were statistically significant, and indeed important. The only exception to this was one factor from the security benefits category, namely the Resource Concentration factor, which had a p-value greater than 0.0027. (Resource concentration factor: $(0.082 > 0.0027)$).

While this result clearly shows that the impact of the Resource Concentration factor on organisations was not statistically significant, the findings from previous studies indicated that this factor has a major effect on the decision to adopt cloud computing, as well as on the use of online services and the adoption of new technology (Catteddu and Hogben, 2009; Tei and Gurgun, 2014). Consequently, the Resource Concentration factor was kept in the proposed framework.

With regard to the qualitative data from the expert interviews, Nvivo software was used to analyse and code the responses, as illustrated in Appendix A. Their opinions were analysed and coded to produce the results listed below. The interviewees were asked to

answer open-ended questions about the framework, with three categories included, namely the Security Risk factor, the Security Social factor, and the Security Benefits factor.

All experts agreed that most of the factors in the framework are important and do affect government organisations' decisions to adopt cloud services. Their opinions were analysed and coded to produce the following findings.

Below are some quotes from **Experts J**:

"I agree that most of the factors in the framework are potential variables that hinder some organisations when they are trying to use cloud services and there are some other factors influencing the adoption of cloud services such as: Encryption and Sophisticated Authentication Techniques".

He went on to say that:

"We should consider Encryption and Sophisticated Authentication Techniques as security risks when we are thinking about adopting cloud services because there is reason behind using services such as Consolidated Services".

Another interesting point was made by **Expert B**:

"There are some challenges that my agency and other organisations in Saudi Arabia have faced since using this technology. I advise that it is important to ensure the proper rising of the cloud-based implementation to satisfy the organisation's needs and security breaches caused by social trends".

Some of the experts agreed that it is necessary for any government to test cloud technology before implementing it. The general feeling was that this would help a government to understand the way in which the technology works and to establish if it meets their needs.

As stated by **Expert F**:

“I agree that all security risk factors, as well as the security social and benefits factors mentioned in your framework are essential when any government organisations are making decisions to adopt cloud computing in their organisations and I recommend that all organisations be aware that data encryption should be prepared before and after using cloud services”.

He also went on to make a number of other suggestions:

“Exclusive allocation of the cloud resources should be considered as a security risk when adopting the cloud. There are three challenges that my organisation has faced while using cloud services, and you may consider them important. These are: setting up cloud infrastructure, training on how to use the cloud and adopting classical applications for the cloud”.

In a similar vein, **Expert L** stated that:

“I think we need to try the cloud service before adopting it. We call it a test phase”.

Another interesting point, made by **Expert L**, can be seen below:

“Social Users’ awareness is important when using cloud platforms in order to avoid shadow IT data leakage and protect staff from inside attacks.

In terms of security risk, in order to ensure there is security transparency, the providers should alert the consumers to the security control updates or policies that are applied to their data. Moreover, to guarantee transparency when an incident occurs, the cloud provider should not cover up any security incident affecting their assets and should share the lessons learned from each incident with the consumers to ensure that there is a well-protected cloud environment.

We should consider cloud multi-geographical infrastructures as a security benefit because they are very important for the consumers, especially when natural catastrophes happen”.

Expert G also stated that:

“Whether the cloud service is more appropriate for the government or the private sector depends on IT technology. Hence, the organisation needs to consider the nature of its business and its requirements before adopting the cloud service. Judging from my experience I agree totally with this framework and it is essential to consider these factors when any government organisations make a decision to adopt cloud services. Many environmental and technical changes have been going on in the IT environment which need to settle down first. The IT environment is not yet ready for cloud computing (readiness)”.

As stated by **Expert D**:

“An organisation needs to know how to be on the cutting edge of technology. I consider it very important to recognise who your corporation is. We are a Saudi food and drug authority, so we are not an IT company, and may not have a high willingness to be on the cutting edge technologically”.

Another interesting point, from **Expert D**, is found below:

*“Other factors should be considered as security risks if using the cloud practically in government organisations, such as use of client-side encryption.
The best things about using cloud computing in my organisation are Ease of Access and Team Work”.*

In addition to this, **Experts B, C, D, and F** stated that:

“In terms of the security risk factor, organisations should prepare data encryption and employ this encryption when using cloud services”.

The security social factors are also important and should be taken into consideration. Culture is defined as the “beliefs, values, habits, rules and communication forms of some of people in a community” (Alharbi et al., 2015). The analysis revealed that culture has an influence on the adoption decision. Indeed, one of the experts specified that, while cloud technology influence reduces the number of jobs in a government system, it creates new jobs in those countries which host the services; this is because, within said countries, there is a need to create jobs for the community and to expand the economy.

Below are a number of interesting points from **Expert E**:

“In my opinion, other important factors need to be considered as security risks when an organisation adopts cloud services, such as Vulnerability and Supply Attacks, including all factors mentioned in your framework.

We have started using the cloud because it provides a better insight, aids collaboration, speed, and gives better engagement”.

Another interesting point, from **Expert E**, is found below:

“Service quality, access to data and downtime and accessibility are some of the challenges we have faced while using the cloud”.

The results of the expert interviews confirmed that all factors in the framework do actually affect the adoption of cloud computing services.

Moreover, the experts suggested certain other important factors that should be considered when adopting cloud computing, although most of them had already been discussed in the proposed framework. The experts’ opinions, and the reasons behind using and not using cloud computing services at their organisations, are listed in Table 5-4.

Table 5-4: Expert Interviewees' Reasons for Using and Not Using Cloud Computing.

Reason behind NOT using cloud	Reason behind using cloud
"We made a decision not to using application hosting in the cloud because the application data is reflected intellectual property, and we would to keep it in KSA and train our own teams to manage it. This decreases the risk of the intellectual property being publicised or illegally infiltrated" (Expert H) .	The scalability features of the cloud computing enhanced the high spike of workload during the peak time of the year (Expert A) .
Regarding trust concerns, our data is significant and if we are transferring this to a cloud system the third party will get all the data and everything (Expert J) .	The best things about using cloud computing in my organisation are Ease of Access and Team Work (Expert D) .
Trust problem: only when the data is offsite we can't be assured where it is and if any government organisations will be get into the data (Expert L) .	Because it provides a better insight, aids collaboration, speed, and gives better engagement (Expert E) .
No compliance and regulation is clear and this is one of the causes behind not adopting the cloud service in our department; as a result, we need to update our policies and regulations to comply with cloud services (Expert K) .	Consolidated Services (Expert J) .
Compliance matters could increase the risk of using cloud computing services (Expert A) .	Collaboration and Sharing and Reduce Total Cost of Ownership (Expert B) .
Our data will be with someone else, which makes us unsatisfied (Expert B) .	
Many environmental and technical changes have been going on in the IT environment which need to settle down first. The IT environment is not yet ready for cloud computing (readiness) (Expert G) .	

5.2 Results of the Questionnaire

This section summarises the results of the survey. The quantitative data was collected in August and September of 2016 using an online questionnaire. The questionnaire was initially distributed to 40 respondents, only 32 of whom participated. All of the

respondents were working in different departments in Saudi government organisations and had at least two years' experience in the security and cloud fields. The aim of the survey was also to confirm the proposed framework. The results of the survey were divided into two sections. The first section related to demographic information, while the second section presented closed-ended questions pertaining to 18 security factors that affect the use of the cloud.

5.2.1 Demographic Information

The demographic information for the respondents and their organisations is presented in Table 5-5. Here, four different questions were put to the respondents. With regard to the first question, all of the respondents gave a positive answer, stating that they had worked on an IT project for a government organisation. In terms of the second question, the majority (75%) of participants stated that they had used cloud computing services at their organisation, while the other 8 (25%) respondents admitted that they had not used cloud computing services at their organisation.

Table 5-5: Demographic Survey Frequency

Questions	Answers	Frequency	Percentage
Have you worked on an IT project for a government organisation?	Yes	32	100%
	No	0	0%
Have you used cloud services at your agency?	Yes	24	75%
	No	8	25%
Do you think security affects your organisation's decision to adopt the cloud?	Yes	27	84%
	No	5	16%
Choose the option that best reflects your years of experience in the security field:	2 years	4	12%
	3 to 5 Years	8	25%
	6 to 10 Years	14	44%
	More than 10 years	6	19%

When answering the third question, most (84%) of the respondents agreed that security issues significantly affect their organisation's decision to adopt the cloud. The last question sought to establish respondents' level of experience in the security field. Of the 32 respondents, 44% had 6 to 10 years' experience, 25% of the participants had 3 to 5

years' experience, 19% of the respondents had more than 10 years' experience, and 12% of the respondents had 2 years' experience. Descriptive and frequency analyses were used to recognise the responses information.

5.2.2 Descriptive and Frequency analyses of the Framework Categories for Questionnaire

Descriptive and frequency analyses were used to recognise the responses information. This section provides the results of the closed-ended questions regarding the 18 security factors that affect the adoption of the cloud framework. These questions were answered using a five-point Likert-type scale, with 5 denoting "strongly agree", 4 denoting "agree", 3 denoting "neutral", 2 denoting "disagree", and 1 denoting "strongly disagree". SPSS software was applied to analyse the data. These factors can be split into three categories:

- **Security Risk Factors**

Here, in the first component of the framework, 24 questions were put to 32 participants, who were asked to rate the importance of security risk factors when it comes to the adoption of cloud services in KSA government organisations. The frequency of security risk factors is represented in Table 5-6.

Table 5-6: Security Risks Frequency

Variable	Ref	Percentage					Total 100%
		Strongly agree (5)	Agree (4)	Neutral (3)	Disagree (2)	Strongly disagree (1)	
Insecure Interfaces	II1 (Q1)	65%	29%	3%	3%	0%	100%
	II2 (Q2)	63%	31%	6%	0%	0%	100%
	II3 (Q3)	56%	38%	6%	0%	0%	100%
Shared Technology	ST1 (Q4)	56%	41%	3%	0%	0%	100%
	ST2 (Q5)	30%	38%	16%	16%	0%	100%
Account or Service Hijacking	AH1(Q6)	53%	22%	19%	6%	0%	100%
	AH2(Q7)	38%	41%	9%	12%	0%	100%
	AH3(Q8)	41%	31%	16%	12%	0%	100%
Malicious Insiders	MI1(Q9)	50%	34%	9%	7%	0%	100%
	MI2(Q10)	60%	34%	6%	0%	0%	100%

	MI3(Q11)	66%	31%	3%	0%	0%	100%
Failure to Comply with Regulations	CR1(Q12)	44%	25%	22%	6%	3%	100%
	CR2(Q13)	44%	44%	6%	6%	0%	100%
	CR3(Q14)	44%	41%	6%	9%	0%	100%
	CR4(Q15)	60%	31%	9%	0%	0%	100%
Data Ownership	DO1(Q16)	50%	44%	6%	0%	0%	100%
	DO2(Q17)	47%	38%	9%	6%	0%	100%
	DO3(Q18)	45%	34%	12%	9%	0%	100%
Service and Data Integration	SDI1(Q19)	53%	44%	3%	0%	0%	100%
	SDI2(Q20)	41%	41%	9%	6%	3%	100%
	SDI3(Q21)	35%	56%	3%	6%	0%	100%
Data Leakage	DL1(Q22)	41%	44%	12%	3%	0%	100%
	DL2(Q23)	28%	60%	3%	9%	0%	100%
	DL3(Q24)	35%	44%	12%	6%	3%	100%

With regard to the factor of Insecure Application Programming Interfaces Risk, 65% of participants strongly agreed, and 29% of participants agreed, that this factor has an impact on decisions to use cloud services. In addition, 94% of respondents felt that awareness of the Insecure Application Programming Interfaces Risk factor affects cloud adoption decisions; in addition, 94% of participants stated that people should be aware of security risks related to the use of the cloud, such as Insecure Interfaces.

Of all the participants, 56% strongly agreed, and 41% agreed, that the Secure Sharing Technology factor must be considered when adopting cloud services, while only 3% of participants gave no opinion. Approximately 30% of respondents strongly agreed, and 38% of respondents agreed, that the Shared Technology Model factor negatively affects the decision to use cloud services; 16% of participants gave no opinion. On the other hand, 16% of respondents disagreed with the notion that the Shared Technology Model factor negatively affects the decision to use cloud services.

However, when it came to the Account or Service Hijacking factor, 75% of participants stated that users should be aware that account hijacking could occur when using the cloud. Moreover, of the 32 participants, 79% felt that the Service Hijacking factor is the highest cloud security risk and 9% of participants gave no opinion. In addition to this, 41% of participants strongly agreed, and 31% of participants agreed, that the Service

Hijacking factor often involves stolen identifications, and this affects the decision to adopt the cloud.

With regard to the Malicious Insiders risk factor, most of the respondents agreed that, without full knowledge and control, a government agency is at risk of being infiltrated by Malicious Insiders; 94% of respondents felt that the Malicious Insiders factor affects the confidentiality, integrity, and availability of government information; in addition, almost all (97%) of the respondents agreed that the Malicious Insiders factor is important when it comes to governments understanding what providers are doing to protect the cloud from such a risk.

Moreover, with regard to the Failure to Comply with Regulations factor, 69% of respondents felt that the existing laws and regulations are not sufficient to protect information stored on the cloud; 88% of participants stated that Comply with Regulations is an effective factor when it comes to making secure transfers to the cloud; moreover, 85% of the 32 respondents felt that the Failure to Comply with Regulations factor negatively influences the decision to adopt the cloud. These essential cloud computing regulations comply with Saudi law.

However, with regard to the Data Ownership risk factor, 94% of the 32 participants agreed that Data Ownership is a critical factor when it comes to cloud security risk, and that government organisations must consider it. In total, 95% of respondents felt that any government agency adopting the cloud should be qualified and that the ownership of data should be exclusive when adopting the cloud.

On the other hand, with regards the Service and Data Integration factor, most (97%) of the respondents agreed that, when dealing with data integration, every government agency must be assured that its own data is protected. Approximately 82% of respondents were of the opinion that unsecured data is more liable to interception when it is transmitted to the cloud and that service integration is one of the top challenges faced by many government organisations when adopting the cloud.

Finally, when it came to the Data Leakage risk factor, 85% of participants stated that users should be concerned about the service provider's authentication systems, as these allow access to data. Approximately 88% of respondents felt that data leakage results from weaknesses in the physical transport system used for cloud data and backups, while 79% of the respondents were worried that data leakage will affect the decision to adopt the cloud.

- **Security Social Factors**

For this category, 8 questions were put to 32 respondents, who were asked to rate the importance of security social factors in relation to the adoption of the cloud service by KSA government organisations, as illustrated in Table 5-7.

Table 5-7: Security Social Factors Frequency

Variable	Ref	Percentage					Total 100%
		Strongly agree (5)	Agree (4)	Neutral (3)	Disagree (2)	Strongly disagree (1)	
Trust	TR1(Q25)	41%	44%	6%	9%	0%	100%
	TR2(Q26)	47%	47%	6%	0%	0%	100%
	TR3(Q27)	19%	50%	6%	16%	9%	100%
Security Culture	SC1(Q28)	38%	54%	3%	6%	0%	100%
	SC2(Q29)	38%	50%	6%	3%	3%	100%
	SC3(Q30)	44%	44%	6%	3%	3%	100%
Privacy	PR1(Q31)	57%	33%	10%	0%	0%	100%
	PR12(Q32)	44%	44%	6%	6%	0%	100%
	PR3(Q33)	35%	25%	19%	12%	9%	100%

Of the 32 participants, 85% felt that secure cloud technology was trustworthy, 94% of respondents expressed concerns in relation to surrendering an organisation's data to third-party control, and 69% of participants felt confident about storing government data on the cloud.

In terms of the Security Culture risk factor, 92% of participants felt that it is an important factor that should be taken into consideration when adopting the cloud, while 88% of respondents believed that it could support government organisations' decisions. In addition, 88% of participants were of the opinion that the Security Culture risk factor affects the execution of information security policies within government organisations.

Of the 32 participants, 90% stated that one of the most critical risks affecting the decision to use cloud services is privacy; indeed, 88% of respondents felt that government organisations would use the cloud service if the privacy of the information were guaranteed.

- **Security Benefits Factors**

In this section of the survey, 18 questions were put to 32 people who were asked to rate the importance of the Security Benefits factor in relation to the adoption of cloud services by government organisations. The frequency of the Security Benefits factor is illustrated in Table 5-8.

Table 5-8: Security Benefits Frequency

Variable	Ref	Percentage					Total 100%
		Strongly agree (5)	Agree (4)	Neutral (3)	Disagre e (2)	Strongly disagree (1)	
Smart Scalable security benefits	SS1(Q34)	28%	63%	9%	0%	0%	100%
	SS2(Q35)	25%	59%	16%	0%	0%	100%
	SS3(Q36)	31%	56%	13%	0%	0%	100%
	SS4(Q37)	28%	53%	13%	6%	0%	100%
Cutting-Edge Security Market	CE1(Q38)	34%	53%	13%	0%	0%	100%
	CE2(Q39)	28%	63%	9%	0%	0%	100%
Advanced Security Mechanism	AS1(Q40)	38%	44%	18%	0%	0%	100%
	AS2(Q41)	35%	59%	6%	0%	0%	100%
	AS3(Q42)	38%	56%	6%	0%	0%	100%
Standardised Security Interfaces	SSI1(Q43)	38%	47%	13%	2%	0%	100%
	SSI2(Q44)	44%	44%	12%	0%	0%	100%
	SSI3(Q45)	47%	44%	9%	0%	0%	100%
Cloud Security Auditing	CS1(Q46)	34%	50%	16%	0%	0%	100%
	CS2(Q47)	31%	50%	19%	0%	0%	100%
SLA Audit Enforcement	SLA1(Q48)	28%	50%	22%	0%	0%	100%
	SLA2(Q49)	41%	47%	9%	3%	0%	100%
Resource Concentration	RC1(Q50)	25%	44%	31%	0%	0%	100%
	RC2(Q51)	28%	44%	28%	0%	0%	100%

With regard to the Smart Scalable benefit factor, 91% of the respondents felt that the smart scalable to multiple locations security benefit is an important driver when it comes to adopting the cloud; moreover, 84% of participants agreed that the ability to extend

the security features in edges networks is an important benefit of adopting the cloud. In addition to this, 87% of respondents felt that Time of Response is an important smart scalable security benefit when it comes to adopting the cloud. Finally, 81% of the 32 participants expressed the opinion that Smart Scalable security benefits help their government agency to make decisions regarding the adoption of the cloud.

Furthermore, in terms of the Cutting-Edge Cloud security market benefits factor, 87% of respondents felt that this is important when it comes to securing assets during the adoption of the cloud; moreover, most (91%) of the respondents classed it as one of the top benefits of adopting the cloud.

Among the 32 participants, 81% concluded that the cloud provider can provide centralised security in the form of service patches to help their government agency adopt the cloud; the remaining 19% of respondents gave no opinion. Approximately 94% of the respondents agreed that updates for the stakeholders are more efficient than traditional organisations' security capability when it comes to advanced security mechanisms. Most of the respondents opined that users should implement the advanced security mechanisms feature when adopting the cloud in order to protect assets.

However, with regard to the Standardised Security Interfaces benefit factor, 84% of participants were of the opinion that Standardised Security Interfaces can enhance any government's ability to change from one provider to another in a short period. In addition to this, 88% of respondents agreed that Standardised Security Interfaces help to reduce cost when the government is using the cloud, and 91% of the 32 respondents felt that it is important to consider the Standardised Security Interfaces feature when making the decision to adopt the cloud. In terms of the Cloud Security Auditing benefit factor, 84% of respondents stated that the auditing security benefit should be better organised if the government wishes to adopt the cloud; moreover, 78% of respondents opined that users should consider the service level agreement audit enforcement when adopting the cloud. Added to this, in terms of the Service Level Agreement Audit Enforcement benefit factor, 88% of participants saw it as one of the most important

benefits, as the provider has to comply with audit demands stated in the service level agreements; 9% of participants provided no opinion. Indeed, it was clear that most (88%) of the participants agreed that people should consider the Service Level Agreement Audit Enforcement factor when adopting the cloud.

The final factor in this category was the Resource Concentration benefit factor; 69% of respondents concluded that this factor can adequately protect a government's data, while 72% of participants saw it as an 'important' factor when adopting the cloud.

5.2.3 Analysis of Each Category Using One-Sample T-Test

In this section of the questionnaire, 24 questions were put to participants for the first category, namely Security Risk Factors. These participants also had to answer 9 questions for the second category, namely Security Social Factors, and 18 questions for the third category, namely Security Benefit Factors; there were between 2 and 4 questions for each factor.

In the Security Risk Factors category, the statistical One Sample T-Test (2-tailed) was used to analyse the quantitative data, as illustrated in Table 5-9. The Bonferroni correction was applied by dividing the alpha ($\alpha = 0.05$) by the number of items ($p\text{-value} = (\alpha/n)$, $(0.05/24) = 0.0020$). For this test, a factor was deemed to be statistically significant if the $p\text{-value} < 0.0020$; otherwise, it was not statistically significant.

Table 5–9: Analysis of Security Risk Factors Using One–Sample T–Test

Variable	Ref	t	N	Mean	Sig (2-tailed)
1. Insecure Interfaces	II1	10.072	32	4.50	<0.001
	II2	13.940	32	4.53	<0.001
	II3	13.940	32	4.53	<0.001
2. Shared Technology	ST1	16.102	32	4.59	<0.001
	ST2	3.050	32	3.75	0.05
3. Account or Service Hijacking	AH1	5.638	32	4.13	<0.001
	AH2	4.008	32	3.91	<0.001
	AH3	3.768	32	3.88	<0.001
4. Malicious Insiders	MI1	6.445	32	4.22	<0.001
	MI2	14.281	32	4.56	<0.001
	MI3	19.416	32	4.66	<0.001

Variable	Ref	t	N	Mean	Sig (2-tailed)
5. Failure to Comply with Regulations	CR1	4.473	32	3.91	<0.001
	CR2	6.416	32	4.16	<0.001
	CR3	5.171	32	4.06	<0.001
	CR4	13.940	32	4.53	<0.001
6. Data Ownership	DO1	13.371	32	4.47	<0.001
	DO2	6.445	32	4.22	<0.001
	DO3	4.844	32	4.03	<0.001
7. Service and Data Integration	SDI1	15.661	32	4.56	<0.001
	SDI2	5.536	32	4.09	<0.001
	SDI3	6.731	32	4.19	<0.001
8. Data Leakage	DL1	7.721	32	4.25	<0.001
	DL2	5.018	32	3.97	<0.001
	DL3	5.438	32	4.06	<0.001

In the security social factors category, the statistical One Sample T-test (2-tailed) was used to analyse the quantitative data, as illustrated in Table 5-10. The Bonferroni correction was applied by dividing the alpha ($\alpha = 0.05$) by the number of items ($p\text{-value} = (\alpha/n)$, $(0.05/9) = 0.0055$). For this test, a factor was deemed to be statistically significant if the $p\text{-value} < 0.0055$; otherwise, it was not statistically significant.

Table 5-10: Analysis of Security Social Factors Using One-Sample Test

Variable	Ref	t	N	Mean	Sig (2-tailed)
1. Trust	TR1	4.980	32	4.00	<0.001
	TR2	12.938	32	4.41	<0.001
	TR3	1.877	32	3.44	0.070
2. Security Culture	SC1	6.731	32	4.19	<0.001
	SC2	7.215	32	4.19	<0.001
	SC3	7.440	32	4.25	<0.001
3. Privacy	PR1	11.811	32	4.50	<0.001
	PR2	6.960	32	4.25	<0.001
	PR3	1.815	32	3.41	0.027

In terms of the Security Benefits Factors category, the statistical One Sample T-Test (2-tailed) was used to analyse the quantitative data, as illustrated in Table 5-11. The Bonferroni correction was applied by dividing the alpha ($\alpha = 0.05$) by the number of items ($p\text{-value} = (\alpha/n)$, $(0.05/18) = 0.0027$). For this test, a factor was deemed to be statistically significant if the $p\text{-value} < 0.0027$; otherwise, it was not statistically significant.

Table 5-11: Analysis of Security Benefits Factors Using One-Sample Test

Variable	Ref	t	N	Mean	Sig (2-tailed)
1. Smart Scalable Security Benefits	SS1	11.392	32	4.16	<0.001
	SS2	9.659	32	4.09	<0.001
	SS3	9.658	32	4.16	<0.001
	SS4	5.568	32	4.00	<0.001
2. Cutting-Edge Security Market	CE1	10.718	32	4.31	<0.001
	CE2	12.535	32	4.31	<0.001
3. Advanced Security Mechanism	AS1	9.105	32	4.19	<0.001
	AS2	13.939	32	4.34	<0.001
	AS3	12.636	32	4.34	<0.001
4. Standardised Security Interfaces	SSI1	7.400	32	4.16	<0.001
	SSI2	10.849	32	4.34	<0.001
	SSI3	12.938	32	4.41	<0.001
5. Cloud Security Auditing	CS1	9.698	32	4.19	<0.001
	CS2	8.399	32	4.06	<0.001
6. SLA Audit Enforcement	SLA1	8.395	32	4.03	<0.001
	SLA2	8.036	32	4.25	<0.001
7. Resource Concentration	RC1	7.874	32	4.00	<0.001
	RC2	7.407	32	3.97	<0.001

Following a rigorous factors selection stage, it was assumed that all factors were potentially important and should be kept unless there was a strong reason to remove them (e.g., if experts disagreed on their importance). Therefore, it was decided that a test value of 3 on a five-point Likert-type scale was the criterion based on which the judgment would be made as to whether to exclude or include factors. The full Likert scale ranged from 5 (strongly agree) to 1 (disagree), with 3 denoting neutral. The discussion and findings related to these categories will be explained in the next section after the reliability test section.

5.2.4 Reliability Test of Questionnaire (Cronbach's Alpha)

The Cronbach's alpha method was used in the present research to ensure that the items were reliable and could measure the factors effectively. SPSS software was used to conduct the Cronbach's alpha test. Table 5-12 illustrates the overall reliability test for

the factors; the Cronbach's alpha was 0.756, thus demonstrating that the results were reliable.

Table 5-12: Reliability Statistics of Questionnaire

Reliability Statistics		
Cronbach's Alpha	Cronbach's Alpha Based on Standardised Items	No. of Items
.756	.786	51

Figure 5-2 presents the mean averages of the items and the reliability results of the questionnaire for each factor; moreover, Table 5-13 displays the results for each factor in terms of the alpha value.

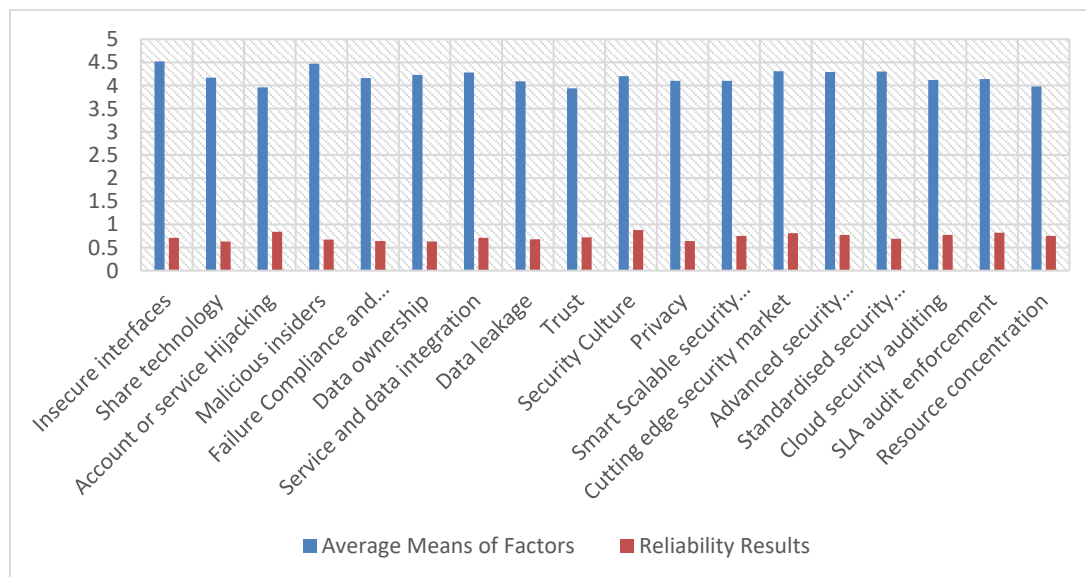


Figure 5-2: Mean and Reliability Chart of the Questionnaire

Table 5-13: Questionnaire Reliability Statistics Based on Cronbach's Alpha Measure

Factors	Number of Items	Reliability Results of Cronbach's alpha
Insecure Interfaces	3	0.716
Shared Technology	2	0.636
Account or Service Hijacking	3	0.848
Malicious Insiders	3	0.679
Failure to Comply with Regulations	4	0.641
Data Ownership	3	0.637
Service and Data Integration	3	0.716
Data Leakage	3	0.685
Trust	3	0.724
Security Culture	3	0.884
Privacy	3	0.642
Smart Scalable Security Benefits	4	0.756
Cutting-Edge Security Market	2	0.813
Advanced Security Mechanism	3	0.771
Standardised Security Interfaces	3	0.694
Cloud Security Auditing	2	0.772
SLA Audit Enforcement	2	0.821
Resource Concentration	2	0.754

5.3 Discussion of Findings

This section presents the overall findings of the interviews and questionnaires which were conducted with security experts and IT professionals from different government organisations in the KSA. The research sought to confirm that all of the categories, along with their factors in the suggested framework, are essential when it comes to adopting cloud services in Saudi government organisations.

5.3.1 Findings Regarding the Categories in the Framework

The findings pertaining to the factors in the framework were all derived from statements made by the experts and IT security specialists in the questionnaire. All experts agreed that security is the top priority in an organisation. If an organisation does not ensure that proper security is in place, then the services will not be reliable or acceptable to the users. In terms of attitude towards categories and their factors, the experts strongly agreed that these have an impact on the adoption of cloud services in Saudi government

organisations. Furthermore, the statistical results of the expert interviews revealed that the answers were strongly significant; the means of these factors were between 3.2 and 4.9. Moreover, the questionnaire results indicated that security social attitude and its associated items have an effect on government organisations' intention to adopt cloud computing.

Moving to the Security Risk Factors category, the following factors were statistically confirmed: Insecure Interfaces, Shared Technology, Account or Service Hijacking, Malicious Insiders, Failure to Comply with Regulations, Data Ownership, Service and Data Integration, and Data Leakage. The results of the interviews revealed that the 12 experts agreed that these factors are either important or very important when it comes to the adoption of cloud computing in Saudi government organisations; they also concluded that these factors have a significant impact on stakeholders' behaviour when adopting cloud services.

The means resulting from the quantitative analysis of the interviews in this category were between 4.7 and 4.8, thus signifying a very high impact. Furthermore, with regard to the security risk factors, the statistical results of the questionnaire showed that all items were statistically significant, with the exception of one item which belonged to the Shared Technology factor (ST2). With a p-value greater than 0.0020, ST2 was not statistically significant, thus suggesting that the effect was due to chance; this item was removed.

The results of the interviews specified that the security social factors category, and its sub-factors, are essential to any government organisations when deciding whether or not to adopt the cloud. Upon examining the expert reviews, it is clear that security culture, trust, and privacy were deemed to be very important factors; none of the experts disagreed with the statement that "these factors are essential to helping organisations use cloud services".

In addition, when rating the importance of this statement, the experts selected 'very important' and 'important', with mean scores ranging from 4.6 to 4.9. In terms of the questionnaire responses, all of the security social category factors and their items were

deemed to be important. However, two items belonging to the Trust and Privacy factors (TR3 and PR3) respectively, were not statistically significant, thus suggesting that their effects were due to chance. Consequently, these items, both with a p-value greater than 0.0055, were removed.

Finally, from the perspective of the experts interviewed, the cloud computing service provides a number of benefits to users. This research showed that, with regard to the security benefits category (Smart Scalable security benefits, Cutting-Edge Security Market, Advanced Security Mechanism, Standardised Security Interfaces, Cloud Security Auditing, SLA Audit Enforcement and Resource Concentration), all factors were found to be crucial, with means ranging from 3.25 to 4.75. In terms of the interview results, one exception was the Resource Concentration factor, with a mean of 3.25. This factor was not statistically significant. However, the questionnaire results for the same category indicated statistical significance for all of the category's factors and sub-items, with means ranging from 3.97 to 4.41. The participants agreed that the security features of the cloud were an important element and should be considered when government organisations are deciding whether or not to adopt the cloud.

Although the results for the Resource Concentration factor differed between the questionnaire and the interviews, this factor was kept in the proposed framework due to the fact that several past studies have emphasised its importance in terms of influencing the use of cloud services and the adoption of new technology (Tei and Gurgen, 2014; Catteddu and Hogben, 2009).

In summary, the results showed that 'there is a positive attitude to adopt cloud services in KSA government organisations: 75% of participants specified that their organisations expect to adopt cloud computing services in the near future'.

5.3.2 Suggested Factors from Experts

The experts were also asked to suggest any other factors, not included in the proposed security adoption framework, that they felt could have an influence on the adoption of the cloud. When asked to make these suggestions, the experts placed particular emphasis on one factor that they felt KSA government organisations should take into account when adopting the cloud, namely Failure of Client-side encryption.

This revelation makes client-side encryption an important factor. The perception is that every part of the data should be encrypted on the client-side in a way which means that even an attacker with substantial computing power cannot access the confidential information or violate end-users' privacy. Indeed, there is also the perception that, if this were the case, then the use of a cloud service would not influence information policies (Souza and Puttini, 2016).

Client-side encryption obviously increases users' ability to protect data and files. By rejecting viewing access to servers and service providers, client-side encryption guarantees that the data and files that are stored in the cloud stay private, thus eliminating the chance that critical information or photos can be accessed, stolen or leaked (Xu et al., 2013). This was deemed to be an important factor, with five of the experts suggesting that it should be added to the framework. They pointed out this factor, as it has a beneficial effect on stakeholders' attitude towards using cloud services. As such, this factor was included in the security risks category in the framework. Figure 5-3 shows the validated factors in this framework after editing according to the results of the expert interviews and the questionnaire.

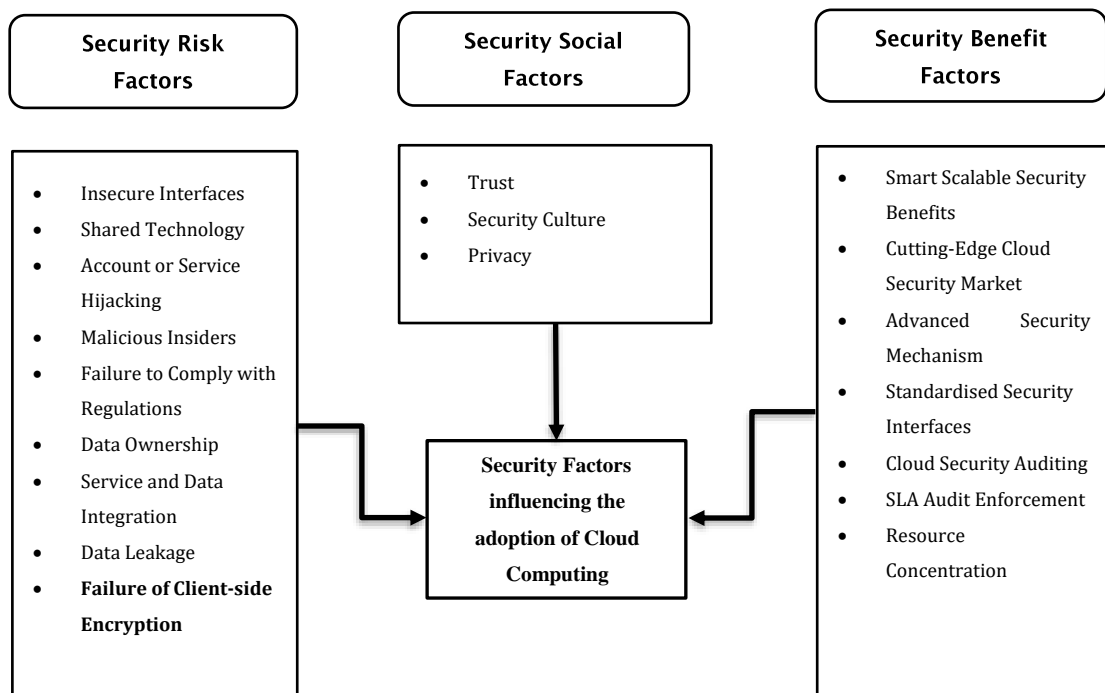


Figure 5-3: Confirmed Framework Including Security Factors that Influence the Cloud Computing Adoption in Saudi Government Organisations

5.4 Summary

This chapter discussed the results of the expert interviews and questionnaires. Semi-structured interviews were applied to explore and review the factors recognised previously in the literature review, and to explore other factors that had not been specified in previous studies. Of particular importance in this study was the confirmation of security factors in the proposed framework which influence cloud adoption in Saudi government organisations.

This was the first step in the investigation of the factors that enable these organisations to adopt the cloud in the KSA. The aim was to utilise these confirmed factors from the preliminary research to survey a larger sample of IT experts and decision makers from several government organisations in the KSA. Finally, this chapter concluded with a discussion of the outcomes from the interviews and questionnaires. The results of this research were used to improve the proposed framework. Following on from this, the

next chapter will explain the aspects of, and methods used, in the second stage of this research, namely sample size, data analysis, factor analysis procedures and ethical approval.

Chapter 6: Research Methodology Used in the Second Stage for Developing and Validating the Instrument and the Model

6.1 Introduction

While the previous chapter presented the results of the mixed method approach used in the first stage of the research, this chapter concludes the methods used in the second stage of the research, as presented in Figure 6-1. After the confirmation of the security cloud adoption model in the earlier chapters, this chapter presents an overview of the research methods used in the second stage of the research, the aim of which was to test the proposed model and research hypothesis.

The chapter begins with a brief argument of the research philosophy and approach deemed suitable for this study. It presents the research strategy used in this research and discusses the process of developing and designing the instrument.

This chapter also details the selection of the sample size and the tests used to ensure the reliability and validity of this study. Applied correlations and factors analysis will be discussed, while the confirmatory study will be demonstrated in this chapter by using the SEM technique. Finally, the data analysis procedures and ethical approval consideration will be presented.

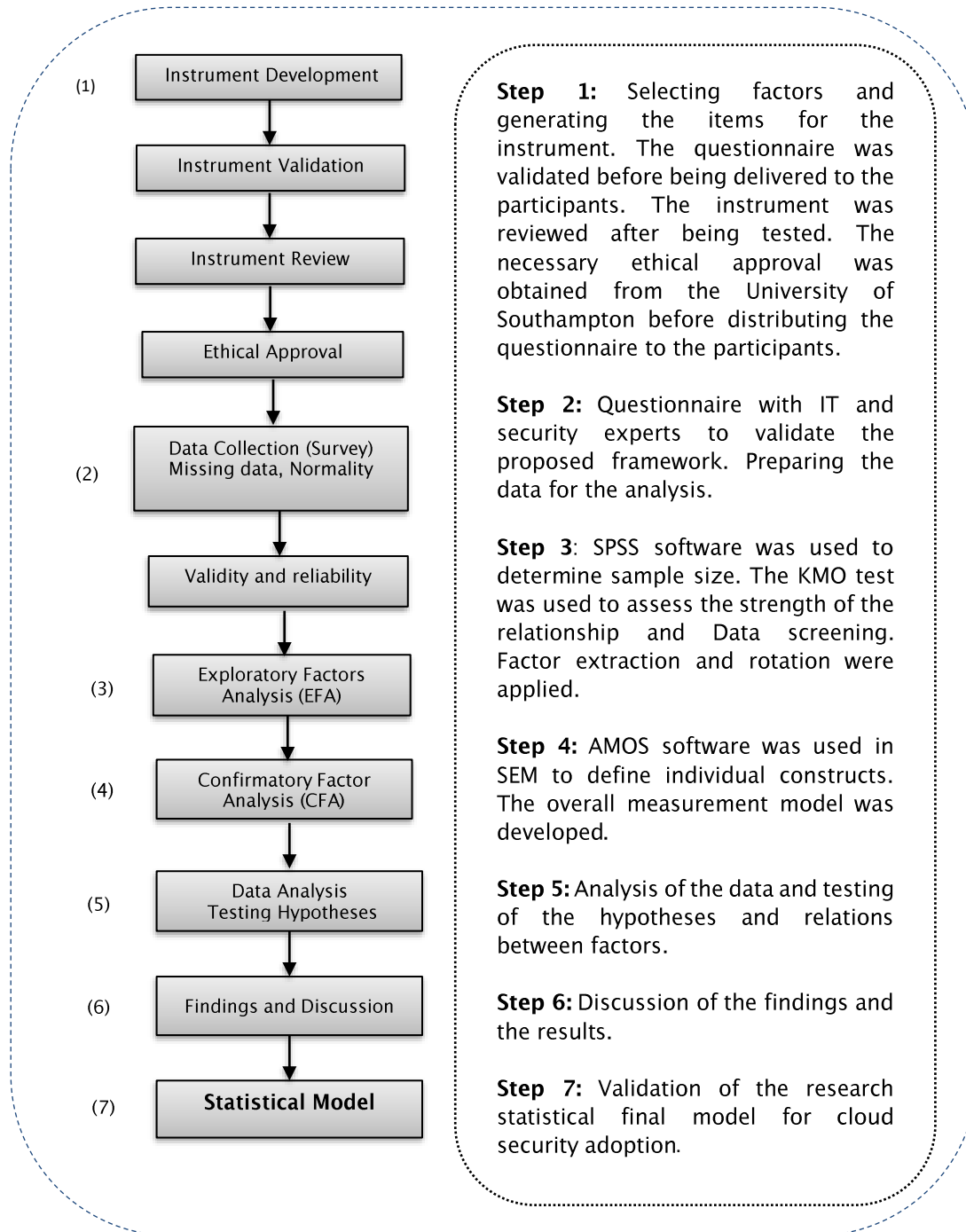


Figure 6-1: Research Design Steps for the Second Stage of this Research

6.2 Research Philosophy

Research philosophy, also known as philosophical assumptions, is defined as *“a set of common assumptions or ways of thinking about some aspects of the world”* (May and Williams, 2002). Philosophical assumptions influence the decisions about research style and the design of a research study (May and Williams, 2002; Creswell, 2012). It is important to understand the underpinning philosophical assumptions which support the definition of the methodology and approach which a researcher uses in their research. In other words, a paradigm is just a set of theories shared by a community of researchers. Guba and Lincoln (1994) suggested that ontological, epistemological and methodological assumptions assist in understanding philosophical assumptions.

Research is based on a philosophy which contains assumptions. These assumptions support the research strategy and the methods. There are four research philosophies, including Positivism, Realism, Interpretivism, and Pragmatism (Creswell, 2003).

- **Positivism:** is an epistemological position. The positivism philosophy involves conducting methods derived from natural sciences. Positivist researchers consider this method to be appropriate for hypothesis testing: determining a phenomenon and making a prediction.
- **Realism:** is a philosophy that relates to technical research. The aim of realism is that what the senses tell us is reality is actually the truth, and this aim has a subsistence which is independent of the human mind (Creswell, 2003). This method is similar to positivism in that it uses a systematic approach for knowledge development.
- **Interpretivism:** involves differentiating between humans as social actors. In interpretivism approaches, the scientists are considered part of the social world, and trust that reality is built on social communication. Therefore, the main idea of interpretivism is to understand phenomena which are offered by human understandings (Myers, 1997).

- **Pragmatism:** is a combination of two philosophies. When a research question might be able to respond to the exact situation, and another situation is suitable to answer the other research question, then pragmatism is the appropriate philosophy (Orlikowski and Baroudi, 1991).

In this study, the need to choose an appropriate research philosophy, method and approach is important, since there exist many kinds of Information Systems (ISs), research methodologies, and approaches to decide upon. This research adopts a positivist position, as it uses methodical methods. The positivist method is in line with the research objectives. The aim of this study is to investigate the security factors that influence decisions to adopt cloud computing in Saudi Arabia's government organisations. Therefore, this study places emphasis on evaluating the relationships between these factors, and their effects on the adoption of cloud computing. In addition, the study hypotheses that have been formulated essential to be tested statistically. Subsequently, all of this fits with the positivist approach. Generally speaking, the methods utilised in this study are very appropriate for such a philosophy. Moreover, the positivist method has been widely used by researchers in the area of technology adoption and acceptance, who have applied this scientific technique for collecting data (Orlikowski and Baroudi, 1991).

6.3 Research Approach

Understanding the philosophical assumptions and the strategy of investigation which can be used to explore said assumptions is very significant when it comes to choosing specific research approaches which, in turn, encourage the method in practice (Creswell, 2003). There are two approaches to conducting research, namely deduction and induction (Myers, 1997). The deductive method is usually implemented in scientific research which addresses a positivist situation, whereas the inductive method is usually in line with the interpretive paradigm. The deduction method is based on developing a philosophy and hypothesis, and then planning a research approach to test said hypothesis (Myers, 1997). With the deductive approach, a researcher uses literature to categorise theories and thoughts. On the other hand, the inductive method is usually

employed in the interpretivism paradigm; the data is collected first, following which the theory is built as a consequence of the data analysis (Saunders et al., 2009). As a result, this research studied the existing literature on adopting technology and security cloud computing in order to propose a framework and to identify factors that affect cloud adoption. After proposing a framework for security cloud adoption, data was collected with a view to extracting the factors that promote or hinder cloud adoption in Saudi government organisations. In this research, a deductive method has been chosen; this was considered the most suitable approach given that it involves conducting an in-depth investigation into relationships between factors and also testing the relationships of the hypothesised.

6.4 Research Strategy

Before classifying which research strategy is most applicable to the research, the purpose of the research should be identified. The selection of a suitable research strategy is a critical decision within any research project. There exist many strategies which are used in the field of social sciences and information technology; examples of these include experiment, survey, case study, action research, and grounded theory (Myers, 1997; Creswell, 2007). In any research, choosing a suitable strategy is a difficult task. The researcher must select the strategy that fits the research questions. Some of these approaches are clearly associated with a qualitative approach, and others with a quantitative approach. Most studies in the field of information system research depend on the strategies and procedures being appropriate to test the hypotheses (Saunders et al., 2009). In addition, the survey has been deemed one of the most commonly-used strategies in researchers related to adopting technology and practice at the individual level and organisational level (Creswell, 2003). The survey is a technique used to gather information to describe or explain an object, and helps scientists to measure the thinking of participants and their decisions regarding the events taking place. As a result, the survey is carefully chosen as the most appropriate strategy for this research.

6.5 Research Design

A research design is a strategy and construction of investigation used to find answers to research questions (Kerlinger, 1986). The research design supports scholars in answering research questions as validly, objectively, accurately and economically as possible. After defining the philosophical assumptions and research approach that direct this research, the research design section completes the presentation of the methodology used in this research by covering the areas connected to the design of the study. The most important thing in formulating a research design is that the researcher essentially thinks about how the chosen design will fit with the research questions that need to be answered.

There are three types of research design: exploratory, descriptive and explanatory (Cooper and Schindler, 2003). In this research, two research design methods were used, namely exploratory and explanatory. The exploratory research approach was implemented during the first stage of the research, and has been presented in previous chapters, which elaborated on the studying of existing literature and previous work, as well as the collecting of qualitative and quantitative data. The exploratory design approach assisted in simplifying problems regarding security in cloud adoption and helping to develop the study model of this research, alongside related factors. It also assisted in constructing the study hypotheses.

In the second stage of this research, an explanatory research methodology was applied in order to evaluate the relationships between the above-mentioned factors. With this explanatory approach, the data was collected using an instrument and used to evaluate the security cloud adoption framework, as well as to test the hypothesised relationships. The instrument strategy was deemed most appropriate for this research, as it allows for the in-depth investigation of relationships between factors; this, in turn, makes it possible to fully answer the main research question: “What is an appropriate framework with which to determine the influence of security factors on the adoption of cloud computing in the Saudi government context?” Added to this, the above-mentioned strategy can also answer the remaining sub-questions of this research, which are:

Q4: What are the relationship(s) among the security factors identified from factor analysis and structural equation modelling?

Q5: Which relationship(s) of security factors will affect the Saudi government organisations' decision to adopt the cloud computing services?

6.6 Population and Sample Size

There exist two sampling techniques: probability sampling and non-probability sampling (Cohen et al., 2011). Probability sampling is a common method that uses random selection (Cohen et al., 2011). Examples of probability sampling are simple random sampling, and stratified random sampling (Creswell, 2007). None-probability sampling does not require random selection; the selection of the sample is based on the decision of the researcher (Podsakoff et al., 2003). As collecting data from the entire population is impracticable, selecting the sample size of a study is essential. Thus, as the context of this study is security experts' behaviour in Saudi government organisations towards adopting cloud services, the research targets only Saudi experts. This sample was selected using the accidental sampling technique, which made things easier and faster given the time frame compared with using other sampling techniques. Accidental sampling is a non-probability sampling technique, whereby the participants' responses are based on their willingness and availability (Podsakoff et al., 2003).

This research investigated the security factors that influence an organisation's decision to adopt cloud computing in the Saudi Arabian government. Therefore, the target respondents of this study were IT and security experts in the government organisations of Saudi Arabia; these experts were deemed particularly suitable given their ability to gauge the existing conditions in their organisations and new information technology. Furthermore, they are also involved in the decision-making process alongside top management, the latter of which are often hard to reach.

Numerous researchers have been confused by the notion that there is no static number for sample size; however, an acceptable sample size is essential in order to certify the

reliability of the study and allow for the possibility of simplifying the results from the data collection (Saunders et al., 2009). In this case, the present study used factor analysis as an exploratory method, followed by Structural Equation Modelling (SEM). The reliability of factor analysis depends on the sample size. The common rule to apply to sample size is that a study has at least 10 to 15 participants per variable (Hill and Loch, 1998; Hair et al., 2010). The usual sample size for a study of this nature is approximately 200 (McDonald and Ho, 2002). Furthermore, the number of participants in this research was recognised based on the observation that greatest published articles which use SEM as a method of analysis are based on 200 cases. In total, 215 respondents participated in this study, all of whom were Saudi security experts.

6.7 Responses' Selection

With regard to responses' selection, the questionnaires were distributed in two ways. As the questionnaire was an electronic version, invitations were first sent by email to experts and certain specialists who met the instrument requirements. Second, the link to the questionnaire was posted on social networking websites, such as Saudi experts' security groups on Twitter and Facebook. With some organisations, authorisation had to be obtained in person, at which point the management (hopefully) agreed that their teams could participate in the study. The instrument used closed-ended questions, with a five-point Likert-type scale applied for all statements; the following ratings were used: "strongly agree = 5; agree = 4; neutral = 3; disagree = 2 and strongly disagree = 1". Revilla et al. (2014) suggested that, if researchers want to use scales, they should offer 5 answer categories rather than 7 or 11, because the latter yield data of a lower quality.

All the participants in this study were working in different IT departments in Saudi government organisations, such as the Saudi Food and Drug Authority, Ministry of Education, Ministry of Health, Ministry of Labour Saudi, Saudi Interior and King Abdul-Aziz University; in addition, they all had at least two years' experience in the cloud fields or security.

6.8 Data Analysis and the Goodness of Instrument

After finalising the design of the instrument, it was important to make sure that the statements in the instrument were accurately assessing the factors in the proposed framework. Therefore, reliability and validity tests were conducted to find perfect results from the instrument (Kaplan and Duchon, 1988). A few validity and reliability tests were conducted for the instrument by using pre-test and content validity techniques. In this research, validity was conducted before and after the data collection, and reliability was measured during the data collection process. In the following sections the reliability and validity of the instrument will be discussed in detail.

6.8.1 Validity of the instrument

After finishing the design of the instrument, it was essential to ensure that the statements in the instrument were assessing the factors. Validity confirms that the collected data and outcomes signify the existing situation correctly. Validation of the instrument is needed in order to certify that the statements of the questionnaire accurately measure the factors that they are supposed to measure (Bryman and Cramer, 2001). The instrument used in this research was measured using pre-test and content validity, which are further discussed in the following chapter.

6.8.2 Reliability of the Instrument

Reliability analysis is one of the most significant techniques when it comes to measuring an instrument's quality in order to subsequently ensure the accuracy and goodness of that instrument. Such analysis becomes particularly essential when there are multiple measurement statements for each variable (Bryman and Cramer, 2001). There are two approaches test of reliability that are generally used: internal consistency and test-retest reliability (Connolly, 2011). While these two approaches are interrelated, they measure the same variable.

- **Internal consistency:** is the level to which the items are consistent and internally reliable to a specific variable in their measurements.
- **Test-retest reliability:** the reliability of this test can be measured by executing the similar test with the similar group but at different times; the correlation between the two outcomes is the mark of reliability (Fink and Litwin, 2003).

This research used an internal consistency reliability test during the initial data analysis stage. It is mostly acknowledged that, when a concept has been operationally well defined, in that a measure of it has been proposed, the ensuing measurement device should be both reliable and valid. It is important to measure the quality of the statements in studies (their reliability), since there are multiple statements for each factor or sub-factor. The reliability measurement relates to the degree of consistency when it comes to measuring the various statements (Bryman and Cramer, 2001). Applying the reliability test to the statements supports the research's aim of examining said statements (Pallant, 2013). Moreover, reliability assessments are most effective when Likert scales (such as strongly agree, agree, disagree, and strongly disagree) are used to answer questions. As such, in this research, the reliability of the statements pertaining to the various factors was measured using Cronbach's alpha (Cronbach's α), which is the most popular method when it comes to conducting a test of reliability (Bryman and Cramer, 2001). In order to ensure the reliability of the research instrument, the Cronbach's alpha reliability test was used. Moreover, Cronbach's alpha values are dependent on the number of items on the scale. When the number of items on the scale is less than 10, Cronbach's alpha values can be quite small (Bryman and Cramer, 2001). Table 6-1 displays the reliability value range and the level of acceptance of the research, in relation to the literature review.

Table 6-1: Cronbach's Alpha Reliability Scores

Cronbach alpha	Level of Internal Consistency	References
$\alpha < 0.5$	Poor	(Hair et al., 2010; Bryman and Cramer, 2001).
$0.5 > \alpha \geq 0.5$	Acceptable	(Bryman and Cramer, 2001; Hair et al., 2010).
$0.8 > \alpha \geq 0.8$	Very Good	(Hair et al., 2010; Bryman and Cramer, 2001).
$\alpha \geq 0.9$	Excellent	(Pallant, 2013; Fink and Litwin, 2003).

In this research, the reliability was measured using Cronbach's alpha after collecting data through SPSS software to evaluate the inter-item correlation and item-to-total correlation values. The results will be discussed in the data analysis chapter. Moreover, this study used reliability test in the confirmatory analysis stage. Composite reliability, which is also called as construct reliability, was intended in order to test the reliability of the construct; this is a needed stage in the confirmatory analysis. The composite reliability result is illuminated in the next chapter in detail.

6.8.3 Missing Values

Missing data is a crucial concern during the data analysis stage, particularly when the instrument is the data collection technique being used. Before beginning the data analysis, the missing data have to be identified, and it must be established that the collected data is free of errors. Missing data is one of the difficulties that occur in any research that applies a questionnaire as a data collection instrument (Bryman, 2006). There exist various methods that can be applied in solving the missing data problem, but when conducting the application of SEM, it is suggested that the following methods be used:

- **Multiple imputations (MI):** MI is a statistical method that used by changing missing values with estimated values. Furthermore, producing values for missing values by using the MI approach may lead to bias, and potentially worthless results (Graham et al., 2007).
- **Full information maximum likelihood (FIML):** with this technique, the progression can be worked by estimating parameters straight from the raw data (Lin and Huang, 2008). This technique could have an emotional impact on the sample if there are any missing items in relation to the data size; such missing items could decrease the statistical power of the sample (King et al., 1998).
- **Listwise Deletion (LD):** LD is a technique in which any situation that comprises multiple or single missing data is eliminated from the analysis. This technique may influence the sample if there are any missing values in relation to the data

size; these missing items could reduce the statistical power of the sample (Hair et al., 2010).

- **Pairwise Deletion (PD):** This method takes into consideration all non-missing data as well as the PD method deleted subjects with missing data on each pair of variables used; in contrast to LD method which perform deletion to subjects with missing data on any variable (Finkelstein 2005, Graham et al., 2007).

It has been postulated that when less than 1% of the data is missing, this is considered small; moreover 1-5% is manageable, 5-15% requires advanced analysis, and above 15% may lead to confusion (King et al., 1998). With regard to this research, if there were any situations where more than 5% of the data was missing, this data was excluded from the analysis, while the survey was developed and managed carefully. The number of answers excluded from this research is stated in detail in the next chapter.

6.9 Factors Analysis Procedures

The starting point in factor analysis, as with other statistical techniques, is the research problem. The common goal of the factor analysis technique is to identify a way to summarise the information contained within a number of original variables into a smaller set of new, composite dimensions or various factors with a lower lack of information. Simply put, this analysis seeks to determine the substantial constructs or sets which it is assumed underlie the original variables (Hair et al., 2010). Factor analysis is conducted to identify the dimensions and significance of variables. It summarises the relationships between datasets and groups these variables accordingly. Moreover, factor analysis is also employed to minimise large sets of variables into smaller sets of underlying variables, which are referred to as a factor or category. Hair et al. (2010) summarised the main purpose of using factor analysis, as can be seen below:

- To identify underlying dimensions called factors, which describe the correlations among sets of variables.
- To assess factors which influence responses to observed variables.
- To achieve data reduction and scale development.

- To identify a new, smaller set of uncorrelated variables to replace the original set of correlated variables for subsequent analysis, such as Regression or Discriminant.

One of the primary deliverables of this research was to build a security model for the adoption of cloud computing in Saudi government organisations. Since no prior models exist in the literature, a model was built following exploratory and confirmatory factor analysis. This research involved two stages of model building: an exploratory stage, and a confirmatory stage. During the exploratory stage, Exploratory Factor Analysis (EFA) was applied in order to propose an initial model, while Confirmatory Factor Analysis (using Structural Equation Modelling) was used to validate and confirm the initial model in the confirmatory stage.

6.9.1 Exploratory Factor Analysis (EFA)

EFA is a data-driven approach which is generally used as an investigative technique to identify relationships among variables (Byrne, 2010). Exploratory factor analysis is defined as an orderly simplification of interrelated measures. EFA is usually employed to explore the possible underlying factor structure of a set of observed factors without imposing a preconceived structure on the outcome (Child, 1990). Subsequently, the procedures of factor analysis can be applied through the following processes (Suhr, 2006; Hair et al., 2010):

- Identifying objectives of factor analysis.
- Designing a factor analysis.
- Identifying assumptions in factor analysis.
- Deriving factors and assessing overall fit.
- Interpreting the factors.
- Validating factor analysis.

EFA is vital when it comes to defining underlying constructs for a set of measured variables. Another alternative in terms of identifying the appropriateness of the data for

factor analysis is to examine the strength of inter-correlations among the variables. Factor analysis should not proceed with variables that correlate very highly with other variables (Williams and Child, 2003). The IBM SPSS statistics 24 software is used to implement EFA. There are certain issues which must be taken into consideration when defining the appropriateness of the data: the sample size, data screening, and the strength of the relationships between the variables (Kaiser-Meyer-Olkin (KMO) measure), interpretation correlation, factor extraction, factor rotation, and the analysis of the factors. The latter of these is further discussed in the chapter concerning data analysis and the results of using SEM and factor analysis.

During the exploratory stage, exploratory factor analysis was used to examine the factors, propose the hypotheses, and build and confirm the initial model. This stage was followed by a confirmatory factor analysis to evaluate the extent to which the model fit the data. This was achieved by using Structural Equation Modelling, which is further discussed in the present chapter.

6.9.1.1 Factor Extraction

In factor analysis, 'factor extraction' involves defining the lowest number of factors (or categories) that can explain the interrelations of all the sets of variables. There are various approaches which can be used to extract the factors, e.g. principal component analysis (PCA), principal axis factoring, and maximum likelihood factoring (Suhr, 2006; Hair et al., 2010). The method that should be selected depends on the goal of the study.

In this research, during the first stage of model building, no prior relationship was assumed, and the model was built from scratch. As such, it was decided that principal component analysis (PCA) was more appropriate to use than factor analysis, in which relationships are assumed (Tabachnick and Fidell, 2007).

PCA is a default extraction technique in several popular statistical software packages e.g., SPSS, SAS and other packages with the same options. In addition, among the advantages of PCA is the fact that it determines the total variance and can provide an explanation for the maximum portion of the overall variance characterised in the original set of variables in SPSS (Pallant, 2007; Field, 2013).

Therefore, to conclude how many factors (or components) are extracted, eigenvalues (Kaiser's criterion) and scree plot are two sets of information that can be referred to (Nunnally, 1978).

Both methods were considered in this research, and the analysis process comprised two stages: a preliminary stage and a final stage. In the preliminary stage, only factors (or components) with eigenvalues above 1 were extracted. The scree plot test from this preliminary stage was used to decide on the correct number of factors (or components) to extract. Following this, in the final stage, the whole analysis was rerun with the chosen number of factors (or components) from the preliminary stage.

6.9.1.2 Factor Rotation

After confirming the number of factors to be retained, the next stage involved interpreting the variables loaded on these factors or components. Factor rotation is a process used to inspect the factor axes and thus obtain a simpler and pragmatically more significant solution (Hair et al., 2010). After the rotation is implemented, the loadings of the variables are maximised on one factor and minimised on the remaining factor. This procedure makes it possible to clearly identify the variables' clustering and their correlated factors (Williams and Child, 2003). There are two methods involved in rotating factors: orthogonal (e.g., varimax) and oblique (e.g., oblimin) (Pallant, 2007). In SPSS, a table called the component correlation matrix displays these correlations (Tabachnick and Fidell, 2012).

Factor rotation, and the aim of applying this technique, were discussed in the chapter detailing the research methodology of the validation study. In this research, in order to gauge which rotation methods were most suitable for the data analysis and to establish whether the assumption of independence could hold for the variables, both the orthogonal (varimax) and oblique (oblimin) techniques were applied.

The orthogonal rotation method is more appropriate when the relationship between the extracted factors (or components) is thought to be poor, while oblique rotation is more suitable when the relationship is strong (Hair et al., 2010). With oblique rotation,

the pattern matrix comprises the factor loading after the rotation, while the structure matrix defines the relationships between the variables.

The results of the factor rotation in this analysis clearly showed that factor rotation achieves a correlation matrix; in this study, factor rotation proved that the factors (or components) did have a relationship and that it cannot be assumed that these factors are independent, since the correlation matrix table showed that the factors were somewhat correlated.

Rotation supports the delivery of methods which make it possible to consider and interpret the factors. The interpretation of factors is generally accomplished using the pattern matrix. However, the structure matrix is beneficial when it comes to determining double examination and describing the relationship between the factors (Field, 2013).

Tabachnick and Fidell (2012) suggested that researchers may experiment with different combinations of extractions and rotations and select the combination that provides the most interpretable solution. However, it should be borne in mind that other researchers have recommended using orthogonal rotation only if there is no expected relationship between the factors. Otherwise, these suggest using oblique rotation. In addition, another string of researchers have recommended using orthogonal rotation, as it provides a simpler solution, and is commonly used by researchers; of particular note here is the debate among researchers surrounding whether orthogonal and oblique rotations generate similar results.

6.9.2 Confirmatory Factor Analysis (CFA)

The CFA technique assists with testing the hypotheses and the existence of relationships between the observed variables and their underlying latent constructs (Byrne, 2010). With this approach, the researcher uses his/her knowledge of theory, empirical research, or both, and predicts the relationship pattern a priori, before then testing the hypotheses statistically. One of the most popular techniques for researchers across disciplines, and particularly for researchers in the social sciences, is Structural Equation

Modelling; this is a special component of CFA, and is further discussed in the following section.

6.9.2.1 Structural Equation Modelling (SEM)

Structural Equation Modelling (SEM) has become one of the most popular techniques for researchers across disciplines, and particularly for researchers in the social sciences (Byrne, 2010). The term Structural Equation Modelling has been used to explain a large number of statistical models which are applied to evaluate the validity of necessary theories using experimental data. Moreover, SEM is a statistical analysis technique that is used to analyse structural relationships; this is considered one of the major benefits of using SEM (Choudrie and Ghinea, 2013). The SME technique is a combination of factor analysis and multiple regression analysis, and is employed to analyse the structural relationship between measured variables and latent constructs (Choudrie and Ghinea, 2013). Subsequently, in this research, the preference was to use the SEM technique, as it represents a conceptually-attractive way to test the theory and define how well the theory fits according to the data. SEM comprises six important stages: developing the model, constructing the path diagram, connecting the relationships, building the measurement model, modifying the measurement model and, finally, model fit (Hair et al., 2010). In order to meet the unique terms and processes of SEM, Figure 6-2 illustrates the above-mentioned processes.

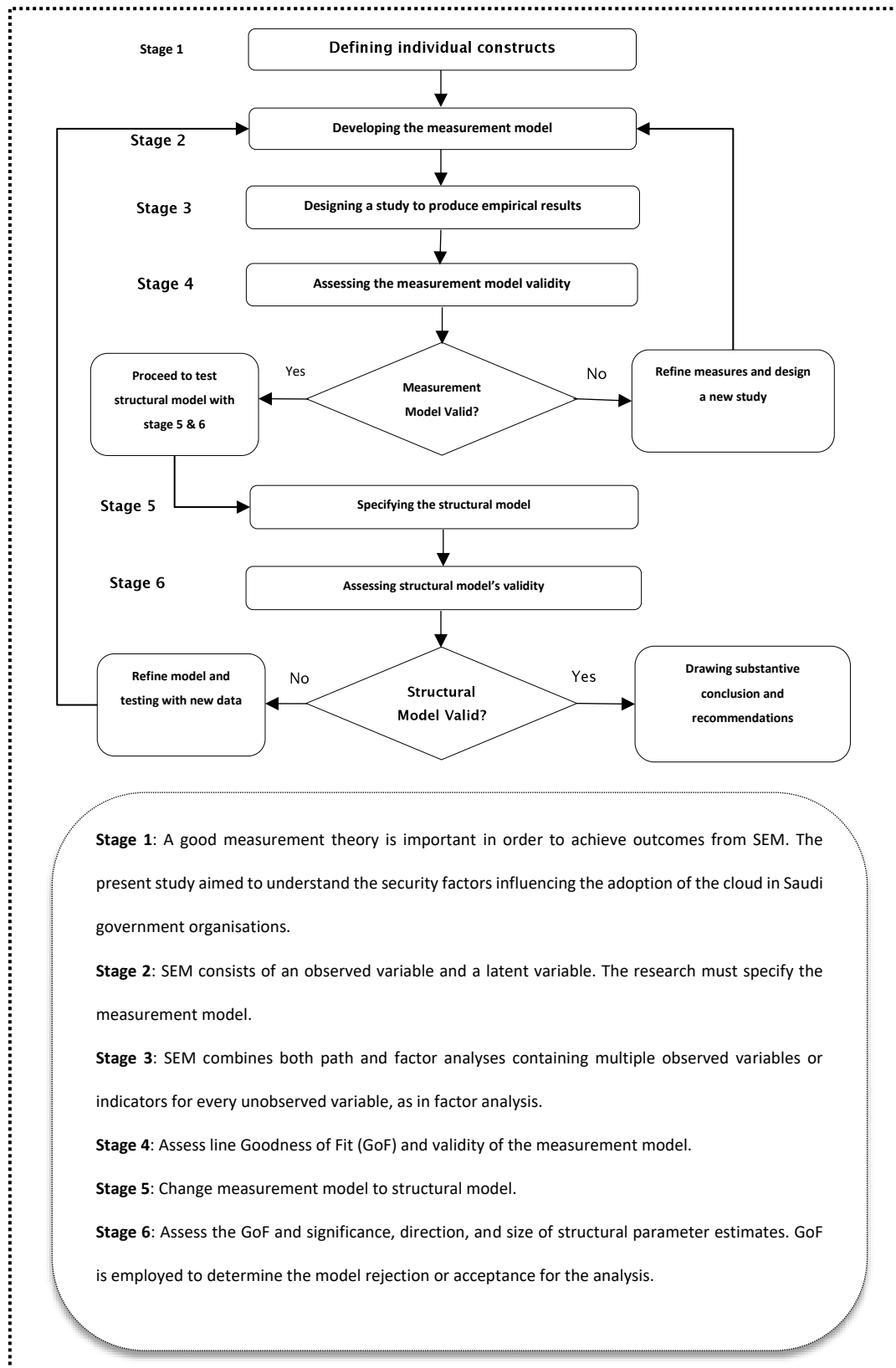


Figure 6-2: Process of Stages for Structural Equation Modelling (Hair et al., 2010)

SEM consists of a series of statistical methods that make it possible to identify complex relationships between one or more independent variable, and one or more dependent variable (Byrne, 2010). As a statistical tool, it can be characterised as an extension of general linear modelling (GLM) processes, including the ANOVA and multiple regression analysis. While SEM is considered a special component of confirmatory factor analysis, it is also known as an a priori theory approach which is most often used to determine the extent to which a previously-established theory regarding relationships among certain variables is supported by empirical data (Ockey, 2014). There are numerous applications that can be used to run SEM analysis, including, but not limited to, AMOS from IBM, Mplus, LISREL, and EQS. Analysis of Moment Structures (AMOS) was used in this research, since its structures met the requirements of the research and also due to its availability.

Therefore, SEM was carefully chosen for this study to conserve parsimony in the proposed model and because of its strength in testing research hypotheses. The proposed framework was produced in AMOS, following which the data was introduced to the program. This analysis revealed whether the data fit the model. In this research, as the links between the proposed variables were not determined, it was deemed appropriate to apply EFA; in contrast, CFA is designed to be used when a researcher has a basic knowledge of how the model is set out. However, the researcher must consider certain issues when applying the SEM, and how these issues affect the credibility of the outcome. The most important considerations when using SEM are:

- The hypothesis is tested
- The sufficient sample size is determined
- Multivariate Normality
- Parameters Identification
- Missing Data
- Statistical tests

6.9.2.2 Structural Model Goodness of fit (GoF) Statistics in SEM

Goodness of Fit (GoF) is one of the most important tools when it comes to testing a proposed model and determining its goodness of fit (Hair et al., 2010). GoF is an important step in SEM, and is regularly used to assess how well the proposed model fits with the collected data (Acuna and Rodriguez, 2004). The results of GoF are assessed by comparing the experimental data (sample covariance matrix) with the proposed hypotheses (predicted model covariance). It has been pointed out that the hypothesised model is tested by the researcher using sample data (Acuna and Rodriguez, 2004).

Furthermore, the Maximum Likelihood (ML) estimation approach is preferred to calculate the GoF indices using AMOS (version 24) (Hair et al., 2010). In this study, in order to estimate the GoF outcome, a chi-square (χ^2) test was applied; this is a vital a statistical test in SEM that estimates the variances between the sample covariance matrix and the predicted model covariance matrix (Khine, 2013). As the assessment of chi-square (χ^2) is affected by sample size, normed chi-square was considered in this research; this involves dividing the value of the chi-square (χ^2) by degrees of freedom (df) computed as (χ^2/df) (Kline, 2011). Hair et al. (2010) suggested that, in order to achieve a good fitting model when the study sample size is less than 250, the value of the normed chi-square must be less than 3. This research sample size in this study was 215.

However, various information system researchers have maintained that chi-square and normed chi-square tests are sufficient proof of model fit; moreover, it has been indicated that providing two to three fit indicators to chi-square is acceptable and convenient (Hair et al., 2010). Many statistical tests can be used to determine the adequacy of the model in terms of fitting the data. In summary, it can be stated that the most frequently-suggested indices are: Comparative Fit Index (CFI), the Goodness of Fit Index (GFI), Root Mean Square Residual (RMR), Standardised Root Mean Square Residual (SRMR), and the Root Mean Square Error of Approximation (RMSEA). All statistics which fit the indexes mentioned above range from 0 to 1.00. Chapter 8 will present the results and accepted values of these statistical tests in detail.

6.9.2.3 The Minimum Sample Size and the Response Rate

Before distributing the designed instrument, it was essential to recognise the target and calculate the sample size. The minimum sample size is thought to produce a reliable and acceptable research outcome. The target group in this research comprised IT security experts from Saudi government organisations. Determining sample size requirements for structural equation modelling is a challenge for researchers. One particularly noteworthy strength of SEM is its flexibility; this quality permits the examination of complex suggestions, using many types of data (e.g., categorical, dimensional, censored, count variables). Such a quality also allows for assessments across alternative models (Byrne, 2010). Considering the sufficient sample size calculations, it should be noted that there are a number of rules of thumb when it comes to the appropriate sample size for both exploratory and confirmatory factor analysis.

A common recommendation that has been used by researchers is that a research sample should comprise at least 200 participants, with 10 cases per factor (Wolf et al., 2013). Based on this recommendation, it is important to consider the number of factors in this study's instrument (20 factors including the factor of Decision to Adopt the Cloud); hence, the number of participants in this research should be no less than 200. In the present research, to obtain valid results, the number of participants was increased to 215 as a contingency plan, in case of missing data.

6.10 Ethics Approval Consideration

As the research was conducted in an academic setting, ethical matters were considered seriously. It is the ethical obligation of a researcher to conduct research honestly and with integrity (Adams et al., 2007). As suggested by Adams et al. (2007), ethical strategies were followed at a number of points throughout this research, e.g., planning the study, piloting the study, analysing the data and writing the results. More essentially, ethical strategies delivered by the university, where the research was conducted, were followed during the entire process. As the questionnaire was part of this research,

before distributing said questionnaire to participants, it was essential to verify and plan the procedure, so that it met the ethical requirements of research. The ethical requirements of this research were approved by the Ethics Committee at the University of Southampton: reference number 26694.

6.11 Summary

This chapter clarified the methods which were applied in the present research. In the first two sections, the research philosophies and approaches were discussed. In the domain of methodology, four main philosophies were identified, namely positivism, realism, pragmatism and interpretivism. This research implemented a positivist philosophical, as the subject of the study was scientific in nature. This pattern also supports neutral views about reality. A deductive method was used in the study, as this was in line with the positivist philosophy. The present research also adopted quantitative methods, as these were consistent with the positivism philosophy, deductive approach, and the research topic.

It was deemed that the most suitable approaches for this stage of the research were an instrument strategy and the process of development, both of which have been described in detail. The applicable sample size was conducted to be greater than 200 samples. Moreover, this chapter provided a detailed examination of the procedure of developing and designing the instrument.

Following this, the next section illustrated, in detail, the Goodness of Fit instrument, with a discussion regarding the validation of the reliability and validity of this instrument in order to obtain accurate results. Pre-test and content validity were used to validate the instrument. The pre-test and content validity were proved before collecting data in order to ensure that the instrument being used in this research accurately measured what it was supposed to measure.

By referring to the research case, a confirmatory study was first undertaken to confirm the proposed factors, as no previous study has addressed this subject area. Testing the model and hypothesis was the main objective of this stage, and both were analysed

using Structural Equation Modelling (SEM) following the use of correlation analysis and factor analysis.

This chapter also explained and discussed the utilisation of SEM to evaluate the model, while the main benefits of SEM were identified, i.e., ability to deal with multi-variables and identify relationships among these multi-variables. At this point, it must be stated that SEM is mostly a confirmatory analysis method, and thus it was necessary to test whether the proposed model was valid.

The procedures used to analyse the data were also discussed in this chapter, while the research ethics were examined. The next chapter presents the details of the data analysis and the results.

Chapter 7: Results of the Development and Validation of the Instrument

The previous chapter identified and explained the research methodology that was applied for the second stage of this research. As seen in Chapter 5, the results of this study confirmed the security cloud computing adoption Framework. The result of this confirmatory study was used to confirm that the security factors of the framework were theoretically sound. Based on this result, an instrument was developed to survey Saudi government organisations and to explore and confirm the relationships between the confirmed factors in the second stage of this research. This chapter presents the development and validation of an instrument which was used to evaluate and validate the security cloud adoption model of this study by addressing the following research question: 'What is the appropriate instrument to evaluate security factors in the cloud adoption framework and how can the instrument be validated?'

In addition, a discussion of the results and findings of the instrument validation study is provided. The instrument validation went through a pre-test stage to make sure the content validity. After the pre-test stage, the validation study sought to establish the validity and reliability of each factor in the instrument, and how they related to each other. Correlation was applied to identify the relationships between the latent variables. Finally, the instrument reliability that used in this research is also presented in detail, and summarised in the present chapter.

7.1 Instrument Development and Design

Instruments are methods used to collect information with a view to describing, comparing or explaining an objective (Clifford et al., 2010). The purpose of an instrument is to obtain accurate and complete information about a research question (Malhotra and Galletta, 1999). This can be achieved by producing a carefully-designed survey that ensures reliable responses from a chosen sample (Myers, 1997). A self-

administered questionnaire was designed in order to answer the research questions and to test the hypothesis regarding the relationships being investigated (Bryman, 2006). The preparation of the instrument's content was the first step in stage two of this research. The more attention which is given to the development of the research instrument, the easier it is to ensure that the research is valid (Cooper and Schindler, 2003). The instrument was used to collect data regarding the security factors that have an effect on the adoption of cloud computing in KSA government organisations. Literature was reviewed in order to develop the instrument statements, which were related to cloud security factors affecting KSA government organisations' decision to adopt the cloud. The instrument was designed to evaluate the factors of the security cloud adoption framework.

In terms of the security cloud framework, 20 factors, including the decision to adopt the cloud factor, were selected for inclusion in order to measure the security factors model. These factors were: *Insecure Interfaces, Shared Technology, Account or Service Hijacking, Malicious Insider Risks, Failure of Compliance with Regulations, Data Ownership, Service and Data Integration, Data Leakage, Failure of Client-side Encryption, Trust, Security Culture, Privacy, Smart Scalable Security Benefits, Cutting-edge Cloud Security Marketing, Advance Security Mechanism, Standardised Security Interfaces, Cloud Security Auditing, Service Level Agreement, SLA Audit Enforcement, Resource Concentration, and Decision to Adopt the Cloud*). In the next chapter, the instrument validation is further deliberated in detail.

The structure and items of the instrument were designed to validate the security factors in the cloud adoption framework. It was administered in English. The instrument began with a welcome, a brief introduction to the research, and a summary of the aim of the questionnaires. The instrument was divided into two parts.

Part 1: Demographic Information: involved general information such as the experience of the expert and their government organisation's decision in terms of adopting and not adopting cloud services. This part was significant, as it gave the investigator an overview of information that might be required in the group evaluation.

Part 2: Instrument measuring items questions: these questions sought to establish the extent to which the respondent agreed with the effect of the following statements on the adoption of cloud computing services in their government organisations.

The instrument was concerned with empirically measuring the suggested factors and their relationships. Therefore, the literature was revisited as a reference, in order to design the appropriate measuring items for the research instrument. These statements were improved to fit this research and the KSA government organisations context. Table 7-1 shows the number of constructs and their items, which were used to measure the variables in this research; the sources from which these items were derived are also specified.

Table 7-1: Measurement Items of Research Variables

Construct	Code	Number of Item	Sources
Insecure Interfaces	II	3 items	(Babu et al., 2010), (Cloud Security Alliance, 2013) ,(Elena and Johnson, 2015)
Shared Technology	ST	3 items	(Paquette et al., 2010), (Cloud Security Alliance, 2013), (Babu et al., 2010)
Account or Service Hijacking	AH	4 items	(Paquette et al., 2010), (Cloud Security Alliance, 2013), (Babu et al., 2010), (Elena and Johnson, 2015)
Malicious Insider Risks	MI	3 items	(Babu et al., 2010), (Cloud Security Alliance, 2013) ,(Elena and Johnson, 2015)
Failure of Compliance with Regulations	CR	4 items	(Paquette et al., 2010), (Cloud Security Alliance, 2013), (Babu et al., 2010), (Alkhater et al., 2015)
Data Ownership	DO	5 items	(Babu et al., 2010), (Cloud Security Alliance, 2013) ,(Elena and Johnson, 2015)
Service and Data Integration	SDI	3 items	(Babu et al., 2010), (Cloud Security Alliance, 2013) ,(Elena and Johnson, 2015)
Data Leakage	DL	4 items	(Babu et al., 2010), (Cloud Security Alliance, 2013) ,(Elena and Johnson, 2015)
Failure of Client-side Encryption	CSE	3 items	Added by the researcher and Experts
Trust	TR	3 items	(Khan and Malluhi, 2010), (Alkhater et al., 2015)
Security Culture	SC	3 items	Added by the researcher and experts

Construct	Code	Number of Item	Sources
Privacy	PR	3 items	(Featherman and Pavlou, 2003), (Sen, 2013), (Alkhater et al., 2015)
Smart Scalable Security Benefits	SS	4 items	(Catteddu and Hogben, 2009), (Cloud Security Alliance, 2013)
Cutting-edge Cloud Security Marketing	CE	3 items	(Catteddu and Hogben, 2009), (Cloud Security Alliance, 2013)
Advance Security Mechanism	AS	3 items	(Cloud Security Alliance, 2013), (Catteddu and Hogben, 2009),
Standardised Security Interfaces	SSI	4 items	(Catteddu and Hogben, 2009), (Cloud Security Alliance, 2013)
Cloud Security Auditing	CS	3 items	(Catteddu and Hogben, 2009), (Cloud Security Alliance, 2013), (Cloud Security Alliance, 2013)
Service Level Agreement (SLA) Audit Enforcement	SLA	3 items	(Catteddu and Hogben, 2009), (Cloud Security Alliance, 2013)
Resource Concentration	RC	3 items	(Cloud Security Alliance, 2013), (Catteddu and Hogben, 2009),
Decision to Adopt the Cloud	DAC	4 items	Added by the researcher and Experts
Total: 20 Constructs		67 Items	

7.2 Validity of the Instrument

After completing the design and development of the instrument, it was essential to make sure that the items in the instrument were evaluating the constructs. The instrument that used in this study was measured using two tests validation, namely pre-test and content validity.

7.2.1 The Instrument Pre-test

A pre-test is a mini version of the main survey, and is used to assess the reliability and validity of an instrument (Straub et al., 2004). Thus, in this test, the same steps as those taken in the main study must be applied to test the instrument in a real context. This step defines the instrument and its measures, while also developing the study procedures (Cooper and Schindler, 2003).

The instrument was pre-tested with seven academic researchers and security experts, all of whom had features similar to those of the sample group participants. The experts were carefully chosen in order to verify content validity through the pre-test. This stage is designed to ensure that the instrument is clear and understandable for the

respondents (Sekaran, 2003). The test involved four experts from IT security in KSA security groups, while three experts were from the University of Southampton from computer science group researchers. The aims of the pre-test were to evaluate whether:

- All items were applicable and sufficient in examining the concept being studied.
- All questions' wording, response format, guidelines, instrument size, and layout were suitable.
- The instrument as a whole was easy to read and understandable.

The pre-test participants provided a number of comments, and the questions were edited according to their comments. The changes made to the original instrument after pre-testing included: selecting a sufficient number of items to represent a factor, adopting player suitable terms and using a layout that would be easy for the participants to read and that would make the instrument easy to distribute during the experiment. The participant's respondents from the pre-test supported the content of the instrument.

7.2.2 Content Validity of the Instrument

The most important stage of developing the instrument was to establish the content validity of the measuring items for each construct before collecting the data. Had content validity not been undertaken, the instrument may not have been usable and the results of the study may have been invalid (Garver, 1999). Content validity mentions to how perfectly the instrument demonstrates the construct of the statements; this kind of validity depends on the understanding of specialists, and on the specific content filed (Cronbach and Shavelson, 2004). Content validity refers to *"how appropriate items or scales seem to a set of reviewers who have some knowledge of the subject matter"* (Fink, 2003). Straub et al. (2004) recommended that using statements which have been validated in the literature is essential if they are available. However, in this research, the statements from the literature were adopted and improved to suit the existing research objectives.

The two recommended steps of content validity were used in order to validate the instrument's content. These two steps are: the development stage and the judgement quantification stage (Lynn, 1986). The development stage starts with measuring the aim of the instrument and identifying the full content scope. This stage can be achieved through the use of a literature review and by consulting the views of experts.

The second stage is judgment quantification, which comprises two conceptions: the content of all items displayed is valid, and the content of the developed instrument is valid for the research objective. Lynn (1986) recommended that a minimum number of five experts ought to be used; however, this number may depend on the availability of such experts.

To validate the research instrument, seven experts with experience in instrument design were asked to assess the instrument content. A printed copy of the questionnaire, as well as a brief background of the research, was sent to them. Some changes in the measures were recommended to improve the instrument. Thus, in order to make sure content validity, the experts were asked separately to deliver feedback and recommendations on the instrument. The first step of judgment quantification involved a two-hour meeting with three researchers. During their review, a few typographical mistakes were removed and improvements were made to some statements not clear. Each expert answered the questions and responded to each statement. Following this, the new version of the instrument was ready to be shown to the next four security experts. In the following step of the judgment quantification, it was managed using the same procedure; this involved an online face-to-face Skype video meeting with Saudi security experts. The modifications to the questions were improved. Overall, 67 items were reformulated.

7.2.3 Results of Content Validity Ratio (CVR)

The content validity ratio (CVR) was used to assess the results of the instrument's content validity test, based on the thoughts of the seven experts who participated in the judgment quantification; the statistical significance level for each factor was also assessed (Lawshe, 1975). At this point, the results of the content validity test for the

instrument were in hand, thanks to the seven experts who participated in the judgment quantification; this yielded a statistical significance level for each factor. The significance levels were assessed using the content validity ratio (CVR) (Lawshe, 1975).

CVR is a quantitative method used to establish content validity. With the quantitative content validity method, confidence is kept in selecting the most significant and accurate content in an instrument, which is measured using the content validity ratio (CVR) (Ayre and Scally, 2014). In this way, the experts are demanded to identify whether or not an item is essential for operating a concept in a set of items. The items deemed 'Essential' by the experts were calculated, as presented in Table 7-7-2. The evaluation criteria of the items/scale were as follows:

- **Essential:** The question is necessary to define the security factors in cloud computing adoption. It must be involved and, if not involved, would affect the factors negatively.
- **Useful but not essential:** The question may be valuable but NOT necessary to define the factors in cloud computing adoption.
- **Not Necessary:** The question is NOT obligatory in terms of defining the security factors in cloud computing adoption. It does NOT need to be involved, and if involved, would NOT affect the factors.

Consequently, the responses of the experts were gathered, and the items which the experts deemed 'Essential' were calculated using CVR formula (see equation 1) as follows:

$$CVR = (N_e - N/2) / (N/2) \quad (1)$$

Where N_e is the number of experts that deemed the item to be 'essential', and N is the total number of participating experts. For the CVR to be considered important, the level of agreement among experts had to be more than 50% agreement provides some guarantee of content validity (Ayre and Scally, 2014). For example, if the CVR was bigger than 0.50, the item in the instrument with an acceptable level of statistical significance

was accepted and items with a significance level of lower than 0.50 were considered not significant (Ayre and Scally, 2014; Lynn, 1986).

The results showed that, from a pool of 67 items, only 62 items were statistically significant at the range of more than 0.50, while five of the items were insignificant because they were lower than 0.50, and thus were removed from the instrument. Consequently, this Content Validity Ratio identified that the security items of the cloud computing adoption framework had acceptable content validity, thus meaning that the items are capable of measuring the model being studied (Ayre and Scally, 2014). After these experiments, 30 security experts were invited to participate in this research. Slight modifications to the final design of the instrument were made upon receiving the feedback. The modifications were made to the original instrument and the final instrument was developed.

Table 7-7-2: Content Validity Ratio among Items of the Instrument

Construct	Total of items	Significant Items	CVR item 1	CVR item 2	CVR item 3	CVR item 4	CVR item 5	Average CRV
II	3 items	3 items	0.7	1.00	1.00	-	-	0.90
ST	3 items	3 items	0.7	1.00	0.7	-	-	0.81
AH	4 items	3 items	0.7	1.00	0.7	0.4	-	0.71
MI	3 items	3 items	0.7	0.7	0.7	-	-	0.71
CR	4 items	3 items	1.00	1.00	0.7	0.1	-	0.90
DO	5 items	4 items	0.7	1.00	1.00	1.00	0.1	0.77
SDI	3 items	3 items	0.7	0.7	0.7	-	-	0.71
DL	4 items	3 items	1.00	1.00	1.00	0.4	-	0.86
CSE	3 items	3 items	0.7	1.00	0.7	-	-	0.81
TR	3 items	3 items	0.7	0.7	1.00	-	-	0.81
SC	3 items	3 items	1.00	1.00	0.7	-	-	0.90
PR	3 items	3 items	0.7	0.7	0.7	-	-	0.71
SS	4 items	3 items	1.00	0.7	0.7	0.1	0.4	0.64
CE	3 items	3 items	0.7	0.7	1.00	-	-	0.81
AS	3 items	3 items	1.00	1.00	0.7	-	-	0.90
SSI	4 items	3 items	1.00	0.7	0.7	0.1	-	0.64
CS	3 items	3 items	0.7	0.7	1.00	-	-	0.90
SLA	3 items	3 items	1.00	0.7	0.7	-	-	0.81
RC	3 items	3 items	0.7	0.7	0.7	-	-	0.71
DAC	4 items	4 items	0.7	1.00	0.7	1.00	-	0.86
Total	67	62						

7.3 Instrument Validation

The purpose of the instrument validation study is to explore the relationship between all factors and items, and the scale as a whole. The improved instrument was distributed to a sample of participants, and their responses were analysed to establish the instrument's reliability.

Statisticians have stated that a sample size of 30 is adequate, as this is the value put forth in the Central Limit Theorem (Field, 2013). A total of 30 security experts were asked to participate in the research. The goal was for the respondents to state that the instrument was clear and understandable. In addition, the purpose of the respondents validated the content of the instrument. During the valuation, the security experts also delivered a number of recommendations. The recommendations commonly related to wording and the building of the sentences. The response items (5 (strongly agree) to 1 (strongly disagree) were deemed to be applicable. These minor modifications to the final design of the instrument and the modifications made to the original instrument are illustrated in Table 7-3.

Table 7-3: Validated Questionnaire's Items

Construct	Code	Items
Insecure interfaces	II1	Insecure application interfaces have an impact on the decision to adopt cloud services.
	II2	By understanding the dependency chain associated with secure interfaces, you can reduce the risks in adopting cloud services.
	II3	Awareness of the risks of insecure application interfaces affects the decision of adopting cloud services.
Shared technology	ST1	Secure shared technology affects the adoption of cloud services.
	ST2	Having a high quality of service in sharing technology would encourage us to use cloud computing.
	ST3	Some applications may be designed without using trusted computing practices, depending on the type of risks associated with the shared technology which affects the organisation's decision to adopt the cloud.
Account hijacking	AH1	It is important to be aware of account hijacking risks while adopting cloud services.

Construct	Code	Items
	AH2	Account hijacking is considered to be one of the major risks in cloud services that affect the decision to adopt the cloud.
	AH3	Stolen identities, one of the risks of service hijacking, may affect the decision to adopt cloud services.
Malicious insiders	MI1	Without full knowledge and control, government organisations will be at risk of malicious insider attacks.
	MI2	Malicious insider risks can affect the confidentiality, integrity, and availability of the government organisation's data.
	MI3	Saudi organisations should have knowledge about cloud providers' measures to avoid the risk of a malicious insider.
Failure to Comply with Regulations	CR1	Compliance with regulations affects Saudi government organisations' decision to use cloud services.
	CR2	Current laws and regulations in Saudi government organisations are not sufficient to protect information stored on the cloud.
	CR3	It is necessary that cloud computing regulations comply with Saudi Arabia laws.
Data ownership	DO1	Data ownership affects Saudi government organisations' decision to use cloud services.
	DO2	In order to reduce risks associated with Data Ownership, ownership of data should be authorised while adopting cloud services.
	DO3	The ownership of data should be exclusive when adopting the cloud.
	DO4	Data ownership terms should be clearly stated in the services level agreement.
Service and data integration	SDI1	Data integration affects Saudi government organisations' decision to adopt cloud services.
	SDI2	Integration of Saudi government applications with cloud services presents a challenge for the adoption of the cloud.
	SDI3	Unsecured data is more susceptible to interception while being transmitted in the cloud.
Data leakage	DL1	The fear of leaking Saudi government data affects the decision to adopt the cloud.
	DL2	Non-disclosure of data leakage events on the cloud provider raise concerns in Saudi government organisations.
	DL3	In general, data leakage risks hindering Saudi organisations' adoption of the cloud.
Failure of Client-side encryption	CSE1	Client-side encryption affects Saudi government organisations' decision to use cloud services.
	CSE2	Saudi organisations should be aware of client-side encryption while it plays an important role in data protection.
	CSE3	The organisations feel that the client-side encryption risks outweigh the benefits of adopting the cloud services.
Trust	TR1	Trust affects Saudi government organisations' decision to use cloud services.

Construct	Code	Items
	TR2	Access of third-parties to an organisation's data may raise security concerns and affect the adoption of the cloud.
	TR3	Storing our organisation's data under third-party control is one of our concerns related to adopting the cloud.
Security Culture	SC1	Security culture affects Saudi government organisations' decision to use cloud services.
	SC2	Security culture affects the execution of information security policies within government organisations.
	SC3	Organisations would be more confident in using cloud services if the provider was based in Saudi Arabia.
Privacy	PR1	Privacy concerns affect the government organisations' decision to use cloud services.
	PR2	Government organisations would be more confident to use cloud services if the privacy of the information was guaranteed.
	PR3	Access to personal information by third-party organisations may raise privacy concerns and affect the decision to use the cloud.
Smart Scalable security benefits	SS1	Smart scalable security benefits affect government organisations' decision to adopt cloud services.
	SS2	The ability to extend the security features in the edges network encourages the government organisations to adopt the cloud.
	SS3	Smart scalable to multiple locations security benefits drive the government organisations to adopt the cloud.
Cutting-edge security market	CE1	Cutting-edge cloud security marketing affects government organisations' decision to adopt cloud services.
	CE2	Saudi organisations should consider the cutting-edge benefits of cloud security marketing while adopting the cloud services.
	CE3	Cloud security marketing services affect the adoption of the cloud as they provide solutions to critical problems facing organisations and support remote workforces.
Advanced security mechanism	AS1	Advanced security mechanisms benefits affect government organisations' decision to adopt cloud services.
	AS2	Having sufficient support from the cloud provider in the form of an advance security mechanism would encourage the organisation to use cloud services.
	AS3	With an advance security mechanism, it is necessary to have adequate technical support from the cloud provider before and after adopting cloud services.
Standardised security interfaces	SSI1	Implementation of the standardised security interface features affects government organisations' decision to adopt cloud services.
	SSI2	Saudi organisations' awareness of cloud interfaces security standards benefits (cost reduction), would encourage them to adopt the cloud.

Construct	Code	Items
	SSI3	Standardised security interfaces influence the adoption of the cloud since they can ease the organisations' ability to change from one provider to another quickly.
Cloud security auditing	CS1	Cloud security auditing affects government organisations' decision to adopt cloud services.
	CS2	Saudi organisations' knowledge of cloud security auditing benefits, such as pay as you go auditing, drives them to adopt the cloud.
	CS3	The cloud scalable auditing feature influences the decision to adopt the cloud in Saudi organisations.
SLA Audit Enforcement	SLA1	Enforcing audit terms and conditions in the service level agreement by Saudi organisations would promote the cloud adoption decision.
	SLA2	Cloud providers' compliance with Saudi regulations audit requirements helps the Saudi organisations to adopt their cloud services.
	SLA3	Clear stating of audit responsibilities by both the Saudi organisation and the cloud provider influences the decision of adopting the cloud.
Decision to adopt the cloud	DAC1	It is likely that Saudi organisations will take steps to adopt cloud computing in the future.
	DAC2	Saudi organisations decide to adopt cloud computing.
	DAC3	I think, in the near future, most of the Saudi government organisations are going to decide to adopt the cloud services.
	DAC4	I feel comfortable recommending the adoption of the cloud to my organisation.

7.3.1 Correlations Analysis of the Instrument

Correlation analysis is used to understand the relationship between factors, and can be used to define the strengths and direction of a linear relationship between two variables (Cohen, 1988). Moreover, correlations analysis displays the value of the correlation coefficient. This can be ranged from -1 to +1, and the sign delivers the direction of the relationship; all produce a statistic that ranges from -1.00, indicating a perfect negative correlation, to +1, indicating a good positive correlation. A value of 0 specifies no correlation at all. Cohen (2011) alluded to the strength of the coefficient correlation value, as shown in Table 7-4. In this study, Pearson's correlation coefficient method was used, and the guidelines below were followed in the correlation analysis.

Table 7-4: Strength for Correlation Coefficient (Cohen et al., 2011)

Range of Correlation Coefficient	Strength of Relationship
0.50 to 1.00	Large
0.30 to 0.49	Medium
0.10 to 0.29	Small

7.3.2 Correlation among Security Factors

The items in each factor were calculated, while the mean for each category was found later on. Following this, the variables concerned were entered into the SPSS statistic software in order to obtain the correlation. The correlation matrix displays the strength of the relationship among factors in this section. In Table 7-5, each factor is represented by an abbreviation (to make it simpler):

Table 7-5: Abbreviation Represented for Each Factor

Abbreviation	Factor	Abbreviation	Factor
II	Insecure Interfaces	SC	Security Culture
ST	Shared technology	PR	Privacy
AH	Account or Service Hijacking	SS	Smart scalable security benefits
MI	Malicious insider risks	CE	Cutting-edge cloud security marketing
CR	Failure of compliance with regulations	AS	Advance security mechanism
DO	Data ownership	SSI	Standardised Security interfaces
SDI	Service and data integration	CS	Cloud security auditing
DL	Data leakage	SLA	SLA Audit Enforcement
CSE	Failure of client-side encryption	RC	Resource concentration
TR	Trust	DAC	Decision to adopt the cloud

The results of the correlation test for the security factors show the statistically significant correlations for the security factors associated to this study, as presented in Table 7-6.

The correlation results for the security factors are summarised as:

- Correlation of Insecure Interfaces (II) is statistically significant and correlated with Shared Technology (ST), $r(30) = .646$ and Service and data integration (SDI) $r(30) = .467$, (both $p < 0.01$).
- Correlation of Shared Technology (ST) is statistically significant and correlated with Failure of compliance with regulations (CR), $r(30) = .435$, Service and data integration (SDI), $r(30) = .446$ and Failure of client-side encryption (CSE), $r(30) = .433$, (all $p < 0.05$).
- Correction of Account or Service Hijacking (AH) is statistically significant and correlated with Data Ownership (DO), $r(30) = .630$, service and data Integration (SDI), $r(30) = .484$, Data Leakage (DL), $r(30) = .493$, Failure of client-side Encryption (CSE), $r(30) = .706$, Security Culture (SC) $r(30) = .479$ and Privacy (PR) $r(30) = .571$ (all $p < 0.01$). There is also a statistically significant correlation with Smart Scalable Security Benefits (SS), $r(30) = .395$, Advance security mechanism (AS), $r(30) = .420$ and Standardised Security interfaces (SSI), $r(30) = .441$ (all $p < 0.05$).
- Malicious Insider Risks (MI) is statistically significant and correlated with Service and data integration (SDI), $r(30) = .366$, $p < 0.05$.
- Failure of Compliance with Regulations (CR) is statistically significant and correlated with Data Ownership (DO), $r(30) = .425$, Data Leakage (DL), $r(30) = .402$, Failure of client-side Encryption (CSE), $r(30) = .398$, Trust (TR), $r(30) = .425$, Standardised Security interfaces (SSI), $r(30) = .430$ and SLA Audit Enforcement (SLA), $r(30) = .414$ (all $p < 0.05$). There is also a statistically significant correlation with Service and data integration (SDI), $r(30) = .464$ and Smart scalable security benefits (SS), $r(30) = .527$ and Advance security mechanism (AS), $r(30) = .590$ (all $p < 0.01$).
- Data Ownership (DO) is statistically significant and correlated with Service and data integration (SDI), $r(30) = .510$, Data Leakage (DL), $r(30) = .648$, Failure of

client-side Encryption (CSE), $r(30) = .505$ and Security Culture (SC) $r(30) = .470$, (all $p < 0.01$). There is also a statistically significant correlation with Privacy (PR), $r(30) = .384$, Smart scalable security benefits (SS), $r(30) = .426$ and Advance security mechanism (AS), $r(30) = .376$, (all $p < 0.05$).

- Service and data integration (SDI) is statistically significant and correlated with Data Leakage (DL), $r(30) = .540$, Failure of client-side Encryption (CSE), $r(30) = .506$ and Privacy (PR), $r(30) = .517$ (all $p < 0.01$). There is also a statistically significant correlation with Security Culture (SC) $r(30) = .420$, Smart scalable security benefits (SS), $r(30) = .364$, Cutting-edge cloud security marketing (CE), $r(30) = .371$ and Advance security mechanism (AS), $r(30) = .377$, (all $p < 0.05$).
- Data Leakage (DL) is statistically significant and correlated with Trust (TR), $r(30) = .595$, Security Culture (SC) $r(30) = .491$, Privacy (PR), $r(30) = .552$, Advance security mechanism (AS), $r(30) = .609$, and SLA Audit Enforcement (SLA), $r(30) = .487$, (all $p < 0.01$). There is also a statistically significant correlation with Smart scalable security benefits (SS), $r(30) = .427$ and Standardised Security interfaces (SSI), $r(30) = .462$, (both $p < 0.05$).
- Failure of client-side Encryption (CSE) is statistically significant and correlated with Trust (TR), $r(30) = .405$, Smart scalable security benefits (SS), $r(30) = .428$ and Standardised Security interfaces (SSI), $r(30) = .428$, (both $p < 0.05$).
- Trust (TR) is statistically significant and correlated with Smart scalable security benefits (SS), $r(30) = .497$, Advance security mechanism (AS), $r(30) = .662$, Standardised Security interfaces (SSI), $r(30) = .679$, SLA Audit Enforcement (SLA), $r(30) = .728$ and Resource Concentration (RC), $r(30) = .568$, (all $p < 0.01$).
- Security Culture (SC) is statistically significant and correlated with Standardised Security interfaces (SSI), $r(30) = .497$, Cloud Security Auditing (CS), $r(30) = .448$ and SLA Audit Enforcement (SLA), $r(30) = .467$, (all $p < 0.01$).
- Privacy (PR) is statistically significant and correlated with Advance security mechanism (AS), $r(30) = .390$, $p < 0.05$.
- Smart scalable security benefits (SS) is statistically significant and correlated with Cutting-edge cloud security marketing (CE), $r(30) = .592$, Advance security

mechanism (AS), $r(30) = .746$, Standardised Security interfaces (SSI), $r(30) = .753$, Cloud Security Auditing (CS), $r(30) = .654$ and SLA Audit enforcement (SLA), $r(30) = .790$, and Resource Concentration (RC), $r(30) = .793$, (all $p < 0.01$).

- Cutting-edge cloud security marketing (CE) is statistically significant and correlated with Advance security mechanism (AS), $r(30) = .494$, Standardised Security interfaces (SSI), $r(30) = .615$, Cloud Security Auditing (CS), $r(30) = .509$, SLA Audit Enforcement (SLA), $r(30) = .534$, and Resource Concentration (RC), $r(30) = .494$, (all $p < 0.01$).
- Advance security mechanism (AS) is statistically significant and correlated with Standardised Security interfaces (SSI), $r(30) = .781$, Cloud Security Auditing (CS), $r(30) = .456$, SLA Audit Enforcement (SLA), $r(30) = .741$, and Resource Concentration (RC), $r(30) = .572$, (all $p < 0.01$).
- Standardised Security interfaces (SSI) is statistically significant and correlated with Cloud Security Auditing (CS), $r(30) = .569$, SLA audit enforcement (SLA), $r(30) = .847$ and Resource Concentration (RC), $r(30) = .726$, (all $p < 0.01$).
- Cloud Security Auditing (CS) is statistically significant and correlated with SLA Audit Enforcement (SLA), $r(30) = .578$ and Resource Concentration (RC), $r(30) = .510$, (both $p < 0.01$).
- SLA audit enforcement (SLA) is statistically significant and correlated with Resource Concentration (RC), $r(30) = .860$, $p < 0.01$.
- Finally, Decision to Adopt the Cloud (DAC) is statistically significant and correlated with Insecure Interface (II), $r(30) = .552$, Malicious insider risks (MI), $r(30) = .576$, Failure of compliance with regulations (CR), $r(30) = .587$, Service and data integration (SDI), $r(30) = .527$, Data leakage (DL), $r(30) = .578$, Failure of client-side encryption (CSE), $r(30) = .598$, Smart scalable security benefits (CR), $r(30) = .701$, Cutting-edge cloud security marketing (CE), $r(30) = .490$, Advance security mechanism (AS), $r(30) = .468$, Standardised Security interfaces (SSI), $r(30) = .515$, SLA audit enforcement (SLA), $r(30) = .553$, and Resource concentration (RC), $r(30) = .551$, (all $p < 0.01$).

There is also a statistically significant correlation with Shared technology (ST), $r(30) = .411$, Account or Service Hijacking (AH), $r(30) = .319$, Data ownership (DO),

$r(30) = .494$, Trust (TR), $r(30) = .301$, Security Culture (SC), $r(30) = .431$, Privacy (PR), $r(30) = .493$, and Cloud security auditing (CS), $r(30) = .460$, (all $p < 0.05$).

Table 7-6: Correlation Matrix among Security Factors

Inter-Item Correlation Matrix																				
Construct	II	ST	AH	MI	CR	DO	SDI	DL	CSE	TR	SC	PR	SS	CE	AS	SSI	CS	SLA	RC	DAC
II	1	.646**	.160	.348	.228	.076	.467**	.216	.135	-.054	.067	.272	.020	.011	.171	-.146	-.249	-.064	-.053	.552**
ST		1	.335	.296	.435*	.200	.446*	.186	.433*	.083	.119	.355	.081	.168	.169	.063	-.152	.054	.104	.411*
AH			1	.189	.214	.630**	.484**	.493**	.706**	.419*	.479**	.571**	.395*	.329	.420*	.441*	.259	.346	.299	.319*
MI				1	.112	.212	.366*	.234	.190	-.068	-.049	.216	.095	.000	.144	.086	-.142	-.123	-.049	.576**
CR					1	.425*	.464**	.402*	.398*	.425*	.188	.290	.527**	.306	.590**	.430*	.313	.414*	.270	.587**
DO						1	.510**	.648**	.505**	.358	.470**	.384*	.426*	.217	.376*	.348	.273	.296	.192	.494*
SDI							1	.540**	.506**	.213	.420*	.517**	.364*	.371*	.377*	.334	.169	.213	.199	.527**
DL								1	.259	.595**	.491**	.552**	.427*	.187	.609**	.462*	.213	.487**	.306	.578**
CSE									1	.405*	.307	.280	.428*	.346	.319	.428*	.139	.359	.335	.598**
TR										1	.281	.251	.497**	.339	.662**	.679**	.267	.728**	.568**	.301*
SC											1	.212	.349	.347	.346	.497**	.448*	.467**	.308	.431*
PR												1	.129	.049	.390*	.252	.113	.193	.105	.493*
SS													1	.592**	.746**	.753**	.654**	.790**	.793**	.701**
CE														1	.494**	.615**	.509**	.534**	.494**	.490**
AS															1	.781**	.456*	.741**	.572**	.468**
SSI																1	.569**	.847**	.726**	.515**
CS																	1	.578**	.510**	.460*
SLA																		1	.860**	.553**
RC																			1	.551**
DAC																				1
**. Correlation is significant at the 0.01 level (2-tailed).																				
*. Correlation is significant at the 0.05 level (2-tailed).																				

7.4 Reliability of the Instrument

Cronbach's alpha was applied to measure the instrument reliability of the research. A good score of reliability and validity is essential in confirmatory analysis. It was essential to conduct this test at the preliminary data analysis stage of the validation study. This test demonstrated that the results were reliable, which internal consistency of statements, while the Cronbach Alpha reliability of the constructs, Insecure interfaces, Data ownership, Service and data integration, Cutting-edge cloud security marketing and Cloud security auditing were more than 0.8 which shows very good internal consistency.

The Cronbach's alpha reliability statistics were greater than 0.60, as shown in Table 7-8, thus meaning that the internal consistency reliabilities were adequate (Pallant, 2013). The good Cronbach's alpha results also showed that the items used to measure each concept were independent measures and positivity correlated with each other. The Cronbach's alpha for the first category, namely Security Risk Factors, was 0.839, thus indicating a very good reliability. However, for the second category, namely Security Social Factors, the alpha was 0.730, thus indicating acceptable; finally, for the third category, namely Security Benefits Factors, the alpha was 0.927, thus indicating very good reliability.

The overall Cronbach's alpha for all variables was .0945, as presented in Table 7-7. This indicates an excellent level of internal consistency reliability for the instrument (Bryman and Cramer, 2001; Hair et al., 2010).

Table 7-7: Cronbach's alpha reliability analysis for all Items

Cronbach's Alpha	Cronbach's Alpha Based on Standardised Items	N of Items
.945	.948	62

Table 7-8: Cronbach's alpha reliability analysis results

Constructs Measured	Item Used	Item's Code	Cronbach's Alpha Results	Reliability Results
Insecure interfaces	3 items	II1,II2,II3	0.879	Very Good
Shared technology	3 items	ST1,ST2,ST3	0.641	Acceptable
Account or Service Hijacking	3 items	AH1,AH2,AH3	0.637	Acceptable
Malicious insider risks	3 items	MI1,MI2,MI3	0.716	Acceptable
Failure of compliance with regulations	3 items	CR1,CR2,CR3	0.636	Acceptable
Data ownership	4 items	DO1,DO2,DO3	0.848	Very Good
Service and data integration	3 items	SDI1,SDI2,SDI3	0.884	Very Good
Data leakage	3 items	DL2,DL2,DL3	0.642	Acceptable
Failure of client-side encryption	3 items	CSE1,CSE2,CSE3	0.756	Acceptable
Trust	3 items	TR1,TR2,TR3	0.716	Acceptable
Security Culture	3 items	SC1,SC2,SC3	0.685	Acceptable
Privacy	3 items	PR1,PR2,PR3	0.724	Acceptable
Smart scalable security benefits	3 items	SS1,SS2,SS3	0.772	Acceptable
Cutting-edge security marketing	3 items	CE1,CE2,CE3	0.821	Very Good
Advance security mechanism	3 items	AS1,AS2,AS3	0.754	Acceptable
Standardised Security interfaces	3 items	SSI1,SSI2,SSI3	0.716	Acceptable
Cloud security auditing	3 items	CS1,CS2,CS3	0.813	Very Good
(SLA) audit enforcement	3 items	SLA1,SLA2,SLA3	0.771	Acceptable
Resource concentration	3 items	RC1,RC2,RC3	0.694	Acceptable
Decision to Adopt Cloud	4 items	DAC1, DAC2, DAC3, DAC4	0.659	Acceptable
Cloud Security Risk Category			0.0.839	Very Good
Cloud Security Social Category			0.730	Acceptable
Cloud Security Benefits Category			0.927	Excellent
– Listwise deletion based on all variable in the procedure				

7.5 Discussion of the Validation Study and Reliability

In this study, validity and reliability issues were given consideration. Validity is seen as the foundation of defining the accuracy of the findings that the researcher is trying to measure. In this study, two tests were conducted to validate the instrument; pre-test and content validity.

Thus, the results of these tests exposed that the instrument delivered an influence measurement of the developed variables. With the first test of the validation study, namely the pre-test, the instrument contained 20 factors, while 67 items were evaluated. The test involved seven experts, four of whom were from the IT and security experts from Saudi

security groups, while three were researcher's from computer science. The second test used to validate the instrument was content validity.

The content validity ratio (CVR) was used to assess the results of the instrument's content validity test, based on the thoughts of the seven experts who participated in the judgment quantification; the statistical significance level for each factor was also assessed (Lawshe, 1975).

The results of the content validity ratio showed only from the pool of 67 items, only 62 items were significant at the range of more than 0.50, and only five of the items were insignificant, because their significance levels were lower than 0.50; they were subsequently removed from the instrument. Consequently, this content validity ratio (CVR) identified that the security items in the cloud computing adoption framework had acceptable content validity, thus meaning that the items measured the model being studied.

After these experiments, 30 security experts were invited to participate in this research. Slight modifications to the final design of the instrument were made upon receiving the feedback. The modifications were made to the original instrument and the final instrument was developed.

The internal consistency reliability was acceptable. Good Cronbach's alpha results also proved that the items used to measure each factor were independent measures and positivity correlated with each other. The overall reliability outcome for all factors was .645, and thus it was possible to conclude that the 20 factors and 62 items had excellent reliability (Bryman and Cramer, 2001; Hair et al., 2010).

7.6 Summary

This chapter provided the results of the data analysis conducted for the instrument validation. The development process and the validation process of the instrument were presented and the instrument was given consideration in order to define the accuracy of the outcomes that the researcher was attempting to measure. Based on the security cloud adoption framework, 20 factors were carefully chosen, and 67 items were developed for further consideration.

Following this, two experiments were conducted to validate the instrument: pre-test and validation study. The content validation ratio (CVR) was also used. The CVR was applied to the answers of the seven experts to improve the instrument; following this, only 62 items keep on in the reviewed instrument. After these experiments, 30 security experts were asked to take part in this research. Slight modifications to the final design of the instrument were made upon receiving the feedback. The modifications were made to the original instrument and the final instrument was developed.

Data analysis was directed applying correlation analysis to explore the relationship among items and factors. The results of the correlation analysis suggested that the security factors were significantly correlated with each other's. The internal consistency reliability analysis results were very good. Good Cronbach's alpha results also indicated that the items used to measure each factor were independent measures and positivity correlated with each other. The next chapter will discuss the factor analysis details and the outcomes of conducting Structural Equation Modelling (SEM) to validate the relationship between factors that affect government organisations when it comes to the cloud computing adoption implementation decision.

Chapter 8: Results and Discussion of the Model Validation

Using Factor Analysis and Structural Equation Modelling (SEM)

The previous chapter presented the results from the development and validation of the instrument. Following on, this chapter will discuss the results of the model validation, which were obtained through factor analysis and Structural Equation Modelling (SEM). It also discusses the results of the preliminary analysis of the instrument. This chapter details the SEM analysis that was applied to the data obtained from the instrument. The chapter also explores the relationships between the security factors and establishes which security factors affected the decision to adopt the cloud computing services. Exploratory Factor Analysis (EFA) and a Confirmatory Factor Analysis (CFA) using Structural Equation Modelling (SEM) were used in the analysis. The motivation of this analysis was to answer the fourth and fifth sub-questions:

Q4: What are the relationship(s) among the security factors identified from factor analysis and structural equation modelling?

Q5: Which relationship(s) of security factors will affect the Saudi government organisations' decision to adopt the cloud computing services?

Since no prior relationships were assumed, and the model was built from scratch, two factor analyses are discussed in this chapter: exploratory factor analysis and confirmatory factor analysis. Factor Analysis will be discussed in detail in this chapter. The chapter will also discuss the first stage of model building and the factor analysis results. Moreover, the chapter presents the results of the assessment of the proposed hypotheses and the results yielded by the evaluation of the proposed model (two stages in SEM – measurement and structural model valuation. The exploratory factor analysis was conducted using a statistical application called Statistical Parcel for the Social Sciences (SPSS), whereas the SEM modelling was carried out in another statistical application named as Analysis of Moment Structures (AMOS); these were employed to analyse the data collected using the instrument.

8.1 Preliminary Data Analysis

Before conducting data analysis, it is essential to check if there is an error. The main goal of the data examination procedure is to ensure the completeness and consistency of data before starting the analysis (Hair et al., 2010). The preliminary data analysis section discussed the results of the data in the instrument. Moreover, the validation of the instrument in the previous chapter showed that each factor had an acceptable value.

The target respondents of this study were IT and security experts from the government organisations of KSA; this was in line for their ability to gauge the existing condition of their organisation. Furthermore, they are also implicated in the decision of making development, while top management are frequently hard to get.

The sample size was recognised based on the comment that greatest published articles which use SEM as a method of analysis are based on 200 cases (Wolf et al., 2013). The number of experts in this research who accessed the questionnaire was 226; 6 participants did not complete the survey and were deleted. Three cases whose responses were random were also removed from the data analysis. The number of respondents in the study was 215; these participants were Saudi security experts and the security factors in the study were inter-related. A total of 62 questions regarding security in cloud computing adoption were presented to the security practitioners in the government organisations of the KSA.

All the practitioners in this study were working in different IT departments in Saudi government organisations, including education facilities, telecommunication organisations, research institutes, state universities, and ministries; they all had at least two years' of experience in the cloud fields or security. The response item used was a five points Likert-type scale, on which respondents rated the factors; from strongly agree (5) to strongly disagree (1). 'Strongly agree' represents the highest level of agreement, while 'strongly disagree' is the lowest level of agreement respondents can assign.

To arrange the most appropriate data for multivariate analysis, the data was examined for missing values. The IBM SPSS statistics version 24 was used for this analysis, to store the data

in the correct format, and to ensure that the correct data codes were used in this analysis. The second stage provided outcomes involving to demographic information. The third part of the preliminary data analysis discussed the findings of the factor analysis of the questionnaire; this was followed by another test (AMOS), which employed the SEM technique to evaluate the measurement and the structural model in the final stage.

8.2 Handling Missing Values

As mentioned previously in Chapter 6, missing data is one of the concerns in any study using a questionnaire as the research instrument. The instrument was designed carefully, and was prepared to answer all of the questions, and to exclude missing values. While factor analysis was used in this study, missing data was handled using a pairwise technique option, in which case a participant's data was not included. The data was checked for missing values and there were no items where the missing values constituted more than 5% of the data. The total number of respondents for this study, after excluding data, was 215.

8.3 Reliability Analysis Results of the Instrument

As mentioned previously in Chapter 6, in this research, the reliability was measured applying Cronbach's alpha after collecting the data through SPSS software to evaluate inter-item correlation and item-to-total correlation values. Based on Cronbach alpha test, the study used a measure of construct reliability to measure the variables. The overall Cronbach alpha value was 0.865, and as can be seen in Table 8-1, the Cronbach's alpha values for all factors were between 0.6 and 0.8, thus demonstrating the good internal consistency of the items (Pallant, 2013).

Table 8-1: Reliability Analysis Using Cronbach's Alpha

Constructs Measured	Code	Item Used	Cronbach's Alpha	Reliability Results
Insecure interfaces	II	3 items	0.873	Very Good
Shared technology	ST	3 items	0.770	Acceptable
Account or Service Hijacking	AH	3 items	0.789	Acceptable
Malicious insider risks	MI	3 items	0.692	Acceptable
Failure of compliance with regulations	CR	3 items	0.757	Acceptable

Constructs Measured	Code	Item Used	Cronbach's Alpha	Reliability Results
Data ownership	DO	4 items	0.675	Acceptable
Service and data integration	SDI	3 items	0.857	Very Good
Data leakage	DL	3 items	0.854	Very Good
Failure of client-side encryption	CSE	3 items	0.706	Acceptable
Trust	TR	3 items	0.651	Acceptable
Security Culture	SC	3 items	0.620	Acceptable
Privacy	PR	3 items	0.819	Very Good
Smart scalable security benefits	SS	3 items	0.849	Very Good
Cutting-edge security marketing	CE	3 items	0.789	Acceptable
Advance security mechanism	AS	3 items	0.844	Very Good
Standardised Security interfaces	SSI	3 items	0.833	Very Good
Cloud security auditing	CS	3 items	0.777	Acceptable
(SLA) audit enforcement	SLA	3 items	0.865	Very Good
Resource concentration	RC	3 items	0.796	Acceptable
Decision to adopt the cloud	DAC	3 items	0.701	Acceptable

8.4 Demographic Data Analysis

Demographic information was the first type of data collected in the questionnaire; the determination of this was to recognise the context and determine the characteristics of the organisations participating and the expert information being provided in this research. The questionnaire was conducted with 215 experts. Demographic analysis for the respondents and their organisations is presented in Table 8-2.

Table 8-2: The Demographic Data of the Participants' Responses.

Questions	Answers	Frequency	Percentage
Have you worked on an IT or security project in a Saudi government organisation?	Yes	215	100%
	No	0	0%
Have you ever used cloud services at your organisation?	Yes	151	70%
	No	64	30%
Does your organisation adopt cloud services yet?	Yes	80	37%
	No	135	63%
Do you think security affects your organisation's decision to adopt the cloud?	Yes	181	84.4%
	No	34	16%
Choose the option that best reflects your years of experience in the IT or security field	2 years	38	18%
	3-5 Years	77	36%
	6-10 Years	61	28%

More than 10 years	39	18%
-----------------------	----	-----

The demographic information part consisted of five questions. With regard to the first question, all (100%) of the respondents gave a positive answer, stating that they had worked on an IT/security project for a government organisation in the KSA. In terms of the second question, the majority (70%) of the participants indicated that they had used cloud computing services at their organisation, while the other 64 (30%) respondents admitted that they had not used cloud computing services at their government organisation, as presented in Table 8-2.

The third question asked practitioners to classify whether their organisations had adopted cloud computing services. The findings displayed that the majority of the members' organisations had not adopted cloud computing services (63%), but only 37% of the practitioners stated that their organisation previously used cloud services, as illustrated in Table 8-2.

When answering the fourth question, most (84%) of the respondents agreed that security issues significantly affected their organisation's decision to adopt the cloud, and only 16% of the respondents disagreed, as shown in Table 8-2. The last question asked about the respondents' level of experience in the IT/security project field. Of the 215 respondents, 28% had 6-10 years' experience, 36% of participants had 3-5 years' experience, 18% of the respondents had more than 10 years' experience, and 18% of respondents had 2 years' experience, as presented in Table 8-2.

Frequency analyses and descriptive were used to know the responses information. The results of the demographic analysis show that more than 60% of organisations used the cloud, but more than 84% of them were concerned about security, which strongly affected decisions to adopt the cloud services.

8.5 Results of Exploratory Factor Analysis (EFA)

This section discusses the findings of the factor analysis applied in this research. Factor analysis helps to identify underlying factors that summarise a group of items. However, it is the researcher's role to interpret and label these factors – a crucial step in factor analysis. In order to select the items for this study, experts were asked to rate the importance of each item in the instrument.

As mentioned in Chapter 6, Principle Component Analysis (PCA) was used in the factor analysis. There are different approaches to choosing the number of components which should be extracted. Two common approaches were considered in this research: Kaiser's criterion and scree plot inspection. In this study, 62 items related to security in cloud adoption were inspected by practitioners working in different departments at different government organisations in the KSA (see Appendix C).

8.5.1 Assessment for Suitability of Data: Initial Considerations

In this research, there were three considerations for assessing the suitability of data for EFA: sample size, the strength of the relationships between the factors (using KMO), and data assessment screening. Sample size assessment must be carried out before running EFA, while KMO and data screening may be checked after running the analysis.

8.5.1.1 Sample Size

As considered previously in the chapter concerning research methodology for validation of this study, with factor analysis, the sample size is one of the issues which the researcher must consider in determining the suitability of the data. The most common suggestion in terms of sample size is to have 10 to 15 cases per factor (Tabachnick and Fidell, 2012); indeed, this was alluded to in the section on population and sample size, which is found in the research methodology for validation chapter. A smaller sample size may be considered adequate if results have some factors with upper loading (above 0.80) (Hill and Loch, 1998; Hair et al., 2010). In this analysis, the sample size was 215; most of the factors had good loadings, as presented in Table 8-5.

8.5.1.2 Strength of the Relationships between the Variables (Kaiser-Meyer-Olkin (KMO) measure)

One of the statistical methods that can be used to recognise the suitability of data is Kaiser-Meyer-Olkin (KMO). It uses a metric that ranges from 0 to 1. If the value is more than 0.5, then the correlations between the variables are acceptable and can be used to conduct factor analysis. *“The values between 0.5 and 0.7 are mediocre, values between 0.7 and 0.8 are good, values between 0.8 and 0.9 are great and lastly, values above 0.9 are superb”* (Kaiser, 1970).

A KMO value of 0.6 is recommended as the lowest value for a good factor analysis (Tabachnick and Fidell, 2007). The KMO value for the sample collected in this research was 0.881, which suggests that the factor analysis was suitable for this dataset, as shown in Table 8-3.

Table 8-3: KMO Test Result

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.	0.881
Approx. Chi-Square	4128.125
df	171
Sig.	0.001

8.5.1.3 Data Screening for EFA

It is recommended by researchers to screen data prior to using any statistical technique (Tabachnick and Fidell, 2007). One of the considerations in data screening is checking for and handling missing variables. Fortunately, there were no missing variables in this analysis, and therefore no handling was needed. Another consideration, which is specific to EFA, is that variables should be reasonably correlated with each other. This can be checked by investigating the correlations. Fortunately, the correlation matrix showed that, in this analysis, there were many correlations among variables which exceeded 0.3, thus suggesting that the dataset was suitable for EFA (Tabachnick and Fidell, 2007).

8.5.2 Factor Extraction: Summarising Variables

This section provides the results of the factor extraction in EFA. Chapter 6, Section 6.9.1.1, includes the theoretical aspects related to factor extraction, including its uses and options. As

such, in this analysis, principal component analysis (PCA) was deemed more appropriate for use than factor analysis. This is because, with the latter, relationships are assumed appropriate to review best of the original information (variance) in a smallest number of factors prediction. In order to define how many factors (or components) should be extracted, two methods were used in this analysis: Kaiser's criterion (using eigenvalues > 1) and scree plot investigation.

- **The first method, Kaiser's criterion**, recommended by Guttman and amended by Kaiser, considers factors with an eigenvalue greater than 1.00 as common factors (Nunnally, 1978). The eigenvalue of a factor signifies the amount of the total variance described by that factor.
- Table 8-4 shows the initial eigenvalues from the factor analysis.

Table 8-4: Eigenvalues and Total Variance

Component	Eigenvalues Total	Eigenvalues % of Variance	Eigenvalues Cumulative %
1	9.802	51.588	51.588
2	2.391	12.585	64.173
3	1.310	6.892	71.065
4	.998	5.254	76.319
5	.859	4.516	80.835
6	.858	4.396	81.133
7	.680	3.581	84.415
8	.556	2.928	87.344
9	.521	2.742	90.085
10	.398	2.094	92.179
11	.311	1.639	93.818
12	.295	1.551	95.369
13	.180	.947	96.316
14	.160	.842	97.158
15	.136	.715	97.872
16	.107	.566	98.438
17	.098	.514	98.952
18	.081	.428	99.380
19	.067	.353	99.732
20	.051	.268	100.000

The Eigenvalues Total column shows the eigenvalue for each component. The Eigenvalues % of Variance column shows how much variance each factor explains, while the Eigenvalues Cumulative % column shows the amount of variance accounted for by all previous factors added together. As shown in

Table 8-4, components 1, 2 and 3 had eigenvalues greater than 1. Therefore, as per Kaiser's criterion, they were extracted. The results which were extracted will be discussed in a later section.

- **The second method: investigation of the scree plot**, is another way to define the number of factors which should be extracted from the final solution. This is a plot of the eigenvalues connected with each of the factors extracted, against each factor. In this method, visual inspection is performed, during which there is a careful examination of the intersection point between virtual vertical lines, connecting the factors with another virtual horizontal line (in which the factors should be levelling out) connecting the remaining factors.

The factors to be extracted should lie to the left of this intersection point. With a sample of more than 200 participants, the scree plot offers a properly reliable criterion for factor selection (Field, 2013). Moreover, the scree plot technique from this preliminary is used to decide on the correct number of factors (or components) to be extracted. Many recommend retaining only components above the point, as presented in Figure 8-1.

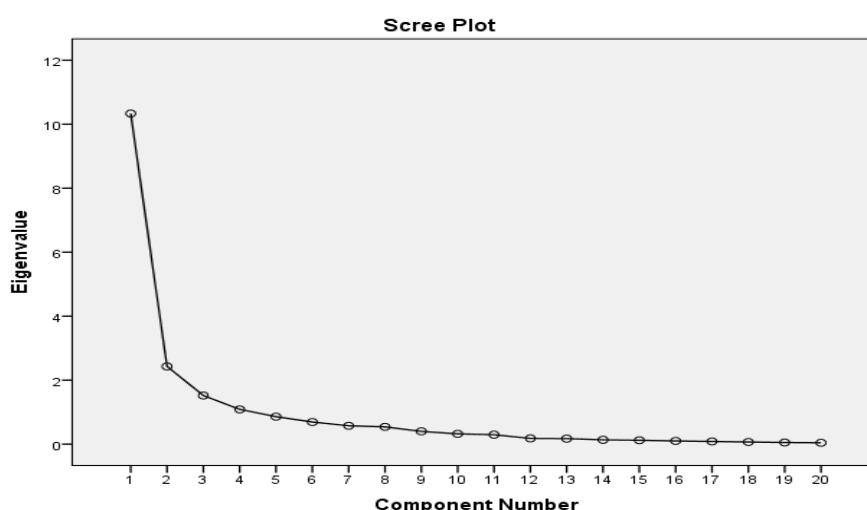


Figure 8-1: Factor Extraction Applied Scree Plot

Looking at Figure 8-1, it can be seen that there are three components to the left of the intersection point between the virtual vertical and horizontal lines. This suggests that three components should be extracted. It should be noted that it is not always the case that the results from the scree plot inspection are in line with Kaiser's criterion. Fortunately, this was the case in the present analysis, and thus there is more confidence in the results.

8.5.3 Factor Rotation: Improving Interpretation of Factors

This section discusses the findings of the factor rotation used in this research. Chapter 6 includes theoretical aspects related to factor rotation, including its uses and options. There are different recommendations and guidelines put forth by researchers as to which rotation method should be used: orthogonal or oblique. More information on this can be found in Chapter 6. As suggested by Tabachnick and Fidell (2007), both orthogonal and oblique rotations were used in this analysis, with the aim of finding the most interpretable solution. In addition, and given the differences between the total eigenvalues of components 3, 4 and 5, as shown in

Table 8-4, the decision was taken to rerun the analysis for each of these components while rotating them once obliquely and again orthogonally.

Table 8-5: Factor Loading (Communalities) Using Orthogonal Rotation

Loading Factors Components No	Item Variables	Code	Initial	Extraction
1	Failure to Comply with Regulations	CR	1.000	0.664
1	Trust	TR	1.000	0.632
1	Smart Scalable Security Benefits	SS	1.000	0.903
1	Cutting-Edge Cloud Security Market	CE	1.000	0.802
1	Advanced Security Mechanism	AS	1.000	0.829
1	Standardised Security Interfaces	SSI	1.000	0.872
1	Cloud Security Auditing	CS	1.000	0.815
1	SLA Audit Enforcement	SLA	1.000	0.878
1	Resource concentration	RC	1.000	0.829
2	Insecure Interfaces	II	1.000	0.505
2	Shared Technology	ST	1.000	0.602
2	Malicious Insiders	MI	1.000	0.595
2	Data Ownership	DO	1.000	0.710
2	Service and Data Integration	SDI	1.000	0.751

2	Failure of Client-side encryption	CSE	1.000	0.770
2	Security Culture	SC	1.000	0.564
3	Account or Service Hijacking	AH	1.000	0.612
3	Data Leakage	DL	1.000	0.644
3	Privacy	PR	1.000	0.827

This means that a total of six runs were conducted. As noted by other researchers (Williams and Child, 2003; Suhr, 2006), the solutions provided by using orthogonal rotation do not differ very much from those provided by using oblique rotation (Tabachnick and Fidell, 2007). However, these combinations made it possible to find the most interpretable solution, namely using orthogonal rotation with three components extracted. This solution was also found to support the theoretical framework suggested in this research. In other words, although considered a form of exploratory analysis, EFA served as a validation tool for the framework. Table 8-5 provides a summary of communalities for all security factors and their correlated indicators.

The factor loading results showed that all variables had a loadings value of 0.5 and above, thus indicating high loadings; for a sample size of 200, a loading would be more than 0.36 (Tabachnick and Fidell, 2007). The next section will present the results of the factor analysis conducted after the factor extraction and rotation.

8.5.1 Factor Analysis Results

This section provides the outcomes of the factor analysis of data from the instrument. During this analysis, requesting only values of 0.4 and higher for the factor loadings provided a significant value at the 0.01 level for each loading in the factor analysis. This significance value of the factor loading shows the essence of that component to the factor. Table 8-5 illustrates the rotated component matrix (only items with a loading of 0.4 are displayed). **Error! Reference source not found.** shows the constructs retrieved from the instrument.

In terms of identifying the factors or components, SPSS does not supplement the identifying or meaning for each factor or component; in fact, SPSS only determines the grouping of

variables. Therefore, it is up to the researcher to recognise the content of the loadings and their meaning regarding the research goals.

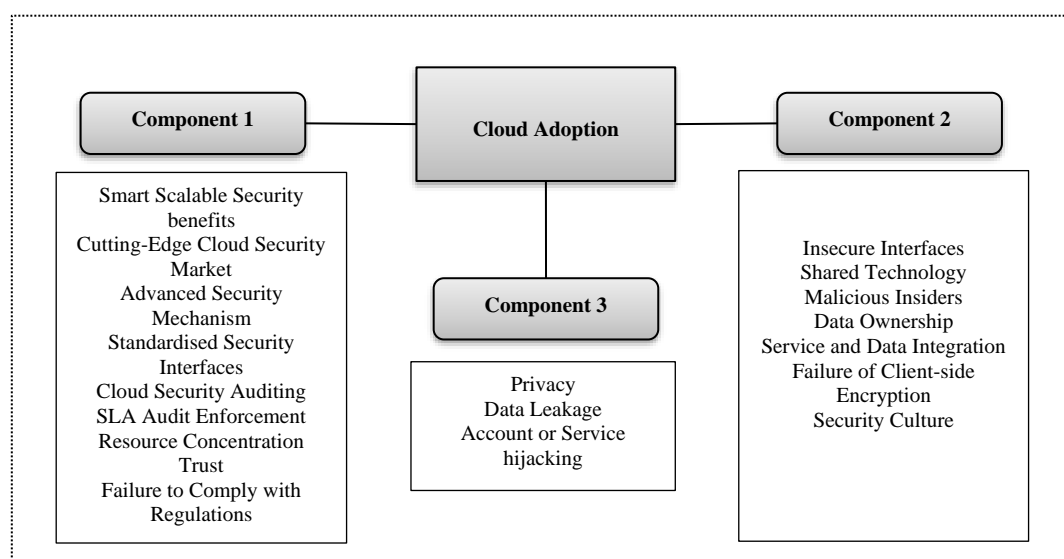


Figure 8-2: Components and Constructs Retrieved from the Instrument

In this factor analysis, the components were clustered based on the questionnaire responses. In addition, it was still necessary to interpret the meanings of all the extracted components. The meanings of the components loaded on the factors are discussed as follows:

- **The first component** was loaded by nine indicators and showed the importance of security benefits in cloud computing, as agreed upon by the security experts in the government organisations. The highest loadings clarified the importance of the Smart Scalable Security Benefits factor in cloud computing adoption, which had a loaded value of 0.903. This factor is defined as the ability to extend security benefits. This was followed by the resource consideration factor, with a loading value of 0.829, which also shows the importance of security benefits in cloud computing when it comes to access control, comprehensive security policy, patch and data management, and maintained processes.

The other indicators with high loading included Standardised security interfaces, SLA audit enforcement, Cloud security auditing, advanced security mechanisms, and Cutting-edge security market, as presented in Table 8-5. This component was thought to refer to **Cloud Adoption Security Benefits**. Only two factors, namely Failure to

Comply with Regulations, and Trust initially belonged to a different group, but were regrouped after being rotated to this first component.

- **The second component** was loaded by eight indicators, and the result from the factor analysis revealed the importance of cloud security risks when implementing the cloud adoption. The highest loading showed the importance of the decision to adopt the cloud factor, with a loading value of 0.862; this was followed by the client-side encryption factor, with a loading value of 0.770. Moreover, the Malicious Insiders factor had a high loading value of 0.595, thus indicating that all organisations must be sure that their own data is protected; this also shows the importance of these factors when making a decision to adopt the cloud.

This component also included Service and data integration, Data Ownership, shared technology, Service and Data Integration, Insecure Interfaces and security cultures. Only one factor, namely security culture, belonged to a different component after the rotation. All of these loadings are important when adopting the cloud services, and are best described as **Cloud Adoption Security Risks**.

- **In the last component**, the three loadings described the fear of leaking data and the privacy of the organisation information; this fear related to the notion that, when personal information is accessed by third-party organisations, this may raise privacy concerns and affect the decision to adopt the cloud.

The highest loading in this component was the privacy factor, with a loading value of 0.827; this was followed by the account hijacking factor, with a loading value of 0.612, and the data leakage factor, with a loading value of 0.644. These loadings are best described as **Cloud Adoption Security Awareness**.

Based on the eigenvalue rules through exploratory factor analysis, three components were extracted and retained for additional investigation. After the rotation was implemented, the factors that were loaded on these three components were interpreted and the meanings of the three components were defined.

Two indicators of the total variance showed that it could belong to the first and third components. However, it was decided that it should be grouped in the first component, because the factor loading was strongly explained in the first component. The analysis of the factors made it possible to summarise that a structure for data gained from instrument was recognised; 62 items conducted and were gathered into 20 constructs. The further section will be tested the structure which identified using confirmatory factor analysis; this will include a measurement model and a presentation of the results.

8.6 Results of Confirmatory Factor Analysis Using Structural Equation Modelling (SEM)

As considered previously in the chapter on research methodology for the validation of this study in Section 6.9.2, a confirmatory factor analysis (CFA) is a kind of structural equation modelling (SEM) that contracts particularly with measurement models.

In this research, the SEM analysis approach was applied to test the proposed security cloud adoption model and to determine the strength of the relationships among the dependent variables and independent; this approach also made it possible to evaluate how good this model was in terms of fit. The IBM SPSS AMOS 24 software was generated to analyse data via SEM; this was due to the ease of use and free of availability of this software and the fact that its structures met the requirements of this research (Byrne, 2010). AMOS software is an additional part of SPSS, which has the task of taking on CFA and SEM. The next section will present the analysis of the structural measurement model.

8.6.1 Analysis of Structural Measurement Model

The measurement model of the research was performed in accordance with 20 constructs or latent variables (unobserved variables), that were measured by 62 items or measured variables (observed variables or indicators). The procedure started by defining different constructs, and listing constructs that would be included in the measurement model. Given the results achieved in the security cloud model, exploratory factor analysis was conducted (described in the earlier section) to explain the basic structure of the data.

The measured variables were concepts acquired based on the initial findings and the results obtained throughout this research (which were stated in the previous section, Section 8.5).

The pattern structure made it possible to recognise that the 20-factor indicators can be grouped into three constructs or components. In this study, each latent variable was measured by more than two items; the latent variables and their indicators are presented in Table 8-6. The next section will present the results of the validity measurement for the model.

Table 8-6: Latent Constructs and Indicator Variables

Latent Variable	Item's Code	Items Used
1 Insecure Interfaces	II	II1, II2, II3
2 Shared Technology	ST	ST1,ST2,ST3
3 Account or Service Hijacking	AH	AH1,AH2,AH3
4 Malicious Insider Risks	MI	MI1,MI2,MI3
5 Failure of Compliance with Regulations	CR	CR1,CR2,CR3
6 Data Ownership	DO	DO1,DO2,DO3
7 Service and Data Integration	SDI	SDI1,SDI2,SDI3
8 Data Leakage	DL	DL2,DL2,DL3
9 Failure of Client-side Encryption	CSE	CSE1,CSE2CSE3
10 Trust	TR	TR1,TR2,TR3
11 Security Culture	SC	SC1,SC2,SC3
12 Privacy	PR	PR1, PR2, PR3
13 Smart Scalable Security Benefits	SS	SS1,SS2,SS3
14 Cutting Edge Security Marketing	CE	CE1,CE2,CE3
15 Advance Security Mechanism	AS	AS1,AS2,AS3
16 Standardised Security Interfaces	SSI	SSI1,SSI2,SSI3
17 Cloud Security Auditing	CS	CS1,CS2,CS3
18 SLA Audit Enforcement	SLA	SLA1,SLA2,SLA3
19 Resource Concentration	RC	RC1,RC2,RC3
20 Decision to Adopt the Cloud	DAC	DAC1,DAC2,DAC3,DAC4

8.6.2 The Assessment of Measurement Analysis Model Validity

In this section, each latent component (termed a measurement model), alongside its factors, was evaluated and estimated individually. This was carried out once the measurement model was specified, sufficient data was collected, and the key decisions, such as the estimation method, had already been made. This is the reason for assessing the measurement model's validation, while the estimation is to demonstrate that its items predict the factors. Before assessing the fit of the measurement model, it is advisable to check the specifics associated with the SEM.

This process involved two steps. First, reliability analysis was implemented so as to obtain statistical results, using Cronbach's alpha. Second, an assessment of the measurement model's validity was conducted to ensure that it measured what it was supposed to measure. The reliability and validity of the measurements were shown in this research, and the findings are discussed in the next sections.

8.6.2.1 Reliability

As mentioned in Chapter 6, Section 6.8.2, reliability analysis is one of the most significant techniques to measure a set of indicators contain latent constructs (Hair et al., 2010). In this analysis, three types of reliability were used, namely construct reliability, average variance extracted , and internal reliability.

The first type of reliability is internal reliability, which was measured using Cronbach's alpha, which is very sensitive to the number of items measured (Pallant, 2013). In this research, the reliability test was measured by using Cronbach's alpha, which can be applied for assessing reliability only when the number of indicators are similarly loaded on a construct's variable or for the model underlying a single construct (Shevlin et al., 2000).

The second type of reliability in this analysis is construct reliability (CR), or as it is also called, composite reliability; this is an important step in SEM. The construct reliability "*measures reliability and internal consistency of the measured variables representing a latent construct*" (Hair et al., 2010). To measure the reliability, construct reliability was calculated by using the following formula (See equation 2), as proposed by Hair et al. (2010):

$$\text{Construct Reliability (CR)} = \frac{(\sum_{i=1}^n L_i)^2}{(\sum_{i=1}^n L_i)^2 + (\sum_{i=1}^n e_i)} \quad (2)$$

In the above equation, (1), L_i is standardised factor loading, n is the number of items, and e_i is the error variance term for a construct. The factor loading of variables (L_i) shows the path between measured items (observed variables) and their constructs. A construct reliability value of above 0.7 is thought to signify high reliability, while a reliability between 0.6 and 0.7 is acceptable (Hair et al., 2010).

With regard to the third type of reliability, namely average variance extracted (AVE), a value of 0.5 or higher specifies that the items have a high ratio of variance in common. In contrast, a value lower than 0.5 signifies that, on average, more error rests in the items than differences are explained by the latent factor structure linked to the measure (Hooper et al., 2008; Hair

et al., 2010). Summaries of these three types of reliability and their criteria are presented in Table 8-7, while the results are presented in Table 8-8.

Table 8-7: Summarisation of Criteria for the Reliability of the Measurement Model

Reliability	Criteria
Internal Reliability	Internal reliability is accomplished when the Cronbach's alpha value is 0.6 or greater.
Construct Reliability	The measure of reliability and internal consistency of the measured variables demonstrate a latent construct. In order to succeed in constructing reliability, a value of CR \geq 0.6 is essential.
Average Variance Extracted	Average Variance Extracted (AVE) is the average percentage of variation explained by the variable in a construct. An AVE of \geq 0.5 is essential.

Table 8-8: Results of the Reliability Analysis Test for the Measurement Model

Construct	Observed Items	Standardised factor loading (>0.5)	Error Variance			
TR	TR1,TR2,TR3	0.657	0.108			
CR	CR1,CR2,CR3	0.735	0.091			
CE	CE1,CE2,CE3	0.852	0.115			
AS	AS1,AS2,AS3	0.91	0.070			
CS	CS1,CS2,CS3	0.869	0.091			
SLA	SLA1,SLA2,SLA3	0.938	0.046			
SSI	SSI1,SSI2,SSI3	0.907	0.070			
RC	RC1,RC2,RC3	0.892	0.084			
SS	SS1,SS2,SS3	0.941	0.053			
CSE	CSE1,CSE2,CSE3	0.871	0.072			
MI	MI1,MI2,MI3	0.658	0.055			
SDI	SDI1,SDI2,SDI3	0.83	0.044			
DO	DO1,DO2,DO3	0.843	0.057			
II	II1,II2,II3	0.609	0.082			
ST	ST1,ST2,ST3	0.693	0.061			
SC	SC1,SC2,SC3	0.723	0.094			
PR	PR1,PR2,PR3	0.687	0.090			
AH	AH1,AH2,AH3	0.78	0.064			
DL	DL2,DL2,DL3	0.533	0.094			
DAC	DAC1,DAC2,DAC3,DAC4	0.640	0.038			
$CR = \frac{(\sum_{i=1}^n L_i)^2}{(\sum_{i=1}^n L_i)^2 + (\sum_{i=1}^n e_i)}$	SB Component		SR Component		SA Component	
	CR	0.98	CR	0.98	CR	0.94
	Highly Reliable		Highly Reliable		Highly Reliable	
** Value > 0.7						
Notes: (SR) Security Risks, (SB) Security Benefits, (SA) Security Awareness						

8.6.2.2 Validity

Validity refers to the ability of an instrument to measure what is hypothetical to be measured for a construct (Awang, 2015). The validity of a measurement model is gauged based on the requirements of three types of validity: convergent validity, construct validity, and discriminant validity. These types of validity are described, alongside their requirements, in Table 8-9.

Table 8-9: Descriptions of Validity Types in Structural Equation Modelling with Their Requirements

Validity	Description and Requirement
Convergent validity	<p>Convergent validity is the extent to which a set of measured variables in a construct are correlated and which variables display a significant correlation with each other (Hair et al., 2010). Convergent validity is used to evaluate the correlation among measured variables of the same construct (Straub et al., 2004; Pallant, 2013). The convergent validity is achieved when all items in a measurement model are statistically significant.</p> <p>To achieve a high convergent validity, factor loadings have to be statistically significant and the value must be 0.5 or more. The top is 0.7, as the square of consistent factor loading signifies how much variation in an item is clarified by the latent factor. Moreover, Average Variance Extracted (AVE) could also prove this validity, as presented in Table 8-10. AVE is one of the collective approaches that is used for assessing convergent validity. The following equation was used to calculate AVE (See equation 8.6.2.2), as recommended by Hair et al. (2010):</p>

$$\text{Average Variance Extracted (AVE)} = \frac{\sum_{i=1}^n L_i^2}{n} \quad 8.6.2.2$$

	<p>In formula (2), λ_i is the standardised factor loading, and n signifies the number of items. The value of AVE should be greater or equal to 0.5 in order to accomplish this validity.</p>
Construct validity	<p>Hair et al. (2010) described the construct validity as: <i>“The extent to which a set of measured items actually represent the theoretical latent construct those items are designed to measure”</i>. The construct validity is accomplished when the Fitness Indexes achieve the level of acceptance.</p> <p>In this analysis, construct validity discusses to whether the data achieved from the instrument measures the construct sufficiently.</p>
Discriminant validity	<p>Discriminant validity defines to the “extent to which a construct is truly distinct from other constructs, both in terms of how much it correlates with other constructs and how distinctly measured variables represent only this single construct” (Kline, 2011). The discriminant validity is accomplished when the measurement model is free from redundant items. The other requirement for discriminant validity is that the correlation between constructs have to be a smaller than 0.85 (Hair et al., 2010). Other than that, the square root of AVE for the construct must be greater than the correlation between the corresponding constructs.</p> <p>Table 8-11 illustrates the findings of discriminant validity. It is perfect from the findings that the value of the square root of AVE for all latent constructs, as emphasised in Table 8-11, was greater than the correlation between these constructs. Therefore, the findings presented acceptable evidence regarding the discriminant validity of the latent constructs.</p>

Table 8-10: The Analysis of Convergent Validity

Component	Construct	Observed Items	Estimate	Error Variance	Squared Correlations
SB	TR	TR1,TR2,TR3	0.657	0.108	0.623
	CR	CR1,CR2,CR3	0.735	0.091	0.683
	CE	CE1,CE2,CE3	0.852	0.115	0.737
	AS	AS1,AS2,AS3	0.91	0.070	0.806
	CS	CS1,CS2,CS3	0.869	0.091	0.784
	SLA	SLA1,SLA2,SLA3	0.938	0.046	0.868
	SSI	SSI1,SSI2,SSI3	0.907	0.070	0.811
	RC	RC1,RC2,RC3	0.892	0.084	0.796
	SS	SS1,SS2,SS3	0.941	0.053	0.821
SR	CSE	CSE1,CSE2,CSE3	0.871	0.072	0.756
	MI	MI1,MI2,MI3	0.658	0.055	0.434
	SDI	SDI1,SDI2,SDI3	0.83	0.044	0.692
	DO	DO1,DO2,DO3	0.843	0.057	0.708
	II	II1,II2,II3	0.609	0.082	0.371
	ST	ST1,ST2,ST3	0.693	0.061	0.481
	SC	SC1,SC2,SC3	0.723	0.094	0.522
SA	PR	PR1,PR2,PR3	0.687	0.090	0.511
	AH	AH1,AH2,AH3	0.78	0.064	0.567
	DL	DL2,DL2,DL3	0.533	0.094	0.289
	DAC	DAC1,DAC2,DAC3,DAC4	0.640	0.038	0.648
AVE = $\frac{\sum_{i=1}^n L_i^2}{n}$		SB AVE	SR AVE	SA AVE	
** Value > 0.5		0.73	0.57	0.55	
Notes: (SR) Security Risks, (SB) Security Benefits, (SA) Security Awareness					

Table 8-11: Discriminant Validity Analysis Test

	CR	AVE	MSV	Max R(H)	SR	SB	SA
SR	0.900	0.567	0.445	0.918	0.753		
SB	0.961	0.736	0.373	0.979	0.611	0.848	
SA	0.733	0.555	0.445	0.981	0.667	0.433	0.696

Discriminant Validity: Compare the squared correlations and AVE scores for each of the pairwise constructs

Notes: SR Security Risks, SB Security Benefits, SA Security Awareness

8.6.3 Specifying Structural Model and Assessing the Relations

Specifying the measurement model is an important stage in developing a SEM Model. The structural model is the further stage following verification of the convergent validity and composite reliability, as described in the previous sections. Structural model specification focuses on the relationships between construct variables instead of relationships among construct variables and their measured variables (indicators) (Hair et al., 2010).

Moreover, the researcher employed the structural model to allow for certain relationships between the latent variables to be shown by the direction of the arrows (Finkelstein, 2005).

In this study, the relationships between the latent variables were evaluated via the use of standardised path coefficients (regression coefficients, Critical Ratio (C.R.), p-value and squared multiple correlations (R^2) (Hair et al., 2010)). P-value was used to evaluate exactly how statistically significant the relationship was between the measured variables and the latent variables.

The squared multiple correlations (R^2) represent *“the proportion of variance that is explained by the predictors of the variable in question”* (Hair et al., 2010). The range of squared multiple correlations (R^2) values is between 0 and 1.00, and there is a stronger relationship between two variables if it is near to 1.00, whereas a value close to 0 indicates a poor relationship (Tabachnick and Fidell, 2012). If the model fit is acceptable, the parameter estimates are examined, as is the ratio between each parameter estimate and its standard error. The ratio is significant at the level 0.05 if its value exceeds 1.6, and at the level of 0.01 if it exceeds 2.56 (Hoyle, 1995).

At this stage, it is important to present the output from the analysis, including the standardised regression for each path, standard error (S.E), critical ratio (C.R), and their significant path. These are illustrated in Table 8-12.

Table 8-12: The Hypotheses Measurement Paths in the Structural Model Specification (CFA Model)

Hypotheses Path Regression	Standardised Estimate Loadings	S.E.	C.R.	P	Significant Path
H1: TR \leftarrow SB	.790	.031	10.030	***	✓

H2: CR \leftarrow SB	.827	.029	7.866	***	√
H3: CE \leftarrow SB	.859	.013	7.022	***	√
H4: AS \leftarrow SB	.898	.019	9.779	***	√
H5: CS \leftarrow SB	.886	.015	9.677	***	√
H6: SLA \leftarrow SB	.932	.012	9.511	***	√
H7: SSI \leftarrow SB	.900	.008	9.058	***	√
H8: RC \leftarrow SB	.892	.010	9.267	***	√
H9: SS \leftarrow SB	.870	.006	8.321	***	√
H10: CSE \leftarrow SR	.658	.008	9.029	***	√
H11: MI \leftarrow SR	.832	.009	9.195	***	√
H12: SDI \leftarrow SR	.841	.007	8.842	***	√
H13: DO \leftarrow SR	.609	.010	7.658	***	√
H14: II \leftarrow SR	.694	.006	9.692	***	√
H15: ST \leftarrow SR	.723	.005	8.407	***	√
H16: SC \leftarrow SR	.715	.007	8.242	***	√
H17: PR \leftarrow SA	.753	.008	9.842	0.003	√
H18: AH \leftarrow SA	.538	.006	9.553	***	√
H19: DL \leftarrow SA	.790	.010	9.411	***	√
SB \rightarrow DAC	.614	.044	9.727	***	√
SR \rightarrow DAC	.516	.115	8.723	***	√
SA \rightarrow DAC	.704	.101	6.620	***	√

Notes: (SR) Security Risks, (SB) Security Benefits, (SA) Security Awareness, (DAC) Decision to adopt the cloud.

S.E. Approximate standard error,

C.R. Critical ratio. The critical ratio is the parameter estimate divided by an estimate of its standard error,

***** Probability (P) < 0.001: p-value should be < 0.001**

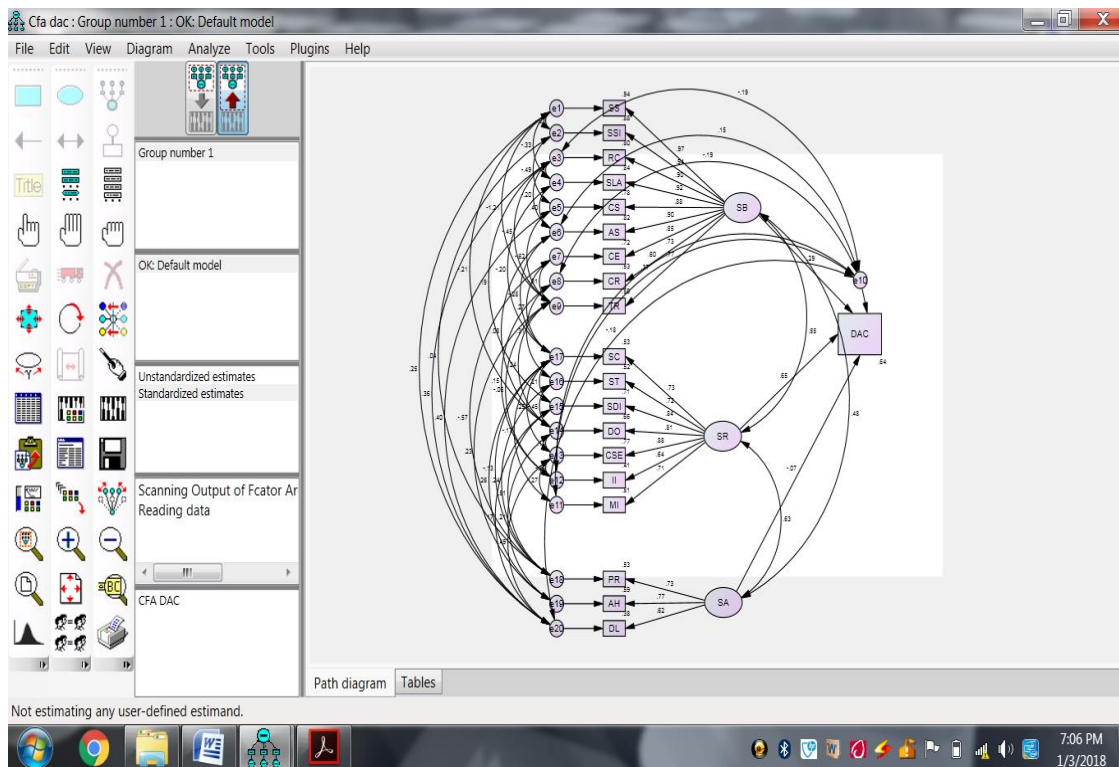


Figure 8-3: Screenshot of Specified Hypothesised and Standardised Output
Estimates of Structural Model

The results showed that the paths for all hypotheses (from H1 to H19) were statistically significant, and most of the exogenous variables had strong and positive relationships with their fellow exogenous variables as presented in Figure 8-3. This can be inferred from the critical ratio (C.R), which was greater than the absolute value of 2.56, and the p-value, which was less than 0.001. The structural relationships between the components and the decision to adopt the cloud in the model generated by Amos, are presented in Table 8-13. These relationships between the model components include the following estimation values:

- The estimated correlation between the Security Benefits component and the Security Awareness component in the model was 0.534, which indicates a good correlation.

- The estimated correlation between the Security Benefits component and the Security Risks component in the model was 0.648, which indicates a good correlation.
- The estimated correlation between the Security Risks component and the Security Awareness component in the model was 0.573, which indicates a good correlation.

Table 8-13: Squared Multiple Correlation between Construct Variables and Components

Latent variables	Correlation
H1: DL \leftarrow SA	.534
H2: AH \leftarrow SA	.774
H43: PR \leftarrow SA	.696
H4: SC \leftarrow SR	.684
H5: ST \leftarrow SR	.747
H6: II \leftarrow SR	.622
H7: DO \leftarrow SR	.874
H8: SDI \leftarrow SR	.819
H9: MI \leftarrow SR	.674
H10: CSE \leftarrow SR	.860
H11: SS \leftarrow SB	.941
H12: RC \leftarrow SB	.895
H13: SSI \leftarrow SB	.902
H14: SLA \leftarrow SB	.952
H15: CS \leftarrow SB	.846
H16: AS \leftarrow SB	.936
H17: CE \leftarrow SB	.817
H18: CR \leftarrow SB	.770
H19: TR \leftarrow SB	.693
SB \leftrightarrow SR	.534
SB \leftrightarrow SA	.648
SR \leftrightarrow SA	.573
Notes: SR Security Risks Component, SB Security Benefits Component, SA Security Awareness Component	

The highest variance in the decision to adopt the cloud (with value $R^2 = 0.704$), indicated that 70% of variance in the decision to adopt the cloud is significantly influenced by independent variables. In contrast, the results of the correlation between the latent variables in the research model for all latent variables were statically significant; moreover, all results had a positive effect on the decision organisation's to adopt cloud services, as presented in Table 8-13. However, some were weaker than others.

Overall, these outcomes showed that the proposed security cloud adoption model is statistically significant in explaining cloud adoption at the organisational level. The relationships for the latent variables in the above table showed that there were 19 significant paths in the model for relationships and hypotheses.

8.6.4 Structural Model Goodness of Fit (GoF) and Estimation Analysis of Indices

As considered previously in the research methodology concerning the validation of this study chapter, the Goodness of Fit (GoF) is one of the approaches used to test a proposed model to determine the goodness of fit (Hair et al., 2010). In summarising the structural model goodness of fit, it can be determined that the most recommended indices are Comparative Fit Index (CFI), the Goodness of Fit Index (GFI), Root Mean Square Residual (RMR), Standardised Root Mean Square Residual (SRMR), the Root Mean Square Error of Approximation (RMSEA), and the Tucker Lewis Index (TLI). All statistics which fit the above-mentioned indexes range from 0 to 1.00. The results, and the accepted value of the statistical tests, will be presented in detail as follows:

- **Root Mean Square Error of Approximation (RMSEA):** is linked to remaining in the model, and its reported as a poor fit when the value is greater than 0.1 (Hair et al., 2010). RMSEA is a very common guide and is widely applied with difficult models that contain large numbers of measured variables and large sample sizes: the RMSEA value should be in the range 0 to 0.08, and a model is well-fitting when it is close to 0 (Bentler, 1990).
- **Root Mean Square Residual (RMR) and Standardised Root Mean Square Residual (SRMR):** a RMR statistics fit that would be appropriate if its value was lower than 0.1, while it is reported as an acceptable fitting model with a value of 0.05 or lower (Acuna and Rodriguez, 2004).
In addition, SRMR is a standardised value of RMR (Kline, 2011). The approved value of RMR is less than 0.1, and the value of SRMR would be less than 0.08 if signifying a good fitting of the model (Hair et al., 2010).
- **The Comparative Fit Index (CFI):** is the same as the discrepancy function, but is adjusted for sample size. The range of CFI varies from 0 to 1, with a higher

value demonstrating a better model fit. The acceptable model fit is indicated by a CFI value of 0.90 or greater (Bentler, 1990).

- **The Tucker Lewis Index (TLI):** is one of the most commonly-suggested indices for use in estimating GoF. The TLI test compares the values of the normed chi-square. It ranges from 0 to 1, and the model is fitting if the TLI value is more than 0.90 (Bentler, 1990; Hair et al., 2010).

Table 8-14 presents the summarisation of these statistical tests and information about the model fit category, as well as its level of acceptance and references.

Table 8-14: Goodness of Fit Indexes with Their Level of Acceptance and References

Goodness of fit Index	Index Name	Level of Acceptance	Reference
RMSEA	Root Mean Square Error of Approximation	RMSEA < 0.05 Good Fit RMSEA < 0.08 Adequate fit RMSEA value up to 0.10 poor fit	(Bentler, 1990; Hair et al., 2010)
RMR,	Root Mean Square Residual	RMR < 0.1	(Hair et al., 2010; Kline, 2011)
SRMR	Standardised Root Mean Square Residual	SRMR < 0.08	(Hair et al., 2010; Kline, 2011)
CFI	Comparative Fit Index	CFI > 0.90	(Bentler, 1990)
GFI	Goodness of Fit Index	GFI > 0.90 good fit GFI = 1.00 perfect fit	(Bentler, 1990)
Normed chi-square χ^2/df	Discrepancy chi square	χ^2/df < 3.0 good fit	(Wheaton, 1987)
TLI	Tucker Lewis Index	TLI > 0.90	(Bentler, 1990; Hair et al., 2010)

In this analysis, the Maximum Likelihood (ML) estimation method was applied to calculate the GoF indices conducting AMOS (version 24). ML is an estimation approach that is applied to generate parameter estimates of SEM. Further, it is an iterative step that seeks to reduce any discrepancy between the model and the sample covariance (Hooper et al., 2008). The GoF

statistics for the structural model are presented in Table 8-15, and it is clear that the indices confirm that the model has a good fit with the observed data.

Table 8-15: Goodness of Fit Indices Results for the Structural Model

Chi-square $\chi^2 = 372.518$, p < 0.001	The results of proposed model fit
N	215
Normed chi-square χ^2/df	1.79
RMSEA	0.096
CFI	0.945
RMR	0.013
SRMR	0.076
TLI	0.918
GFI	0.923

**Note: df = degree of freedom; Normed chi-square or ratio of likelihood (χ^2) to degrees of freedom = χ^2/df ; RMSEA = Root mean square error of approximation; TLI = Tucker–Lewis Index; CFI = Comparative fit index.*

**Benchmark for sample size <250 and Variables > 30 (Hair et al., 2010).*

For the Root Mean Square Error of Approximation (RMSEA) method, a lower RMSEA is a sign of improved fit for the model. As can be seen in Table 8-16, the RMSEA test value was 0.096, which indicates a small value. In this fit statistic, PCLOSE is the connected p-value, which in this case was equal to 0.100 > 0.05; this indicates that the hypothesised model fits the data very well (Byrne, 2010).

Table 8-16: Model Fit Indices – RMSEA

Model	RMSEA	LO 90	HI 90	PCLOSE
Default model	.096	.084	.108	.100
Independence model	.335	.326	.343	.000

Overall, in this analysis, the following were used to evaluate model fit: RMSEA, RMR, SRMR, CFI, PCLOSE indices, and degree of freedom (df), along with the chi-square (χ^2), degree of freedom and normed chi-square values. The sample size of this research was 215, and the number of measured variables was 62 items for 20 factors. To conclude, the values of these GoF indices, as shown in Table 8-15 and Table 8-16, confirmed that the model indicates a good fit and the hypothesised 19-factor model fits the sample data. The absolute fit measures

of RSMEA (0.096), PMR (0.013), and SRMR (0.076), as well as the incremental fit measures of TLI (0.918) and CFI (0.945), were above the minimum requirement values. However, the likelihood ratio chi-square (Chi-square (X^2) = 372.518; df = 121, $p=0.0001$) was significant ($p<0.001$).

8.6.5 Assessment of Hypotheses

The theoretical model of the study and the hypothesised relationships within the model were assessed through Path analysis, which was applied in this research to examine the hypothesised relationship of the suggested model, by employing the standardised path coefficients, as presented previously. This section will illustrate, the suggested hypothesised relationships that were tested and supported by the data, in detail, as presented in Table 8-17:

Table 8-17: Summarisation of the Hypotheses Assessment and Results

Hypotheses Path Regression	Results and Discussions of the Hypotheses Assessment	Results
H1: DL ← SA	<p>The Data Leakage (DL) factor is positively related to the Security Awareness (SA) Component, which can be affected by an organisation's decision to adopt the cloud services. DL was found to have a significant direct positive effect on security implementations to adopt the cloud.</p> <p>The standardised direct effect of SA on DL is 0.534, with a critical ratio of 9.411. That is, due to the direct effect of SA on DL, when SA rises by 1 standard deviation, DL rises by 0.534 standard deviations. This is in addition to any indirect effect that SA may have on DL.</p> <p>This result suggests that the path between DL and SA is statistically significant at the $p < 0.001$ level, indicating strong support for the H1 hypothesis proposed in the conceptual model.</p>	Supported

Hypotheses Path Regression	Results and Discussions of the Hypotheses Assessment	Results
H2: AH ← SA	<p>The Account or Service Hijacking (AH) factor is positively related to the Security Awareness (SA) Component, which can affect an organisation's decision to adopt the cloud services. AH was found to have a significant direct influence and positive effect on security implementations to adopt the cloud. The standardised direct effect of SA on AH is 0.771, with a critical ratio of 9.553.</p> <p>That is, due to the direct effect of SA on AH, when SA rises by 1 standard deviation, AH rises by 0.771 standard deviations. This is in addition to any indirect effect that SA may have on AH.</p> <p>This result proposes that the path between AH and SA is statistically significant at the $p < 0.001$ level, thus indicating strong support for the H2 hypothesis proposed in the conceptual model.</p>	Supported
H43: PR ← SA	<p>The Privacy (PR) factor is positively related to the Security Awareness (SA) Component, which can affect an organisation's decision to adopt the cloud services. PR was found to have a significant direct influence and positive effect on security implementations to adopt the cloud.</p> <p>The standardised direct effect of SA on AH is 0.696, with a critical ratio of 9.842. That is, due to the direct effect of SA on PR, when SA rises by 1 standard deviation, PR rises by 0.696 standard deviations.</p> <p>This is in addition to any indirect effect that SA may have on PR. This result proposes that the path between PR and SA is statistically significant at the $p < 0.001$ level, thus indicating strong support for the H3 hypothesis proposed in the conceptual model.</p>	

Hypotheses Path Regression	Results and Discussions of the Hypotheses Assessment	Results
H4: SC ← SR	<p>The Security Culture (SC) factor is positively related to the Security Risks (SR) Component, which can affect an organisation's decision to adopt the cloud services. SC was found to have a significant direct influence and positive effect on security implementations to adopt the cloud.</p> <p>The standardised direct effect of SR on SC is 0.64, with a critical ratio of 8.242. That is, due to the direct effect of SR on SC, when SR rises by 1 standard deviation, SC rises by 0.64 standard deviations. This is in addition to any indirect effect that SR may have on SC.</p> <p>This result proposes that the path between SC and SR is statistically significant at the $p < 0.001$ level, thus indicating strong support for the H4 hypothesis proposed in the conceptual model.</p>	Supported

Hypotheses Path Regression	Results and Discussions of the Hypotheses Assessment	Results
H5: ST ← SR	<p>The Shared Technology (ST) factor is positively related to the Security Risks (SR) Component, which can affect an organisation's decision to adopt the cloud services. ST was found to have a significant direct influence and positive effect on security implementations to adopt the cloud.</p> <p>The standardised direct effect of SR on ST is 0.747, with a critical ratio of 8.407.</p> <p>That is, due to the direct effect of SR on ST, when SR rises by 1 standard deviation, ST rises by 0.747 standard deviations. This is in addition to any indirect effect that SR may have on ST.</p> <p>This result proposes that the path between ST and SR is statistically significant at the $p < 0.001$ level, thus indicating strong support for the H5 hypothesis proposed in the conceptual model.</p>	Supported
	<p>The Insecure Interface (II) factor is positively related to the Security Risks (SR) Component, which can affect an organisation's decision to adopt the cloud services.</p> <p>II was found to have a significant direct influence and positive effect on security implementations to adopt the cloud. The standardised direct effect of SR on II is 0.622, with a critical ratio of 9.692. That is, due to the direct effect of SR on II, when SR rises by 1 standard deviation, II rises by 0.622 standard deviations.</p> <p>This is in addition to any indirect effect that SR may have on II. This result proposes that the path between II and SR is statistically significant at the $p < 0.001$ level, thus indicating strong support for the H6 hypothesis proposed in the conceptual model.</p>	

Hypotheses Path Regression	Results and Discussions of the Hypotheses Assessment	Results
H7: DO ← SR	<p>The Data Ownership (DO) factor is positively related to the Security Risks (SR) Component, which can affect an organisation's decision to adopt the cloud services.</p>	
	<p>DO was found to have a significant direct influence and positive effect on security implementations to adopt the cloud. The standardised direct effect of SR on DO is 0.874, with a critical ratio of 7.658.</p>	
	<p>That is, due to the direct effect of SR on DO, when SR rises by 1 standard deviation, DO rises by 0.874 standard deviations. This is in addition to any indirect effect that SR may have on DO.</p>	
	<p>This result proposes that the path between DO and SR is statistically significant at the $p < 0.001$ level, thus indicating strong support for the H7 hypothesis proposed in the conceptual model.</p>	Supported

Hypotheses Path Regression	Results and Discussions of the Hypotheses Assessment	Results
H8: SDI ← SR	<p>The Service and Data Integration (SDI) factor is positively related to the Security Risks (SR) Component, which can affect an organisation's decision to adopt the cloud services.</p> <p>SDI was found to have a significant direct influence and positive effect on security implementations to adopt the cloud. The standardised direct effect of SR on SDI is 0.819, with a critical ratio of 8.842. That is, due to the direct effect of SR on DO, when SR rises by 1 standard deviation, SDI rises by 0.819 standard deviations.</p> <p>This is in addition to any indirect effect that SR may have on SDI. This result proposes that the path between SDI and SR is statistically significant at the $p < 0.001$ level, thus indicating strong support for the H8 hypothesis proposed in the conceptual model.</p>	Supported
H9: MI ← SR	<p>The Malicious Insider (MI) factor is positively related to the Security Risks (SR) Component, which can affect an organisation's decision to adopt the cloud services.</p> <p>MI was found to have a significant direct influence and positive effect on security implementations to adopt the cloud. The standardised direct effect of SR on MI is 0.674, with a critical ratio of 9.195. That is, due to the direct effect of SR on MI, when SR rises by 1 standard deviation, MI rises by 0.674 standard deviations.</p> <p>This is in addition to any indirect effect that SR may have on MI. This result proposes that the path between MI and SR is statistically significant at the $p < 0.001$ level, thus indicating strong support for the H9 hypothesis proposed in the conceptual model.</p>	Supported

Hypotheses Path Regression	Results and Discussions of the Hypotheses Assessment	Results
H10: CSE ← SR	<p>The Failure of Client-side Encryption (CSE) factor is positively related to the Security Risks (SR) Component, which can affect an organisation's decision to adopt the cloud services.</p> <p>CSE was found to have a significant direct influence and positive effect on security implementations to adopt the cloud. The standardised direct effect of SR on CSE is 0.860, with a critical ratio of 9.029. That is, due to the direct effect of SR on CSE, when SR rises by 1 standard deviation, CSE rises by 0.860 standard deviations. This is in addition to any indirect effect that SR may have on CSE.</p> <p>This result proposes that the path between CSE and SR is statistically significant at the $p < 0.001$ level, thus indicating strong support for the H10 hypothesis proposed in the conceptual model.</p>	Supported
H11: SS ← SB	<p>The Smart Scalable Security Benefits (SS) factor is positively related to the Security Benefits (SB) Component, which can affect an organisation's decision to adopt the cloud services. SS was found to have a significant direct influence and positive effect on security implementations to adopt the cloud.</p> <p>The standardised direct effect of SB on SS is 0.941, with a critical ratio of 8.321. That is, due to the direct effect of SB on SS, when SB rises by 1 standard deviation, SS rises by 0.941 standard deviations.</p> <p>This is in addition to any indirect effect that SB may have on SS. This result proposes that the path between SS and SB is statistically significant at the $p < 0.001$ level, thus indicating strong support for the H11 hypothesis proposed in the conceptual model.</p>	Supported

Hypotheses Path Regression	Results and Discussions of the Hypotheses Assessment	Results
H12: RC ← SB	<p>The Resource Concentration (RC) factor is positively related to the Security Benefits (SB) Component, which can affect an organisation's decision to adopt the cloud services. RC was found to have a significant direct influence and positive effect on security implementations to adopt the cloud.</p> <p>The standardised direct effect of SB on RC is 0.895, with a critical ratio of 9.267. That is, due to the direct effect of SB on RC, when SB rises by 1 standard deviation, RC rises by 0.895 standard deviations. This is in addition to any indirect effect that SB may have on RC.</p> <p>This result proposes that the path between RC and SB is statistically significant at the $p < 0.001$ level, thus indicating strong support for the H12 hypothesis proposed in the conceptual model.</p>	Supported
H13: SSI ← SB	<p>The Standardised Security Interfaces (SSI) factor is positively related to the Security Benefits (SB) Component, which can affect an organisation's decision to adopt the cloud services. SSI was found to have a significant direct influence and positive effect on security implementations to adopt the cloud.</p> <p>The standardised direct effect of SB on SSI is 0.902, with a critical ratio of 9.058. That is, due to the direct effect of SB on SSI, when SB rises by 1 standard deviation, SSI rises by 0.902 standard deviations.</p> <p>This is in addition to any indirect effect that SB may have on SSI. This result proposes that the path between SSI and SB is statistically significant at the $p < 0.001$ level, thus indicating strong support for the H13 hypothesis proposed in the conceptual model.</p>	Supported

Hypotheses Path Regression	Results and Discussions of the Hypotheses Assessment	Results
H14: SLA ← SB	<p>The Services Level Agreement Audit Enforcement (SLA) factor is positively related to the Security Benefits (SB) Component, which can affect an organisation's decision to adopt the cloud services.</p> <p>SLA was found to have a significant direct influence and positive effect on security implementations to adopt the cloud. The standardised direct effect of SB on SLA is 0.952, with a critical ratio of 9.511. That is, due to the direct effect of SB on SLA, when SB rises by 1 standard deviation, SLA rises by 0.952 standard deviations. This is in addition to any indirect effect that SB may have on SLA.</p> <p>This result proposes that the path between SLA and SB is statistically significant at the $p < 0.001$ level, thus indicating strong support for the H14 hypothesis proposed in the conceptual model.</p>	Supported
H15: CS ← SB	<p>The Cloud Security Auditing (CS) factor is positively related to the Security Benefits (SB) Component, which can affect an organisation's decision to adopt the cloud services. CS was found to have a significant direct influence and positive effect on security implementations to adopt the cloud. The standardised direct effect of SB on CS is 0.846, with a critical ratio of 9.677.</p> <p>That is, due to the direct effect of SB on CS, when SB rises by 1 standard deviation, CS rises by 0.846 standard deviations. This is in addition to any indirect effect that SB may have on CS.</p> <p>This result proposes that the path between CS and SB is statistically significant at the $p < 0.001$ level, thus indicating strong support for the H15 hypothesis proposed in the conceptual model.</p>	Supported

Hypotheses Path Regression	Results and Discussions of the Hypotheses Assessment	Results
H16: AS ← SB	<p>The Advance Security Mechanism (AS) factor is positively related to the Security Benefits (SB) Component, which can affect an organisation's decision to adopt the cloud services. AS was found to have a significant direct influence and positive effect on security implementations to adopt the cloud.</p> <p>The standardised direct effect of SB on AS is 0.936, with a critical ratio of 9.779. That is, due to the direct effect of SB on AS, when SB rises by 1 standard deviation, AS rises by 0.936 standard deviations.</p> <p>This is in addition to any indirect effect that SB may have on AS. This result proposes that the path between AS and SB is statistically significant at the $p < 0.001$ level, thus indicating strong support for the H16 hypothesis proposed in the conceptual model.</p>	Supported
H17: CE ← SB	<p>The Cutting-edge Security Marketing (CE) factor is positively related to the Security Benefits (SB) Component, which can affect an organisation's decision to adopt the cloud services.</p> <p>CE was found to have a significant direct influence and positive effect on security implementations to adopt the cloud. The standardised direct effect of SB on AS is 0.817, with a critical ratio of 7.022.</p> <p>That is, due to the direct effect of SB on CE, when SB rises by 1 standard deviation, CE rises by 0.936 standard deviations. This is in addition to any indirect effect that SB may have on CE.</p> <p>This result proposes that the path between CE and SB is statistically significant at the $p < 0.001$ level, thus indicating strong support for the H17 hypothesis proposed in the conceptual model.</p>	Supported

Hypotheses Path Regression	Results and Discussions of the Hypotheses Assessment	Results
H18: CR ← SB	<p>The Failure of Compliance with Regulations (CR) factor is positively related to the Security Benefits (SB) Component, which can affect an organisation's decision to adopt the cloud services. CR was found to have a significant direct influence and positive effect on security implementations to adopt the cloud. The standardised direct effect of SB on CR is 0.770, with a critical ratio of 7.866.</p> <p>That is, due to the direct effect of SB on CR, when SB rises by 1 standard deviation, CR rises by 0.770 standard deviations. This is in addition to any indirect effect that SB may have on CR. This result proposes that the path between CR and SB is statistically significant at the $p < 0.001$ level, thus indicating strong support for the H18 hypothesis proposed in the conceptual model.</p>	Supported
H19: TR ← SB	<p>The Trust (TR) factor is positively related to the Security Benefits (SB) Component, which can affect an organisation's decision to adopt the cloud services. TR was found to have a significant direct influence and positive effect on security implementations to adopt the cloud. The standardised direct effect of SB on TR is 0.693, with a critical ratio of 10.030. That is, due to the direct effect of SB on TR, when SB rises by 1 standard deviation, TR rises by 0.693 standard deviations.</p> <p>This is in addition to any indirect effect that SB may have on TR. This result proposes that the path between TR and SB is statistically significant at the $p < 0.001$ level, thus indicating strong support for the H19 hypothesis proposed in the conceptual model.</p>	Supported

Additionally, the results indicate that the Security Benefits component had a direct effect on an organisation's decision to adopt cloud computing services. The standardised estimate loading of the Security Benefits Component is 0.614, with a critical ratio of 9.727. This result showed that the path valued among security benefits and an decision of organisation's to adopt cloud computing at the $p < 0.001$ level is statistically significant, thus strongly supporting the hypothesis proposed in the theoretical model. It could therefore be concluded that the Security Benefits Component has a positive influence on an organisation's decision to adopt cloud computing.

The Security Risk Component was found to have a significant direct effect on an organisation's decision to adopt cloud computing services. The standardised estimate loading of the Security Risk component is 0.516, with a critical ratio of 8.723. This outcome showed that the path estimated between security risk and an decision of organisation's to adopt cloud computing at the $p < 0.001$ level is statistically significant, thus strongly supporting the hypothesis proposed in the theoretical model. It could therefore be concluded that the Security Risk Component has an influence on an organisation's decision to adopt cloud computing.

The effect of the Security Awareness Component on an decision of organisation's to adopt cloud computing was positive, with stronge effect loading of 0.704, and a critical ratio of 6.620. This result showed that the path estimated between security awareness and an decision organisation's to adopt cloud computing at the $p < 0.001$ level is statistically significant, thus strongly supporting the hypothesis proposed in the theoretical model. It could therefore be concluded that the Security Awareness Component has a positive influence on an decision of organisation's to adopt cloud computing. Overall, the results of the hypotheses assessment showed that all three components of the model have a positive significant direct effect on an organisation's decision to adopt the cloud.

Therefore, it is clear that the outcomes confirm the model proposed in this study; furthermore, these results demonstrate the suitability of the proposed theoretical model for security cloud computing adoption. All hypotheses are confirmed and have significant paths in the model, as shown in Figure 8-4.

The findings of this study are also consistent with the views of experts and previous studies. In reference to this point, Almorsy *et al.* (2016) found that cloud security risks and variables related to cloud security risks influence the adoption of cloud computing. Furthermore, Changchit and Chuchuen (2016) revealed that security risks and security advantages always play a major role in cloud computing adoption in organisations, especially in developing countries. It is not surprising that cloud computing adoption may be subject to cloud computing security risks and benefits. The findings of this study recommend that organisations educate customers regarding the security of cloud computing. The main goal of conducting SEM in this study is to provide predictive security related factors and guidelines which will allow government organisations to make decisions regarding cloud adoption in full knowledge of what it can deliver.

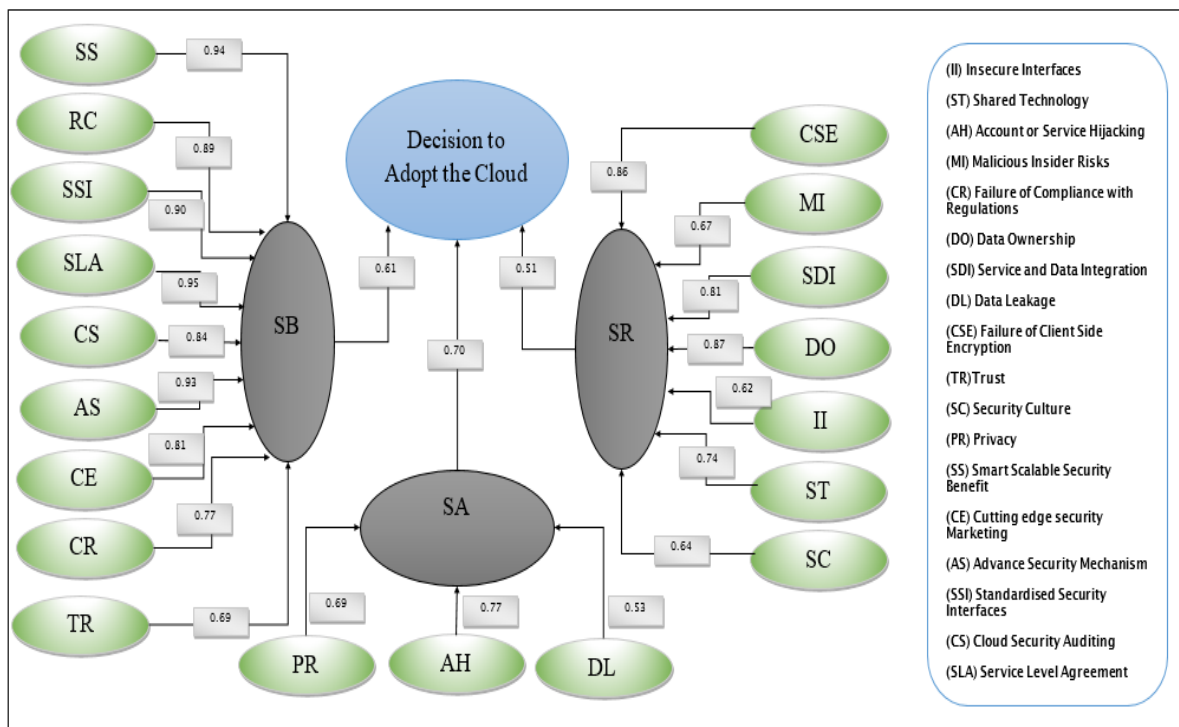


Figure 8-4: Path Diagram of the Structural Model with Direct Effect

8.7 Concluding Comments

This chapter detailed the results from the preliminary analysis of the data, including the data missing from all data collected. In addition, discussion focused on the first part of the instrument, namely demographic information. The data was analysed using IBM SPSS 24 to elicit respondents' demographic information. This chapter also presented the results of data analysis focused on model reliability and validation approaches. The instrument was distributed to security specialists in Saudi organisations, and 215 viable responses were used. In order to arrange the most suitable data for multivariate analysis, the data was examined for missing values.

The results related to the missing data were assessed using the pairwise approach, while the total number of respondents used for analysis in this study, after excluding data with incomplete and random answers, stood at 215. The first part of the instrument was the demographic information section, the purpose of which was to determine the characteristics of the organisations participating in this research. The results of the descriptive and frequency analyses of the demographic information show that more than 30% of organisations used the cloud, but more than 84% of them were concerned about security; this substantially affected other organisations' decision to adopt the cloud computing services.

The research used a measurement of construct internal reliability, namely the Cronbach's alpha statically analysis test. The results of the study generated an overall Cronbach alpha value of 0.865, while the Cronbach's alpha values for most of the constructs were ranged between 0.6 and 0.9, thus indicating very good internal consistency of the items' rating scores. The study also pointed out that there was strong agreement regarding security cloud adoption across the 19 factors. Those factors are: "*Insecure interfaces, Shared technology, Account or Service Hijacking, Malicious Insider Risks, Failure of Compliance with Regulations, Data Ownership, Service and Data Integration, Data Leakage, Failure of Client-side Encryption, Trust, Security Culture, Privacy, Smart Scalable Security Benefits, Cutting Edge Security Marketing, Advance Security Mechanism, Standardised Security Interfaces, Cloud Security Auditing, SLA Audit Enforcement, and Resource Concentration*".

Exploratory factor analysis (EFA) and confirmatory factor analysis (CFA) were applied in order to test the data obtained from the security cloud adoption instrument. EFA was performed, and 19 factors were extracted and retained for further investigation. All of the latent factors had a high loading. A Kaiser-Meyer-Olkin (KMO) was carried out, and yielded a value of 0.881, thus suggesting that the factor analysis, as a statistical measure, was suitable for the instrument data.

Moreover, the sample of data had to be subjected to initial suitability considerations before factor analysis could be performed. After applying the correlation between the extracted factors, the correlation matrix showed a good relationship between factors. Principal component analysis (PCA) was used in this analysis, since it is an applicable method with this kind of instrument.

Following this, the rotation was applied; the decision was taken to rerun the analysis for each of these components while rotating them once obliquely and once orthogonally. A total of six runs were conducted, and of these combinations, the most interpretable solution was discovered after using orthogonal rotation, with three components extracted. In addition to this, numerous steps were undertaken in CFA: describing individual constructs, developing the measurement model, using existing instrument data to produce empirical results, and assessing the model's validity. In evaluating the model's validity, some validity and reliability tests were considered, such as construct reliability, convergent validity, discriminant validity, and the reliability of the measurement model.

Following EFA, the next stage in the analysis was applying Confirmatory Factor Analysis (CFA) to the data; the hypothesised measurement model comprised 62 pre-specified item indicators and 20 constructs. This section summarises the results of SEM for the data grouped using Factor Analysis. Given the significant value, the results of the fit statistics, which sought to establish whether the model was fit are as follow: $\chi^2/df = 1.79$, GFI=0.923, CFI= 0.945, TLI= 0.918, RAR= 0.013, SRAR= 0.076. Theses fit indices results are in fact show that the model fit the data well.

In terms of the structural model analysis, the outcome, as presented in this chapter, showed that the construct variables had direct effects. This chapter also revealed how, through standardised path coefficients, it was found that all hypotheses indicate that security factors proposed in the model had a positive influences on cloud adoption in Saudi government organisations. The main goal of conducting SEM in this chapter was to provide predictive factors which could help organisations to make decisions regarding the adoption of cloud computing services. Following on from this, the next chapter will present conclusions, theoretical contributions, practical contributions and future research directions.

Chapter 9: Future Work

While the previous chapter discussed the results of the model validation through factor analysis and SEM, this chapter delivers an overview of the research conducted in the KSA. It also provides conclusions regarding the work carried out and how the research questions were answered. Moreover, the chapter outlines and discusses the main and useful contributions of this research. Finally, the chapter recommends directions for future work.

9.1 Conclusions

This research established by delivering an overview of cloud computing in order to outline the basic features of the cloud. The most characteristics of cloud computing services is that it offers assets to multiple users at any time in a dynamic way, and based on these users' needs. Furthermore, users only pay for the services that they need.

The main aim of this research was to investigate and develop a security cloud framework by exploring a number of security factors in cloud computing. As the context of this research focused mainly on Saudi Arabian government organisations, it revealed security factors that were significantly relevant to different technological and organisational aspects. Further exploration of these aspects led to the identification of security factors that affect Saudi organisations' decision to adopt the cloud.

This work identified a gap in the research literature concerning security factors and their influence on cloud computing adoption. In order to understand the experts' behaviour, the literature review was used to identify a number of security factors deemed important when it comes to the adoption of cloud computing services. These factors were reconstructed and filtered to avoid duplication.

In addition, these security factors were regrouped to accommodate the Saudi context, following which the selected security factors were developed into a proposed framework. The research proposed a framework related to the significant factors that encourage a government to, or deter a government from, considering cloud adoption. The literature

review revealed that security in cloud adoption in the KSA is limited, especially in government organisations. As such, this research sought to investigate the security risks, as well as the security social and benefits factors that influence the adoption of cloud computing services in Saudi government organisations. The main aim was to help Saudi government organisations to successfully implement cloud-based services and to be aware of security risks, as well as social and benefits factors when adopting the cloud. The main research question was specified in Chapter 1, and is stated again below:

RQ: 'What is an appropriate framework with which to determine the influence of security factors on the adoption of cloud computing in the Saudi government organisations context?'

In order to answer this main research question, it was divided into six sub-questions, which were answered during two stages of this research, as rigorously described in Table 9-1 and **Error! Reference source not found..**

- **First Stage of this research (Confirmatory Study):**

In a confirmatory study conducted during the first stage of this research, three questions were answered. The purpose of these questions was to explore the attitudes of IT project workers and security experts towards using the cloud. It was also deemed important to investigate the security risk, as well as social and benefits factors that influence Saudi government organisations' decision to adopt cloud computing. Consequently, the findings of confirmatory study in the first stage of this research can be summarised based on the following sub questions:

Q1. What are the security risk factors which affect cloud adoption?

Q2. What are the security benefits factors which affect cloud adoption?

Q3: What are the security social factors which affect cloud adoption?

These questions were answered in two phases. During the first phase, the proposed factors in the framework were identified using a literature review, which is presented in Chapter 2. Confirmation of the framework was achieved using both qualitative and quantitative

methods; semi-structured interviews were carried out with IT and security experts in different government organisations across the KSA.

Moreover, 32 security and IT specialists completed an online questionnaire. The purpose of this questionnaire was to confirm the importance of the security factors proposed in the cloud adoption framework and to identify any missing factors based on the perspectives of the experts. The results from the survey indicated that all of the proposed factors were statistically significant.

Table 9-1: Summary of Methods Used in the First Stage of this Research
(Confirmatory Study)

Questions	Methods	Purpose
Q1. What are the security risk factors which affect cloud computing adoption?	Literature review	To critically review the literature on the cloud adoption approaches and frameworks, while investigating the global context of cloud computing adoption leading to the case of Saudi organisations.
Q2. What are the security benefits factors which affect cloud computing adoption?	Semi-structured Interviews with IT staff and security experts in different Saudi government organisations.	To explore the IT staff and security experts' attitudes toward using the cloud.
Q3: What are the security social factors which affect cloud computing adoption?	Online questionnaire distributed to the IT staff and security experts in different Saudi government organisations.	To assess and investigate the importance of the security factors proposed in the cloud adoption framework. To identify additional factors that were not mentioned in previous studies and are related to the Saudi context. To develop and confirm the security factors that already exist in the proposed framework.

The analysis of the interview outcomes and the questionnaire results identified an additional factor which may affect the adoption of cloud services in Saudi government organisations: Client-side Encryption. The experts also suggested that this factor should be included as a potential risk under the Security Risk Factors category. The initial framework has been updated based on the expert reviews and the questionnaire.

The findings pertaining to the security factors in the framework were all derived from statements made by the experts and IT security specialists in the questionnaire. All experts agreed that security is the top priority in an organisation. If an organisation does not ensure that proper security is in place, then the services will not be reliable or acceptable to the users.

In terms of attitude towards categories and their factors, the experts strongly agreed that these have an impact on the adoption of cloud services in Saudi government organisations. Furthermore, the statistical results of the expert interviews revealed that the answers were strongly significant. Moreover, the questionnaire results indicated that security social attitude and its associated items have an effect on government organisations' intention to adopt cloud computing.

Moving to the Security Risk Factors category, the following factors were statistically confirmed. The results of the interviews revealed that the 12 experts agreed that these factors are either important or very important when it comes to the adoption of cloud computing in Saudi government organisations; they also concluded that these factors have a significant impact on stakeholders' behaviour when adopting cloud services.

The results of the interviews specified that the security social factors category, and its sub-factors, are essential to any government organisations when deciding whether or not to adopt the cloud. Upon examining the expert reviews, it is clear that security culture, trust, and privacy were deemed to be very important factors; none of the experts disagreed with the statement that "these factors are essential to helping organisations use cloud services".

Finally, from the perspective of the experts interviewed, the cloud computing service provides a number of benefits to users. This research showed that, with regard to the security benefits category

Regards to the suggested factors from expert interviews, the experts were also asked to suggest any other factors, not included in the proposed security adoption framework that they felt could have an influence on the adoption of the cloud. When asked to make these suggestions, the experts placed particular emphasis on one factor that they felt KSA government organisations should take into account when adopting the cloud, namely Failure of Client-side encryption.

This revelation makes client-side encryption an important factor. The perception is that every part of the data should be encrypted on the client-side in a way which means that even an attacker with substantial computing power cannot access the confidential information or violate end-users' privacy. Indeed, there is also the perception that, if this were the case, then the use of a cloud service would not influence information policies (Souza and Puttini, 2016).

Client-side encryption obviously increases users' ability to protect data and files. By rejecting viewing access to servers and service providers, client-side encryption guarantees that the data and files that are stored in the cloud stay private, thus eliminating the chance that critical information or photos can be accessed, stolen or leaked (Xu et al., 2013). This was deemed to be an important factor, with five of the experts suggesting that it should be added to the framework. They pointed out this factor, as it has a beneficial effect on stakeholders' attitude towards using cloud services. As such, this factor was included in the security risks category in the framework.

In summary, the results showed that 'there is a positive attitude to adopt cloud services in KSA government organisations: 75% of participants specified that their organisations expect to adopt cloud computing services in the near future'.

- **Second Stage of this research (Validation Study):**

With regards the validation study conducted during the second stage of this research and based on the confirmed framework, three questions were answered, as presented in Table 9-2, which also lists the details and purpose of the methods used. The research developed an instrument intended to measure the affecting of the decision by the KSA organisations to adopt cloud computing, based on the confirmed security cloud framework.

Table 9-2: Summary of Methods Used in the Second Stage of this Research

Questions	Methods	Purpose
Q4: What is a suitable instrument with which to evaluate security factors in the cloud adoption framework and how can the instrument be validated?	Instrument distributed to 215 IT specialists and security experts.	To measure the effectiveness of the decision of the KSA organisations to adopt cloud computing, based on the security cloud framework which was confirmed during the first stage of this research. To evaluate and validate the security cloud adoption model.
	Content Validity Pre-test	To assess whether an item is applicable and sufficient in examining the concept being studied. To ensure that all questions' wording, response format, instructions, instrument length, and layout are appropriate. To ensure that the instrument as a whole is easy to read and understandable.
Q5: What are the relationship(s) among the security factors (identified from factor analysis and structural equation modelling)? Q6: Which relationship(s) of security factors will affect the Saudi government organisations' decision to adopt the cloud computing services?	Exploratory Factor Analysis & Confirmatory Factor Analysis (Structural Equation Modelling (SEM))	To measure the strength of the relationship(s) between independent and dependent variables. To explore factors that have a strong influence, both positive and negative, on government organisations' adoption of cloud services. To test the developed security model for cloud adoption. To evaluate how good the fit of this model is.

A quantitative technique was utilised during validation stage. The instrument was used to collect data on the security factors which have an effect on the adoption of cloud computing

in KSA government organisations. Literature was reviewed in order to develop the instrument statements, which were related to cloud security factors that affect the decision of cloud adoption. The instrument was designed to evaluate the factors within the security cloud adoption framework.

The findings of validation study can be summarised as followed: based on the confirmed framework in the first stage of this research, an instrument was developed to survey Saudi government organisations and to explore and confirm the relationships between the security factors in the framework. The instrument development and validation which was used to evaluate and validate the security cloud adoption model of this study by addressing the following research question:

Q4: What is the appropriate instrument to evaluate security factors in the cloud adoption framework and how can the instrument be validated?’

Based on the instrument development in this study, validity and reliability issues were given consideration. Validity is seen as the foundation of defining the accuracy of the findings that the researcher is trying to measure. In this study, two tests were conducted to validate the instrument; pre-test and content validity.

Thus, the results of these tests exposed that the instrument delivered an influence measurement of the developed variables. With the first test of the validation study, namely the pre-test, the instrument contained 20 factors, while 67 items were evaluated. The test involved seven experts, four of whom were from the IT and security experts from Saudi security groups, while three were researcher’s from computer science. The second test used to validate the instrument was content validity.

The content validity ratio (CVR) was used to assess the results of the instrument’s content validity test, based on the thoughts of the seven experts who participated in the judgment quantification; the statistical significance level for each factor was also assessed (Lawshe, 1975).

The results of the content validity ratio showed only from the pool of 67 items, only 62 items were significant at the range of more than 0.50, and only five of the items were insignificant, because their significance levels were lower than 0.50; they were subsequently removed from the instrument. Consequently, this content validity ratio (CVR) identified that the security items in the cloud computing adoption framework had acceptable content validity, thus meaning that the items measured the model being studied. After these experiments, 30 security experts were invited to participate in this research. Slight modifications to the final design of the instrument were made upon receiving the feedback. The modifications were made to the original instrument and the final instrument was developed.

The internal consistency reliability was acceptable. Good Cronbach's alpha results also proved that the items used to measure each factor were independent measures and positivity correlated with each other. The overall reliability outcome for all factors was .645, and thus it was possible to conclude that the 20 factors and 62 items had excellent reliability (Bryman and Cramer, 2001; Hair et al., 2010).

The findings of this stage of this research, approximately 215 of IT specialists and security experts in different departments of the KSA government organisations completed the instrument. These organisations included ministries, telecommunication organisations, state universities, research institutes, and education facilities. The collected data was analysed through two stages. Firstly, Exploratory Factor Analysis (EFA) was implemented in order to propose an initial model, since no prior models, as such, exist in the literature; a model was built from scratch. Secondly, Confirmatory Factor Analysis (using Structural Equation Modelling) was applied to validate the initial model during the confirmatory stage. The motivation of this analysis was to answer the fifth and sixth sub-questions:

Q5: What are the relationship(s) among the security factors identified from factor analysis and structural equation modelling?

Q6: Which relationship(s) of security factors will affect the Saudi government organisations' decision to adopt the cloud computing services?

Based on these questions, the results from the preliminary analysis of the data, including the data missing from all data collected. The data was analysed using IBM SPSS 24 to elicit

respondents' demographic information. The instrument was distributed to security specialists in Saudi organisations, and 215 viable responses were used. In order to arrange the most suitable data for multivariate analysis, the data was examined for missing values.

The results related to the missing data were assessed using the pairwise approach, while the total number of respondents used for analysis in this study, after excluding data with incomplete and random answers, stood at 215. The first part of the instrument was the demographic information section, the purpose of which was to determine the characteristics of the organisations participating in this research. The results of the descriptive and frequency analyses of the demographic information show that more than 30% of organisations used the cloud, but more than 84% of them were concerned about security; this substantially affected other organisations' decision to adopt the cloud computing services.

The research used a measurement of construct internal reliability, namely the Cronbach's alpha statically analysis test. The results of the study generated an overall Cronbach alpha value of 0.865, while the Cronbach's alpha values for most of the constructs were ranged between 0.6 and 0.9, thus indicating very good internal consistency of the items' rating scores.

Exploratory factor analysis (EFA) and confirmatory factor analysis (CFA) were applied in order to test the data obtained from the security cloud adoption instrument. EFA was performed, and 19 factors were extracted and retained for further investigation. All of the latent factors had a high loading. A Kaiser-Meyer-Olkin (KMO) was carried out, and yielded a value of 0.881, thus suggesting that the factor analysis, as a statistical measure, was suitable for the instrument data.

Moreover, the sample of data had to be subjected to initial suitability considerations before factor analysis could be performed. After applying the correlation between the extracted factors, the correlation matrix showed a good relationship between factors. Principal component analysis (PCA) was used in this analysis, since it is an applicable method with this kind of instrument.

Following this, the rotation was applied; the decision was taken to rerun the analysis for each of these components while rotating them once obliquely and once orthogonally. A total of six runs were conducted, and of these combinations, the most interpretable solution was discovered after using orthogonal rotation, with three components extracted. In addition to this, numerous steps were undertaken in CFA: describing individual constructs, developing the measurement model, using existing instrument data to produce empirical results, and assessing the model's validity. In evaluating the model's validity, some validity and reliability tests were considered, such as construct reliability, convergent validity, discriminant validity, and the reliability of the measurement model. Following EFA, the next stage in the analysis was applying Confirmatory Factor Analysis (CFA) to the data; the hypothesised measurement model comprised 62 pre-specified item indicators and 20 constructs.

In terms of the structural model analysis, the outcome showed that the construct variables had direct effects and it was found that all hypotheses indicate that security factors proposed in the model had a positive influences on cloud adoption in Saudi government organisations. The main goal of conducting SEM in this analysis was to provide predictive factors which could help organisations to make decisions regarding the adoption of cloud computing services.

The conclusions of the validation study part confirmed that the proposed model fit well with the collected data. In addition, the outcomes presented that the factors had a direct impact on an organisation's decision to adopt the cloud. In summation, it can be determined that the proposed model is valuable in explaining the adoption of the cloud in organisations. Moreover, it is supposed that the outcomes of this research can help decision makers, cloud providers and researchers in formulating reputable strategies which will encourage the adoption of cloud computing. The outcomes of this study can also enhance the above-mentioned parties' awareness and considerate of why some government organisations are implementing the cloud, while some are not.

9.2 Fulfilling the Objectives of this Research

This section details the way in which the aims and objectives of the present study were fulfilled. In order to achieve said aims and objectives, one main question and six sub-questions were identified, as stated in Chapter 1.

The first three questions sought to establish the security factors (Risk, Social, and Benefit) that may affect KSA government organisations in adopting cloud computing services. These three questions were addressed by providing a critical and comprehensive literature review, as discussed in Chapter 2 and Chapter 3. A total of 18 security factors were identified and explained in detail as potential factors that may affect the adoption of cloud computing in the government organisations context. As a result, the hypotheses of the present study were designed and tested during the first stage of this research. These factors were also examined by conducting interviews with experts and a questionnaire-based survey (see Chapter 4 and Chapter 5). One factor was added due to the experts' suggestions after the results of the first stage of the study had already been obtained. As such, in total, 19 security factors were confirmed. The third, fourth and sixth questions were answered in the second stage of this study. These questions were answered by conducting a study using the same instrument with a large number of cases, involving IT specialists and security experts in different departments of KSA government organisations, as presented in Chapter 6, Chapter 7 and Chapter 8. The data analysis of the validation study – which was presented in Chapter 8- showed that the model fit indices were good.

As a result of this research, the model was developed and validated; the empirical evidence resulting from the full study will contribute to the literature on cloud computing, and provide a 'Potential for success' rate for cloud computing adoption projects. This can, in turn, aid the decision-making process when organisations are choosing whether or not to adopt cloud computing. The results from this study will give IT practitioners and cloud service providers corroborated experimental data that can inform the engagement and marketing of cloud computing projects. Moreover, KSA government organisations could use the model in order to help encourage their organisations to use and then adopt the cloud computing services. Additionally, as the results of this research contribute to knowledge on the subject of the cloud, it may be possible for this developed model to be used in other countries in the Middle East; after all, most of these countries are similar and share many things, such as language, religion, and culture.

9.3 Research Contributions

The general outcomes of this research have contributed to, and extended, knowledge in area of cloud computing services and security in cloud adoption in a government organisations context. Cloud computing is valuable for general organisations as well as corporations. The adoption level in KSA is in the early stage. As previously mentioned, Saudi government organisations have particular characteristics, and their vision is to implement and promote communication and IT systems with a view to realising an IT community and a digital economy.

On the other hand, there are certain organisations that still worry about the idea of moving their present system to the cloud. Several published works have made efforts to help decision makers address their concerns about cloud adoption. These studies are truly remarkable, in that most of the proposed frameworks and identified security factors have focused on pinpointing the benefits of adopting cloud computing. Furthermore, the majority of prior studies have not considered the security risks, security social factors, or security benefits associated with the adoption of cloud computing in KSA government organisations. Given this situation, it was essential to recognise the issues affecting security cloud adoption. After reviewing these previous studies, it was clear, to the best knowledge of the researcher, that no formal studies had examined or combined the security factors that affect cloud adoption in Saudi government organisations. As such, this research made three specific contributions, as follows:

9.3.1 First Contribution

The first contribution of this research is the framework; the present study sought to find an appropriate framework related to the security of cloud computing services in KSA government organisations. A review of the literature identified security factors that may affect the adoption of cloud computing in organisations. This review, which improves existing knowledge in the field, proposed 19 security factors.

The framework was constructed following the literature review on technology acceptance and industrial organisations; the purpose of said framework was to answer the main research

question, 'What is an appropriate framework for the adoption of cloud computing in the Saudi government organisations context?'. This framework was developed and confirmed. The framework was confirmed using the triangulation approach. The process of this contribution was assessed using different methods in the confirmatory study: expert interviews and questionnaires. Expert interviews were used to confirm the identified factors, and to pinpoint factors which had not been mentioned by previous studies. This process was achieved by interviewing IT and security experts, and surveying practitioners in different Saudi government organisations. Expert interviews confirmed the identified factors and suggested another factor, namely Failure of Client-side Encryption. As a result of this process, the security cloud framework was then developed and confirmed.

9.3.2 Second Contribution

The second contribution of this research is the production of a specific instrument. The instrument was developed to measure the effectiveness of the decision by the KSA organisations to adopt cloud computing. It was developed based on literature reviews and the opinions of Saudi security experts. Moreover, the instrument was validated and modified to suit the requirements of this research. The processes involved in developing the instrument resulted in a well-designed instrument that can be used in future studies related to this field.

9.3.3 Third Contribution

The third contribution of this research is a security model capable of establishing the relationships between the security factors. The instrument was used in order to identify the relationships between security factors and to evaluate the final model. The results of this research showed that the model fit the data well. Therefore, it could be stated that the developed model is valid, and thus it is strongly recommended that said model be used in Saudi government organisations which are planning to adopt cloud services.

This model includes three categories. The first category is Security Risk Factors (*Insecure Interfaces Programming, Shared Technology, Account or Service Hijacking, Malicious Insiders, Failure to Comply with Regulations, Data Ownership, Service or Data Integration and Data*

Leakage). The second category is Security Social Factors (*Trust, Security Culture, and Privacy*), while the third category is Security Benefit Factors (*Smart Scalable Security Benefits, Cutting-Edge Cloud Security Market, Advanced Security Mechanism, Standardised Security Interfaces, Cloud Security Auditing and SLA Audit Enforcement*).

The model developed in this thesis can be used for cloud computing adoption in public KSA organisations. It also makes relevant suggestions on how to achieve a favourable implementation environment for the adoption of cloud computing. The findings of this thesis will help to increase the security perceptions of users, and therein lies a milestone for academics and institutions with regard to future work. Lastly, this research signifies one of the first in-depth attempts to establish how participants can make the adoption of cloud security successful.

9.4 Research Implications

This study has made a determination to make a significant contribution to the subject of cloud adoption in KSA organisations. Further, the obtained research data and outcomes will serve as valuable information for policymakers, practitioners, and researchers. The implications of the outcomes of this study, from the methodological and practical perspectives, are discussed in the present section.

9.4.1 Implications for Government Organisations

The results of this research indicated that the physical location of cloud data centres has a substantial influence on compliance with regulations and on privacy, since each country has different policies and regulations. To avoid concerns about the regulation and compliance, there is an essential need for provision from the government context. The KSA government department's services have to work to present appropriate regulations or update their current regulations to meet the terms of the requirements of the cloud services.

9.4.2 Implications for Security Practitioners

For security practitioners, the security cloud model presented in this study is helpful in terms of allowing them to break down the concept of security in cloud adoption into smaller,

theoretically distinct and adaptable security factors to support the project of security in cloud adoption.

9.4.3 Implications for Researchers

For researchers, the security cloud model delivers a common framework which will allow them to theorise and simplify their research, so that they can more easily see how the security factors suitable into the wide picture. In addition, this study offers a valued information source for upcoming researchers in the field of security and cloud adoption, and also in the area of new technologies adoption in general.

9.5 Future Work Directions

Despite the fact that the research objectives were achieved, the study suffered from some limitations. These limitations can be used to help the researcher determine future directions for this work.

As clearly seen in the above chapters, and specifically Section 8.6.5, the framework presented delivers new empirical results related to perceptions and benefits regarding the security implementation factors of cloud adoption in the Saudi government organisations context.

It is certainly true that this research discussed the security factors that influence the adoption of cloud computing services in Saudi government organisations; indeed, these factors were analysed and validated using exploratory factor analysis and confirmatory factor analysis (Structural Equation Modelling (SEM)) techniques. With this said, however, future directions for this research could involve utilising other research methods, including case studies, which can be carried out by interviewing different experts in various organisations. Case studies allow a researcher to employ the research instruments and models in real world settings, so that they can be revalidated in different contexts in order to improve their content. The case studies should involve the use of multiple techniques and data sources to explore or explain the research phenomena.

Moreover, it may be effective to extend this model to a wider context in order to improve said model by providing detailed guidelines on the various steps and measures which organisations need to follow; this could well lead to the formulation of an adoption roadmap.

Another direction for future work could involve the model from the SEM analysis being evaluated again with new sets of data. The differences flagged up by the new data could be analysed and compared with the results of this research. The experts participating in this research were from various different Saudi government organisations in the services sector; this meant that the present study collected data from organisations located in the KSA's big four cities: Riyadh, Jeddah, Madinah and Damam. Despite this, however, there remain certain organisations and sectors, such as private organisations, which were not involved in this study's data collection process. These organisations must be considered in future studies.

The main aim of this research was to develop a security cloud model that can serve as a guideline for Saudi organisations' decision makers as they consider adopting cloud services. A potential, and very interesting implication of this model, is that it could be employed by researchers and stakeholders (cloud providers and users) for cloud adoption projects.

In addition, the study model can be conducted in additional countries and areas. Since other Middle Eastern countries have cultural and demographic characteristics in common with the KSA, the same model could be validated for these regions. Besides this, the model can be used in the future for studying the adoption of new IT innovations whose IT architecture is similar to that of the cloud.

9.6 Final Remarks

The researcher acknowledges that this empirical study has been challenging, particularly with regard to designing the research methods and minimising the subjective bias during all lifecycle stages of the research. Lastly, it was determined that using statistical analyses could be very valuable in empirical cloud security study.

On the other hand, finding appropriate statistical analysis tests for the collected data required a good understanding of the data itself, the objectives of the study, and the statistical tests which were presented to help achieve the stated objectives.

References

- Acuna, E., Rodriguez, C., 2004. The Treatment of Missing Values and its Effect on Classifier Accuracy, in: *Classification, Clustering, and Data Mining Applications*. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 639–647. https://doi.org/10.1007/978-3-642-17103-1_60
- Adams, J., Khan, H.T. a., Raeside, R., White, D., 2007. Research Methods for Graduate *Business and Social Science Students*, *Zhurnal Eksperimental'noi i Teoreticheskoi Fiziki*. <https://doi.org/10.1007/s13398-014-0173-7.2>
- Ahn, S.M., Hong, K.S., Lee, C., 2014. Cloud Computing Risk Assessment: A Systematic Literature Review. *Lecture Notes in Electrical Engineering* 276, 413–420. <https://doi.org/10.1007/978-3-642-40861-8>
- Alarifi, A., Tootell, H., Hyland, P., 2012. A study of information security awareness and practices in Saudi Arabia. 2012 International Conference on Communications and Information Technology (ICCIT) 6–12. <https://doi.org/10.1109/ICCITechnol.2012.6285845>
- Alateyah, S., Crowder, R., Wills, G., 2013. An Exploratory study of proposed factors to Adopt e-government Services,. *International Journal of Advanced Computer Science and Applications* 4, 57–66. <https://doi.org/10.14569/IJACSA.2013.041108>
- Albugmi, A., Walters, R., Wills, G., 2016. Data Security in Cloud Computing. Fifth International Conference on FGCT, IEEE 2, 1–169. <https://doi.org/10.1109/FGCT.2016.7605062>
- Alfifi, F., Wang, W., Davis, G.A., Kovacs, P.J., 2015. Cloud Computing : a Cross-Cultural Comparative Study Between Computer and Information Systems. *Issues in Information Systems* , International Association for Computer Information Systems 16, 41–50.
- Alharbi, F., Atkins, A., Stanier, C., 2015. Strategic Framework for Cloud Computing Decision-Making in Healthcare Sector in Saudi Arabia. *The Seventh International Conference on eHealth, Telemedicine, and Social Medicine* 1, 138–144. <https://doi.org/10.1109/ICIHT.2017.7899001>
- Alharbi, S.T., 2017. Trust and acceptance of cloud computing: A revised UTAUT model, in: *Proceedings - 2017 International Conference on Computational Science and Computational Intelligence*, CSCI 2017. pp. 131–134. <https://doi.org/10.1109/CSCI.2014.107>
- Alharthi, A., Alassafi, M.O., Walters, R.J., Wills, G.B., 2016. An exploratory study for

- investigating the critical success factors for cloud migration in the Saudi Arabian higher education context. *Telematics and Informatics* 34, 664–678. <https://doi.org/10.1016/j.tele.2016.10.008>
- Alharthi, A., Yahya, F., Walters, R.J., Wills, G.B., 2015. An Overview of Cloud Services Adoption Challenges in Higher Education Institutions. *Proceeding of the 2nd international conference workshop on emerging software as a services* 1, 102–109. <https://doi.org/10.5220/0005529701020109>
- Alkhater, N., Wills, G., Walters, R., 2014. Factors Influencing an Organisation's Intention to Adopt Cloud Computing in Saudi Arabia. *IEEE 6th International Conference on Cloud Computing Technology and Science* 1040–1044. <https://doi.org/10.1109/CloudCom.2014.95>
- Almorsy, M., Grundy, J., Müller, I., 2016. An analysis of the cloud computing security problem. *17th Asia-Pacific Software Engineering Conference (APSEC 2010) Cloud Workshop*, Sydney, Australia 7. <https://doi.org/arXiv:1609.01107>
- Alnatheer, M., Nelson, K., 2009. A Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context. *Proceedings of the 7th Australian Information Security Management Conference*, December 2009 6–17. <https://doi.org/10.4225/75/579850d331b4d>
- Alsanea, M., Barth, J., 2014. Factors Affecting the Adoption of Cloud Computing in the Government Sector: A Case Study of Saudi Arabia. *International Journal of Cloud Computing and Services* 1, 1–16. <https://doi.org/10.11591/closer.v3i6.6811>
- Alshahrani, S. a., Alsadiq, A.J., 2014. Economic Growth and Government Spending in Saudi Arabia: an Empirical Investigation. *International Monetary Fund* 14, 1. <https://doi.org/10.5089/9781484348796.001>
- Alshehri, M., Drew, S., 2010. Challenges of e-Government Services Adoption in Saudi Arabia from an e-ready citizen Perspective. *World Academy of Science, Engineering and Technology* 4, 881–887. <https://doi.org/10.1179/204264411X12961227987886>
- Alturki, S.M., 2017. Analysis and Identification of Cloud Usage in Private and Public Sector in Saudi Arabia. *Computer, SM Alturki - International Journal of* 2017, Undefined 162, 17–21. <https://doi.org/10.5120/ijca2017913270>
- Anderson, C., 2010. Presenting and evaluating qualitative research. *American journal of pharmaceutical education*. <https://doi.org/10.5688/aj7408141>
- Avram, M.G., 2014. Advantages and Challenges of Adopting Cloud Computing from an Enterprise Perspective. *The 7th International Conference Interdisciplinarity in Engineering (INTER-ENG 2013) Advantages* 12, 529–534. <https://doi.org/10.1016/j.protcy.2013.12.525>

- Awang, Z., 2015. SEM Made Simple: A Gentle Approach to Learning Structural Equation Modelling, MPWS Rich Publication. <https://doi.org/10.1016978-967-12581-7-0>
- Ayre, C., Scally, A.J., 2014. Critical values for Lawshe's content validity ratio: Revisiting the original methods of calculation. *Measurement and Evaluation in Counseling and Development* 47, 79–86. <https://doi.org/10.1177/0748175613513808>
- Azeemi, I.K., Lewis, M., Tryfonas, T., 2013. Migrating to the cloud: Lessons and limitations of "traditional" is success models, in: *Procedia Computer Science*. pp. 737–746. <https://doi.org/10.1016/j.procs.2013.01.077>
- Babu, S., Ph, C., Bansal, V., Telang, P., 2010. Cisco: Top 10 Cloud Risks That Will Keep You Awake at Night. CSICO 1–35.
- Badger, L., Bernstein, D., Bohn, R., de Vault, F., Hogan, M., Iorga, M., Mao, J., Messina, J., Mills, K., Simmon, E., Sokol, A., Tong, J., Whiteside, F., Leaf, D., 2014. US Government Cloud Computing Technology Roadmap, Nist Special Publication. Gaithersburg, MD. <https://doi.org/10.6028/NIST.SP.500-293>
- Bannerman, P., 2010. Cloud computing adoption risks: state of play. *Asia Pacific Software Engineering Conference Cloud Workshop* 3, 1–7. <https://doi.org/10.1109/GCE.2008.4738445>
- Bentler, P.M., 1990. Comparative fit indexes in structural models. *Psychological Bulletin* 107, 238–246. <https://doi.org/10.1037/0033-2909.107.2.238>
- Bhattacharjee, A., 2012. *Social Science Research: principles, methods, and practices*, Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License. <https://doi.org/10.1186/1478-4505-9-2>
- Britten, N., 1995. Qualitative Research: Qualitative interviews in medical research. *BMJ* 311, 251–253. <https://doi.org/10.1136/bmj.311.6999.251>
- Brodin, J., 2008. Gartner: Seven cloud-computing security risks. *InfoWorld* July, 2–3.
- Bryman, A., 2006. Integrating quantitative and qualitative research: how is it done? *Qualitative Research* 6, 97–113. <https://doi.org/10.1177/1468794106058877>
- Bryman, A., Cramer, D., 2001. *Quantitative Data Analysis with SPSS Release 10 for Windows*, Taylor & Francis e-Library, 2002. <https://doi.org/10.4324/9780203471548>
- Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J., Brandic, I., 2009. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems* 25, 599–616. <https://doi.org/10.1016/j.future.2008.12.001>

- Byrne, B.M., 2010. Structural equation Modelling with AMOS: Basic concepts, applications, and programming, Routledge. <https://doi.org/10.4324/9781410600219>
- Caracelli, V.J., Greene, J.C., 1993. Data Analysis Strategies for Mixed-Method Evaluation Designs. *Educational Evaluation and Policy Analysis* 15, 195–207. <https://doi.org/10.3102/01623737015002195>
- Catteddu, D., Hogben, G., 2009. Cloud Computing Benefits, Benefits, risks and recommendations for information security (ENISA). ENISA Computing Report 72, 2009–2013. https://doi.org/10.1007/978-3-642-16120-9_9
- Chandra, A., Weissman, J., 2009. Nebulas : Using Distributed Voluntary Resources to Build Clouds. *Proceedings of the 2009 conference on Hot topics in cloud computing* 1, 2.
- Chang, V., Ramachandran, M., 2015. Towards achieving Data Security with the Cloud Computing Adoption Framework. *IEEE Transactions on Services Computing* 1374, 1–1. <https://doi.org/10.1109/TSC.2015.2491281>
- Changchit, C., Chuchuen, C., 2016. Cloud Computing: An Examination of Factors Impacting Users' Adoption. *Journal of Computer Information Systems* 1–9. <https://doi.org/10.1080/08874417.2016.1180651>
- Che, J., Duan, Y., Zhang, T., Fan, J., 2011. Study on the security models and strategies of cloud computing. *international Conference on Power Electronics and Engineering Application* 23, 586–593. <https://doi.org/10.1016/j.proeng.2011.11.2551>
- Cherdantseva, Y., Hilton, J., 2013. A Reference Model of Information Assurance & Security. *International Conference on Availability, Reliability and Security* 546–555. <https://doi.org/10.1109/ARES.2013.72>
- Choudrie, J., Ghinea, G., 2013. Silver surfers, e-government and the digital divide: An exploratory study of UK local authority websites and older citizens. *Interacting with.* <https://doi.org/10.1093/iwc/iws020>
- Clifford, N., French, S., Valentine, G., 2010. Key Methods in Geography, Geographical Research. <https://doi.org/10.1017/CBO9781107415324.004>
- Cloud Security Alliance, 2013. The Notorious Nine. Cloud Computing Top Threats in 2013 CSA. CSA Global Staff 1–14. <https://doi.org/http://www.cloudsecurityalliance.org/topthreats>.
- Cohen, J., 1988. Statistical power analysis for the behavioral sciences. *Statistical Power Analysis for the Behavioral Sciences*. <https://doi.org/10.1016/B978-0-12-17906>
- Cohen, L., Manion, L., Morrison, K., 2011. Research Methods in Education, 7th ed. London: Routledge.

- Connolly, P., 2011. Quantitative Data Analysis using SPSS. An International for Health and Social Science 1–283. <https://doi.org/10.1111/j.1467-8535.2008.00908>
- Cooper, D.R., Schindler, P.S., 2003. Business research methods. Business, New York: McGraw-hill.
- Council, 2012. Security for Cloud Computing 10 Steps to Ensure Success (OWASP). Cloud Standards Customer Council 1–35. [https://doi.org/doi.org/10.1016/S1071-5819\(03\)00111-3](https://doi.org/doi.org/10.1016/S1071-5819(03)00111-3)
- Creswell, J.W., 2007. Research Design: Qualitative, Quantitative and Mixed Method Approaches. SAGE Publications 203–223. <https://doi.org/10.4135/9781849208956>
- Creswell, J.W., 2003. Research design Qualitative quantitative and mixed methods approaches. SAGE Publications International Educational and Professional Publisher 3–26. <https://doi.org/10.3109/08941939.2012.723954>
- Cronbach, L.J., Shavelson, R.J., 2004. My Current Thoughts on Coefficient Alpha and Successor Procedures. Educational and Psychological Measurement 64, 391–418. <https://doi.org/10.1177/0013164404266386>
- Deloitte, 2010. Information Security Briefing Cloud Computing, CPNI. Centre for the Protection of National Infrastructure 1–71. <https://doi.org/https://www.cpni.gov.uk/>
- Driscoll, D.L., Salib, P., Rupert, D.J., 2007. Merging Qualitative and Quantitative Data in Mixed Methods Research : How To and Why Not. Ecological and Environmental Anthropology 3, 18–28. <https://doi.org/10.1016/j.jocn.2003.11.015>
- Economist Intelligence Unit, 2010. Democracy index 2010 Democracy in retreat. Intelligence 46. <https://doi.org/http://graphics.eiu.com>
- Elena, G., Johnson, C.W., 2015. Factors influancing Risk Acceptance of Cloud Computing Sertvices in the UK. International Journal on Cloud Computing: Services and Architecture (IJCCSA) 5. <https://doi.org/10.5121/ijccsa.2015.5301> 1
- Elena, G., W.Johnson, C., 2015. Laypeople's and Experts' Risk Perception of Cloud Computing Services. International Journal on Cloud Computing: Services and Architecture 5, 1–19. <https://doi.org/10.5121/ijccsa.2015.5401>
- Featherman, M.S., Pavlou, P.A., 2003. Predicting e-services adoption: A perceived risk facets perspective. International Journal of Human Computer Studies 59, 451–474. [https://doi.org/10.1016/S1071-5819\(03\)00111-3](https://doi.org/10.1016/S1071-5819(03)00111-3)
- Field, A., 2013. Discovering Statistics using IBM SPSS Statistics. Discovering Statistics using IBM SPSS Statistics 297–321. <https://doi.org/10.1016/B978-012691360-6/50012-4>

- Fink, A., 2003. How to Ask Survey Questions. The survey kit. <https://doi.org/10.4135/9781412984393>
- Fink, A., Litwin, M., 2003. How to assess and interpret survey psychometrics.
- Finkelstein, D.M., 2005. A Beginner's Guide to Structural Equation Modelling, Technometrics. <https://doi.org/10.1198/tech.2005.s328>
- Fumei Weng, M.-C.H., 2014. Competition and Challenge on Adopting Cloud ERP. International Journal of Innovation, Management and Technology 5, 309–313. <https://doi.org/10.7763/IJIMT.2014.V5.531>
- Gangwar, H., Date, H., Ramaswamy, R., 2015. Understanding determinants of cloud computing adoption using an integrated TAM-TOE model. Journal of Enterprise Information Management 28, 107–130. <https://doi.org/10.1108/JEIM-08-2013-0065>
- Gentzoglanis, A., 2011. Risk and Financial Modelling and Cloud Computing: A New Approach. International Conference on Software and Computer Applications 9, 147–151.
- Graham, J.W., Olchowski, A.E., Gilreath, T.D., 2007. How many imputations are really needed? Some practical clarifications of multiple imputation theory. Prevention Science 8, 206–213. <https://doi.org/10.1007/s11121-007-0070-9>
- Grant, J.S., Davis, L.L., 1997. Selection and use of content experts for instrument development. Research in Nursing & Health 20, 269–274.
- Guba, E.G.E., Lincoln, Y.S.Y., 1994. Competing Paradigms in Qualitative Research. Handbook of qualitative research.
- Guest, G., Bunce, A., Johnson, L., 2006. How Many Interviews Are Enough ? An Experiment with Data Saturation and Variability. Family Health International 18, 59–82. <https://doi.org/10.1177/1525822X05279903>
- Hair, J.F., Black, W.C., Babin, B.J., Anderson, R.E., 2010. Multivariate Data Analysis. Vectors. <https://doi.org/10.1016/j.ijpharm.2011.02.019>
- Heiser, J., Nicolett, M., 2008. Assessing the Security Risks of Cloud Computing. Reproduction 1–6.
- Hill, C., Loch, K., 1998. A Qualitative Assessment of Arab Culture and Information Technology Transfer. Journal of Global Information Management 6:3, 29–38. <https://doi.org/10.4018/jgim.1998070103>
- Hooper, D., Coughlan, J., Mullen, M.R., 2008. Structural equation modelling: Guidelines for determining model fit. Electronic Journal of Business Research Methods 6, 53–60.

- Hox, J.J., 2008. Survey Methodology. *International Handbook of Survey Methodology* 387–402. <https://doi.org/10.4324/9780203843123>
- Isaca, 2009. An Introduction to the Business Model for Information Security. *Information Security* 1–28.
- Jasti, A., Shah, P., Nagaraj, R., Pendse, R., 2010. Security in multi-tenancy cloud, in: *Proceedings - International Carnahan Conference on Security Technology*. <https://doi.org/10.1109/CCST.2010.5678682>
- Kaiser, H.F., 1970. A Second-generation Little Jiffy. *Psychometrika* 25, 401–415. <https://doi.org/10.1007/BF02291817>
- Kanday, R., 2012. A Survey on Cloud Computing Security. *2012 International Conference on Computing Sciences* 2, 302–311. <https://doi.org/10.1109/ICCS.2012.6>
- Kaplan, B., Duchon, D., 1988. Combining Qualitative and Quantitative Information Systems. *International Conference on information Systems* 12, 571–586. <https://doi.org/10.2307/249133>
- Katsirikou, A., 2010. Qualitative and Quantitative Methods in Libraries QQML2009. *International Conference QQML2010*.
- Kerlinger, F.N., 1986. Foundations of behavioural research, in: *Foundations of Behavioral Research* (3rd Ed.). pp. 3–14.
- Khan, K.M., Malluhi, Q., 2010. Establishing trust in cloud computing. *IT Professional* 12, 20–27. <https://doi.org/10.1109/MITP.2010.128>
- King, G., Honaker, J., Joseph, A., 1998. List-wise deletion is evil: what to do about missing data in political science. In *Annual Meeting of the American Political Science Association*, Boston.
- Kline, R.B., 2011. Principles and Practice of Structural Equation Modelling, Analysis. <https://doi.org/10.1038/156278a0>
- Ko, A., Leitner, C., Leitold, H., Prosser, A., 2013. Technology-Enabled Innovation for Democracy, *International Conference on Electronic Government* Springer. <https://doi.org/10.1007/978-3-642-40160-2>
- KPMG, 2011. The Cloud: Changing the Business Ecosystem. *Kpmg International* 1–102.
- Kumar, K., 2010. Cloud Computing for Mobile Users: Can Offloading Computation Save Energy? *IEEE Computer Society* 43, 51–56. <https://doi.org/10.1109/MC.2010.98>
- Kurniawan, S., 2004. Interaction design: Beyond human computer interaction. *Springer* 3, 289–289. <https://doi.org/10.1007/s10209-004-0102-1>

- Lake, C., Tessmer, M., 1993. Constructivism ' s Implications For Formative Evaluation. Constructivism and formative evaluation, AECT, 05/10/97, page 1 Constructivism's 1–11.
- Lawshe, C., 1975. A Quantitative Approach To Content Validity. *Personnel Psychology* 563–575. <https://doi.org/10.1111/j.1744-6570.1975.tb01393.x>
- Lin, T., Huang, C., 2008. Understanding knowledge management system usage antecedents: An integration of social cognitive theory and task technology fit. *Information & Management*. <https://doi.org/10.1016/j.im.2008.06.004>
- Lynn, M., 1986. Determination and quantification of content validity. *Nursing research*.
- Lynn, M.R., 1986. Determination and Quantification of Content Validity. *Nursing Research*. <https://doi.org/10.1097/00006199-198611000-00017>
- M. Morse, J., 1991. Approaches to qualitative- quantitative methodological triangulation. *Nursing Research*.
- Mack, Natasha, et al., 2005. Qualitative Research Methods A data collector's field guide, Family Health International,. <https://doi.org/10.1108/eb020723>
- Malhotra, Y., Galletta, D.F., 1999. Extending the Technology Acceptance Model to Account for Social Influence: Theoretical Bases and Empirical Validation. *Proceedings of the 32nd Hawaii International Conference on System Sciences* 00, 1–11. <https://doi.org/10.1109/HICSS.1999.772658>
- Mather, T., Kumaraswamy, S., Latif, S., 2009. Cloud security and privacy: an enterprise perspective on risks and compliance. Sarah Schneider, United States of America. 299. <https://doi.org/10.1073/pnas.0703993104>
- Mauch, V., Kunze, M., Hillenbrand, M., 2013. High performance cloud computing. *Future Generation Computer Systems* 29, 1408–1416. <https://doi.org/10.1016/j.future.2012.03.011>
- McDonald, R.P., Ho, M.-H.R., 2002. Principles and practice in reporting structural equation analyses. *Psychological Methods* 7, 64–82. <https://doi.org/10.1037/1082-989X.7.1.64>
- Mell, P., Grance, T., 2011. The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology. Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, 145, 7. <https://doi.org/10.1136/emj.2010.096966>
- MICHAEL ARMBRUST, A.F., 2010. A view of cloud computing. *Communications of the ACM* 53, 50–58. <https://doi.org/10.1145/1721654.1721672>
- Michael S. Garver, J.T.M., 1999. Logistics Research Methods: Employing Structural Equation Modelling to Test for Construct Validity. *Journal of Business Logistics*.

- Miller, M., 2009. Cloud Computing : Web-Based Applications That Change the Way You Work and Collaborate Online. Que Publishing 1–29.
- Myers, M.D., 1997. Qualitative research in information systems. *Management Information Systems Quarterly* 21, 1–18. <https://doi.org/10.2307/249422>
- NIST, 2011. The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology. Nist Special Publication 145, 7. <https://doi.org/10.1136/emj.2010.096966>
- Nunnally, J.C., 1978. *Psychometric Theory*, rdsepiucsforg.
- Olson, K., 2010. An Examination of Questionnaire Evaluation by Expert Reviewers. *Field Methods* 22, 295–318. <https://doi.org/10.1177/1525822X10379795>
- Oppenheim, a. N., 2000. Questionnaire design, interviewing and attitude measurement. Bloomsbury Publishing 17, 33–34. [https://doi.org/10.1016/0149-7189\(94\)90021-3](https://doi.org/10.1016/0149-7189(94)90021-3)
- Orlikowski, W.J., Baroudi, J.J., 1991. Studying information technology in organizations: Research approaches and assumptions. *Information Systems Research* 2, 1–28. <https://doi.org/10.1287/isre.2.1.1>
- Pallant, J., 2007. *Spss Survival Manual. A step by step guide to data analysis using SPSS for Windows (Version 10)*.
- Paquette, S., Jaeger, P.T., Wilson, S.C., 2010. Identifying the security risks associated with governmental use of cloud computing. *Elsevier Journal* 27, 245–253. <https://doi.org/10.1016/j.giq.2010.01.002>
- Pearson, S., 2013. *Privacy, Security and Trust in Cloud Computing*. Springer London 3–42. <https://doi.org/10.1007/978-1-4471-4189-1>
- Podsakoff, P.M., MacKenzie, S.B., Lee, J.-Y., Podsakoff, N.P., 2003. Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology* 88, 879–903. <https://doi.org/10.1037/0021-9010.88.5.879>
- Recker, J., 2012. Scientific research in information systems. Twenty-Third European Conference on Information Systems (ECIS), Münster, Germany.
- Revilla, M.A., Saris, W.E., Krosnick, J.A., 2014. Choosing the Number of Categories in Agree-Disagree Scales. *Sociological Methods and Research* 43, 73–97. <https://doi.org/10.1177/0049124113509605>
- Sabahi, F., 2011. Cloud computing security threats and responses. 2011 IEEE 3rd International Conference on Communication Software and Networks 245–249. <https://doi.org/10.1109/ICCSN.2011.6014715>

- Saunders, M., Lewis, P., Thornhill, A., 2009. Research Methods for Business Students Fifth Edition. <https://doi.org/10.1007/s13398-014-0173-7.2>
- Schubert, L., Jeffery, K., Neidecker-Lutz, B., 2010. The Future of Cloud Computing. Opportunities for European Cloud Computing Beyond 2010. European Commission, the Cloud Expert Group 66. <https://doi.org/10.1016/B978-1-59749-537-0.00012-0>
- Sekaran, U., 2003. Research and Markets: Research Methods for Business - A Skill Building Approach, John Wiley & Sons. <https://doi.org/http://dx.doi.org/10.1108/17506200710779521>
- Sen, J., 2013. Security and Privacy Issues in Cloud Computing. Architectures and Protocols for Secure Information Technology 42. <https://doi.org/10.1109/HICSS.2011.103>
- Sharp, H., Rogers, Y., Preece, J., 2011. Interaction Design: Beyond Human-Computer Interaction. Book 11, 602. <https://doi.org/10.1162/leon.2005.38.5.401>
- Shevlin, M., Miles, J.N., Davies, M.N., Walker, S., 2000. Coefficient alpha: a useful indicator of reliability? Personality and Individual Differences 28, 229–237. [https://doi.org/10.1016/S0191-8869\(99\)00093-8](https://doi.org/10.1016/S0191-8869(99)00093-8)
- Shirley Radack, 2012. Cloud Computing: A Review Of Features, Benefits, And Risks, And Recommendations For Secure, Efficient Implementations. NIST Special Publication (SP) 800-146.
- Souza, S.M.P.C., Puttini, R.S., 2016. Client-side Encryption for Privacy-sensitive Applications on the Cloud, in: Procedia Computer Science. pp. 126–130. <https://doi.org/10.1016/j.procs.2016.08.289>
- Storey, A.A., Ramirez, J.M., Quiroz, D., Burley, D. V., Addison, D.J., Walter, R., Anderson, A.J., Hunt, T.L., Athens, J.S., Huynen, L., Matisoo-Smith, E.A., 2007. Radiocarbon and DNA evidence for a pre-Columbian introduction of Polynesian chickens to Chile. Proceedings of the National Academy of Sciences 104, 10335–10339. <https://doi.org/10.1073/pnas.0703993104>
- Straub, D., Boudreau, M., Gefen, D., 2004. Validation guidelines for IS positivist research. Association for Information. <https://doi.org/10.2307/249422>
- Straub, D.W.M., Loch, K.D., Hill, C.E., 2003. Transfer of Information Technology to the Arab World. Journal of Global Information Management 9, 6–28. <https://doi.org/10.4018/jgim.2001100101>
- Suhr, D., 2006. Exploratory or confirmatory factor analysis? Statistics and Data analysis 1–17. <https://doi.org/10.1002/da.20406>
- Tabachnick, B.G., Fidell, L.S., 2012. Using multivariate statistics (6th ed.), New York: Harper and Row. <https://doi.org/10.1037/022267>

- Tabachnick, B.G., Fidell, L.S., 2007. Using multivariate statistics, Pearson. <https://doi.org/10.1037/022267>
- Tei, K., Gurgun, L., 2014. ClouT: Cloud of things for empowering the citizen clout in smart cities. 2014 IEEE World Forum on Internet of Things, WF-IoT 2014 369–370. <https://doi.org/10.1109/WF-IoT.2014.6803191>
- Tessmer, M., 2009. Hypothesis testing, type I and type II erro. *Industrial Psychiatry Journal* 1, 127–131. <https://doi.org/10.1017/CBO9781107415324.004>
- Vic, W., 2011. Securing the Cloud, Securing the Cloud. <https://doi.org/10.1016/C2009-0-30544-9>
- von Solms, R., van Niekerk, J., 2013. From information security to cyber security. *Computers & Security* 38, 97–102. <https://doi.org/10.1016/j.cose.2013.04.004>
- Watson, R., 2001. SPSS Survival Manual by Julie Pallant, Open University Press, Buckingham, 2001, 286 pages, f16.99, ISBN 0 335 20890 8. *Journal of Advanced Nursing* 36, 478–478. <https://doi.org/10.1046/j.1365-2648.2001.2027c.x>
- Wei, J., Zhang, X., Ammons, G., Bala, V., Ning, P., 2009. Managing security of virtual machine images in a cloud environment. *Proceedings of the 2009 ACM workshop on Cloud computing security - CCSW '09* 91. <https://doi.org/10.1145/1655008.1655021>
- Wheaton, B., 1987. Assessment of Fit in Overidentified Models with Latent Variables. *Sociological Methods & Research* 16, 118–154. <https://doi.org/10.1177/0049124187016001005>
- Williams, J.S., Child, D., 2003. The Essentials of Factor Analysis., *Contemporary Sociology*. <https://doi.org/10.2307/2061984>
- Wolf, E.J., Harrington, K.M., Clark, S.L., Miller, M.W., 2013. Sample size requirements for Structural Equation Models: An evaluation of power, bias, and solution propriety. *Educational and Psychological Measurement* 76, 913–934. <https://doi.org/10.1177/0013164413495237>
- Wyld, D.C., 2010. The Cloudy Future Of Government IT: Cloud Computing and The Public Sector Around The World. *International Journal of Web & Semantic Technology* 1.
- Wyld, D.C., Robert Maurin, 2009. Moving to the Cloud : An Introduction to Cloud Computing in Government E-Government Series Moving to the Cloud 82. <https://doi.org/10.1109/ICBNMT.2011.6155965>
- Xu, J., Chang, E.-C., Zhou, J., 2013. Weak leakage-resilient client-side deduplication of encrypted data in cloud storage, in: *Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security - ASIA CCS '13*. p. 195.

<https://doi.org/10.1145/2484313.2484340>

Yahya, F., Chang, V., Walters, J., Wills, B., 2014. Security Challenges in Cloud Storage 1–6. <https://doi.org/10.1109/CloudCom.2014.171>

Zhang, L.J., Zhou, Q., 2009. CCOA: Cloud Computing Open Architecture, in: 2009 IEEE International Conference on Web Services, ICWS 2009. pp. 607–616. <https://doi.org/10.1109/ICWS.2009.144>

Zikmund, W.G., 2012. Business research methods. Business Research Methods, Erin Joyner.

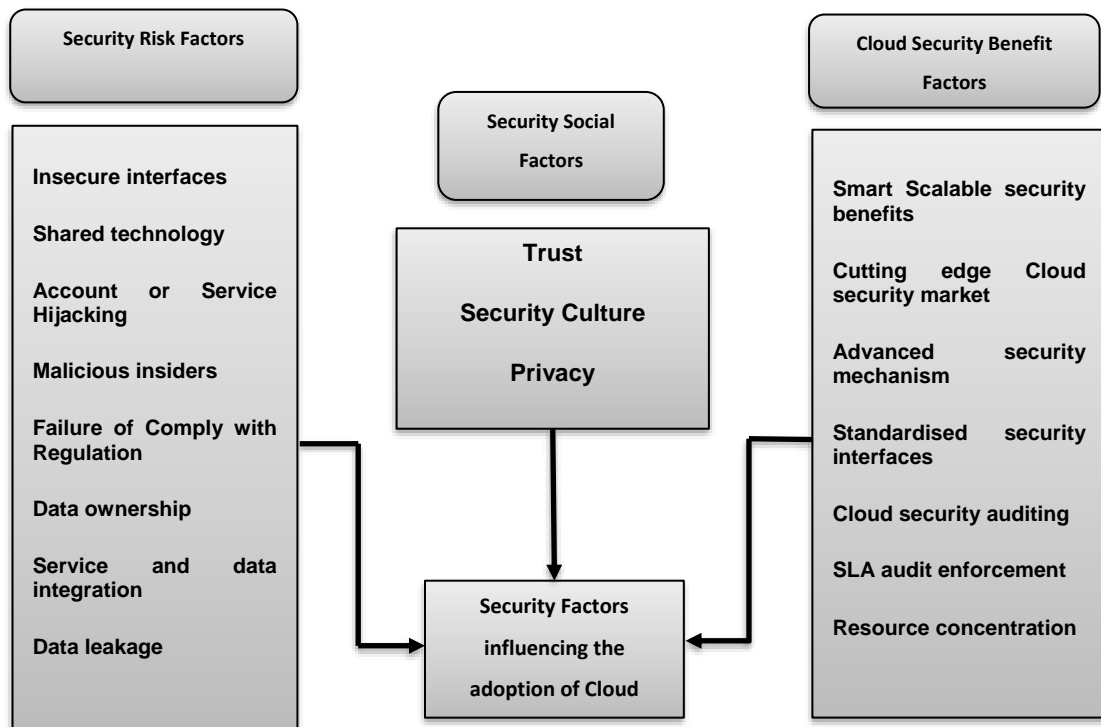
Appendix A Confirmatory Study (Interviews)

A.1 Interview questions

The aim of this research is to investigate the security factors that may influence an organisation to adopt cloud computing in KSA government organisations. Your responses and expertise will help play a major role in addressing the factors that encourage or prevent the wide implementation of cloud computing. All information provided will be used for research purposes only. Thank you very much for taking part in this study.

Interview Questions

Please see the framework for this study before answering the questions.



Q1: How important is the influence of the following security risks to the adoption of cloud services in Saudi government organisations?

Category 1: Security Risk factors						
Coding	Attributes	Very important	Important	May be important	Not important	Not relevant
RF1	Insecure Interfaces					
RF2	Shared Technology					
RF3	Account or Service Hijacking					
RF4	Malicious Insiders					
RF5	Failure to Comply with Regulations					
RF6	Data ownership					
RF7	Service and data integration					
RF8	Data leakage					

Q2: How important is the influence of the following security social factors to the adoption of cloud service in Saudi government organisations?

Category 2: Security Social Factors						
Coding	Attributes	Very important	Important	May be important	Not important	Not relevant
SF1	Trust					
SF2	Security Culture					
SF3	Privacy					

Q3: If you are responsible for digital innovation within your organisation, what is the importance of the following security benefits for your decision to adopt cloud services in Saudi government organisations?

Category 3: Security Benefits						
Coding	Attributes	Very important	Important	May be important	Not important	Not relevant
BF1	Smart Scalable security benefits					
BF2	Cutting-edge Cloud security market					
BF3	Advanced security mechanism					
BF4	Standardised security interfaces					
BF5	Cloud security auditing					
BF6	Service level agreement audit enforcement					
BF7	Resource concentration					

Q4: In your opinion, what other important security (social/risks/benefits) factors need to be considered when an organisation adopting cloud computing?

Q5: Does your organisation adopt cloud computing?

Q6: What are the reasons behind using/not using cloud computing in your organisation?

Q7: What are the challenges that your organisation faced with using cloud computing?
(If your organisation adopted cloud computing answer this question)?

A.2 Interview Analysis

Analysis of factors for cloud adoption using one sample t-test

Variable	Factors	Ref	N	t	Mean	Sig (2-Tailed) P-value
Security Risk Factors	Insecure Interfaces	RF1	12	16.316	4.83	<.001 • ^A
	Shared Technology	RF2	12	7.000	4.17	<.001 • ^A
	Account Hijacking	RF3	12	10.652	4.58	<.001 • ^A
	Malicious Insiders	RF4	12	5.196	4.50	<.001 • ^A
	Failure to Comply with Regulations	RF5	12	9.574	4.25	<.001 • ^A
	Data Ownership	RF6	12	9.950	4.50	<.001 • ^A
	Service and Data Integration	RF7	12	7.000	4.17	<.001 • ^A
	Data Leakage	RF8	12	16.316	4.83	<.001 • ^A
Security Social Factors	Trust	SF1	12	23.000	4.92	<.001 • ^A
	Security Culture	SF2	12	10.652	4.58	<.001 • ^A
	Privacy	SF3	12	23.000	4.92	<.001 • ^A
Security Benefits Factors	Smart Scalable security benefits	BF1	12	9.950	4.50	<.001 • ^A
	Cutting-edge security market	BF2	12	8.124	4.00	<.001 • ^A
	Advanced security mechanism	BF3	12	10.652	4.58	<.001 • ^A
	Standardised security interfaces	BF4	12	13.404	4.75	<.001 • ^A
	Cloud security auditing	BF5	12	10.652	4.58	<.001 • ^A
	SLA audit enforcement	BF6	12	13.404	4.75	<.001 • ^A
	Resource concentration	BF7	12	1.915	3.25	<0.082 •• ^B

^A • P-value < 0.0027.

^B • • P-value > 0.0027.

A.3 Interview Themes Analysis

Expert Interview Suggestions

Job Description	Themes	Experts Suggestions
Security expert	(Expert A): Data Breaches as Risk Factors. The scalability features of the cloud computing enhanced confront of high spike of workload during the peak time of the year	"Exclusive allocation of the cloud resources should be considered as a security risk when adopting the cloud" (Expert F). "I agree that most of the factors in the framework are potential variables that hinder some organisations when they are trying to use cloud services and there are some other factors influencing the adoption of cloud services such as: Encryption and Sophisticated Authentication Techniques" (Expert B).
Head of the Networking Department	(Expert B): Sophisticated Authentication Techniques (Risk Factors) Consolidated Services Collaboration and Sharing Reduce Total Cost of Ownership Ensuring the proper rising of the cloud-based implementation to satisfy the organization needs Security breaches caused by social trends	"We should consider Encryption and Sophisticated Authentication Techniques as security risks when we are thinking about adopting cloud services because there is reason behind using services such as Consolidated Services" (Expert J). "There are some challenges that my agency and other organisations in Saudi Arabia have faced since using this technology. I advise that it is important to ensure the proper rising of the cloud-based implementation to satisfy the organisation's needs and security breaches caused by social trends" (Expert B).
Chief Information officer	(Expert B, C, J): Encryption as risks Working as team Security Breaches Trust issues	"I agree that all security risk factors, as well as the social and benefits factors mentioned in your framework are essential when any government organisations are making decisions to adopt cloud computing in their organisations and I recommend that all organisations be aware of that data encryption should be prepared before and after using cloud services" (Expert F).
Security Expert	(Expert D): Use of client-side encryption (Risk factor) Data access authorization mechanism Team work Ease of Access Data transfer bottlenecks. Culture.	"I think we need to try the cloud services before adopting it. We call it a test phase" (Expert L). "Social Users' awareness is important when using cloud platforms in order to avoid shadow IT data leakage and protect staff from inside attacks" (Expert L).
Data Management	(Expert E): Vulnerability Supply attacks Better insight. Cloud helps collaboration. Cloud gives better engagement. Speed. Service quality. Access to data and downtime. Accessibility.	"In terms of security risk, in order to ensure there is security transparency, the providers should alert the consumers to the security control updates or policies that are applied to their data. Moreover, to guarantee transparency when an incident occurs, the cloud provider should not cover up any
System Administrator	(Expert F): Prepare data encryption before and after using cloud services. Exclusive allocation of the cloud resources. Setting up cloud infrastructure. Training for using the cloud.	

	Adopting classical applications for the cloud.	<p>security incident affecting their assets and should share the lessons learned from each incident with the consumers to ensure that there is a well-protected cloud environment” (Expert L).</p> <p>“We should consider cloud multi-geographical infrastructures as a security benefit because it is very important for the consumers, especially when natural catastrophes happen”.</p> <p>“Whether the cloud service is more appropriate for government or the private sector depends on IT technology. Hence, the organisation needs to consider the nature of its business and its requirements before adopting the cloud service” (Expert G).</p> <p>“There are three challenges that my organisation has faced while using cloud services, and you may consider them important. These are: Setting up cloud infrastructure, Training for using the cloud and adopting classical applications for the cloud” (Expert F).</p> <p>“Many environmental and technical changes have been going on in the IT environment which need to settle down first. The IT environment is not yet ready for cloud computing (readiness)” (Expert G).</p> <p>“An organisation needs to know how to be on the cutting edge of technology. I consider it very important to recognise who your corporation is. We are a Saudi food and drug authority, so we are not an IT company, and may not have a high willingness to be on the cutting-edge technologically” (Expert D).</p> <p>“Other factors should be considered as security risks if using the cloud practically in government organisations, such as use of client-side encryption” (Expert D).</p> <p>“The best things about using cloud computing in my organisation are Ease of Access and Team Work”.</p> <p>“In terms of the security risk factor, organisations should prepare data encryption and employ this encryption when using cloud services” (Experts B, C, D and F).</p> <p>“In my opinion, other important factors need to be considered as security risks when an organisation adopts cloud services, such as Vulnerability and Supply Attacks including all factors mentioned in your framework” (Expert E).</p>
Data Security Expert	(Expert G): As risk factors: reputation and brand name. Many environmental and technical (readiness).	
Security Expert	(Expert H): Culture. Security Privacy Reduces the risk of the intellectual property being publicised or illegally infiltrated.	
President of the IT Department	(Expert I and K): Data breaches as risk factor. No Compliance and regulation is clear and this is one of the reasons behind not adopting cloud service in our organisation, as result we need to update our rules and regulations to comply with cloud computing	
Cloud System Admin	<p>(Expert L): Identifying the cloud core services that needed to enhance the IT services</p> <p>Identifying the apps that can be migrated to the cloud</p> <p>Administrating the cloud data centre</p> <p>Moving the data from legacy systems to the cloud</p> <p>IT practitioners learning curve</p> <p>Data access authorisation mechanism.</p>	

		<p>"We have started using the cloud because it provides a better insight, aids collaboration, speed, and gives better engagement" (Expert E).</p> <p>"Service quality, access to data and downtime and accessibility are some of the challenges we have faced while using the cloud" (Expert E).</p>
--	--	--

A.4 Interview Frequencies

Experts Frequencies

[DataSet2] C:\Users\moa2g15\Google Drive\Phd southampton university\Upgrade\August 13, Madini Documents_\SPSS Experts.sav

RF1

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	4	2	16.7	16.7	16.7
	5	10	83.3	83.3	100.0
	Total	12	100.0	100.0	

RF2

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	3	1	8.3	8.3	8.3
	4	8	66.7	66.7	75.0
	5	3	25.0	25.0	100.0
	Total	12	100.0	100.0	

RF3

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	4	5	41.7	41.7	41.7
	5	7	58.3	58.3	100.0
	Total	12	100.0	100.0	

RF4

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2	1	8.3	8.3	8.3
	3	1	8.3	8.3	16.7
	4	1	8.3	8.3	25.0
	5	9	75.0	75.0	100.0
	Total	12	100.0	100.0	

RF5

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	4	9	75.0	75.0	75.0
	5	3	25.0	25.0	100.0

Total	12	100.0	100.0	
-------	----	-------	-------	--

RF6

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid 4	6	50.0	50.0	50.0
5	6	50.0	50.0	100.0
Total	12	100.0	100.0	

RF7

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid 3	1	8.3	8.3	8.3
4	8	66.7	66.7	75.0
5	3	25.0	25.0	100.0
Total	12	100.0	100.0	

SF1

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid 4	1	8.3	8.3	8.3
5	11	91.7	91.7	100.0
Total	12	100.0	100.0	

SF2

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	4	5	41.7	41.7	41.7
	5	7	58.3	58.3	100.0
	Total	12	100.0	100.0	

SF3

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	4	1	8.3	8.3	8.3
	5	11	91.7	91.7	100.0
	Total	12	100.0	100.0	

BF1

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	4	6	50.0	50.0	50.0
	5	6	50.0	50.0	100.0
	Total	12	100.0	100.0	

BF2

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	3	1	8.3	8.3	8.3
	4	10	83.3	83.3	91.7
	5	1	8.3	8.3	100.0
	Total	12	100.0	100.0	

BF3

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	4	5	41.7	41.7	41.7
	5	7	58.3	58.3	100.0
	Total	12	100.0	100.0	

BF4

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	4	3	25.0	25.0	25.0
	5	9	75.0	75.0	100.0
	Total	12	100.0	100.0	

BF5

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	4	5	41.7	41.7	41.7
	5	7	58.3	58.3	100.0
	Total	12	100.0	100.0	

BF6

		Frequency	Percent	Valid Percent	Cumulative Percent
--	--	-----------	---------	---------------	--------------------

Valid	4	3	25.0	25.0	25.0
	5	9	75.0	75.0	100.0
Total		12	100.0	100.0	

BF7

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	3	7	58.3	58.3	58.3
	4	3	25.0	25.0	83.3
	5	2	16.7	16.7	100.0
Total		12	100.0	100.0	

• One-Sample Statistics of Expert Interviews

	N	Mean	Std. Deviation	Std. Error Mean
RF1	12	4.83	.389	.112
RF2	12	4.17	.577	.167
RF3	12	4.58	.515	.149
RF4	12	4.50	1.000	.289
RF5	12	4.25	.452	.131
RF6	12	4.50	.522	.151
RF7	12	4.17	.577	.167
RF8	12	4.83	.389	.112
SF1	12	4.92	.289	.083
SF2	12	4.58	.515	.149
SF3	12	4.92	.289	.083
BF1	12	4.50	.522	.151
BF2	12	4.00	.426	.123
BF3	12	4.58	.515	.149
BF4	12	4.75	.452	.131
BF5	12	4.58	.515	.149
BF6	12	4.75	.452	.131
BF7	12	3.25	.452	.131

One-Sample Test of Experts with Test Value = 3

Test Value = 3

	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
RF1	16.316	11	.001	1.833	1.59	2.08
RF2	7.000	11	.001	1.167	.80	1.53
RF3	10.652	11	.001	1.583	1.26	1.91
RF4	5.196	11	.001	1.500	.86	2.14
RF5	9.574	11	.001	1.250	.96	1.54
RF6	9.950	11	.001	1.500	1.17	1.83
RF7	7.000	11	.001	1.167	.80	1.53
RF8	16.316	11	.001	1.833	1.59	2.08
SF1	23.000	11	.001	1.917	1.73	2.10
SF2	10.652	11	.001	1.583	1.26	1.91
SF3	23.000	11	.001	1.917	1.73	2.10
BF1	9.950	11	.001	1.500	1.17	1.83
BF2	8.124	11	.001	1.000	.73	1.27
BF3	10.652	11	.001	1.583	1.26	1.91
BF4	13.404	11	.001	1.750	1.46	2.04
BF5	10.652	11	.001	1.583	1.26	1.91
BF6	13.404	11	.001	1.750	1.46	2.04
BF7	1.915	11	.082	.250	-.04	.54

Appendix B Confirmatory Study (Questionnaire)

Practitioners Survey

The aim of this research is to investigate the security factors that may influence an organisation to adopt cloud computing in Saudi Arabia government organisations. Your responses and expertise will help play a major role in addressing the factors that encourage or prevent the wide implementation of cloud computing. All information provided will be used for research purposes only. Thank you very much for taking part in this study.

Part 1 General Questions

1. Have you worked on an IT project for a government organization?
☐ Yes ☐ No
2. Have you used cloud services at your agency?
☐ Yes ☐ No
3. Do you think security affect your organization decision to adopt the cloud?
☐ Yes ☐ No
4. Choose the option that best reflects your years of experience in the security field:
☐ 2 years ☐ 3 – 5 years
☐ 6 – 10 years ☐ More than 10 years

Part 2 Study Questions (Security Risks, Social, and Benefits of Security in the Cloud)

5. The literature identified the following factors. To what extent do you agree with the importance of these factors in adopting the cloud services in your government organisations?

Coding	Attributes	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
II1	Insecure application programing interfaces risk has an impact decision to use cloud services.					
II2	Awareness of the insecure application programing interfaces risks affects the cloud adoption decision					
II3	Should be aware of security risks in the use of cloud such as Insecure Interfaces.					

ST1	Secure shared technology is essential to adopt cloud service.					
ST2	Shared technology model negatively affects the decision to use cloud services.					
AH1	Should be aware about that the account hijacking could occur when using cloud.					
AH2	Account hijacking risk considered the highest cloud security risk.					
AH3	Service hijacking often comes with stolen identifications that affect the decision to adopt cloud.					
MI1	Without full knowledge and control, your government agency will be at risk with malicious insider.					
MI2	Malicious insiders affect the confidentiality, integrity, and availability of the government information.					
MI3	It is important for any governments to understand what providers are doing to protect the cloud from malicious insider.					
CR1	The laws and regulations that exist nowadays are not sufficient to protect information stored in the cloud.					
CR2	Failure to Comply with Regulations is an effective factor that can make a secure reluctant transferring to the cloud.					
CR3	Failure to Comply with Regulations hinder the adoption decisions of cloud.					
CR4	It is necessary that cloud computing regulations comply with law in Saudi Arabia.					
DO1	Data ownership is critical factor in cloud security risk that my government agency require to take it in consideration.					
DO2	Data ownership should be qualified when the government agency adopting cloud.					
DO3	The ownership of data should be exclusive when adopting cloud.					
SDI1	Data integration in every government organisations must be ensure for their own data to be protected since it is moving between the end user and the cloud data Centre.					
SDI2	Unsecured data is more liable to interception when it transmission in the cloud.					
SDI3	Service integration is one of the top challenges that many government organisations face when implementing cloud.					

DL1	Should be concerned about the service provider's authentication systems that allow the access to data.					
DL2	Data leakages are weakness of physical transport system for cloud data and backups.					
DL3	Data leakage affects the adoption decisions of cloud.					
TR1	Secure cloud technology is trustworthy.					
TR2	Storing our organization's data under third-party control is one of our concerns.					
TR3	I feel confident storing my government data in the cloud.					
SC1	Security culture aspect is an important factor that should be taken into consideration when adopt the cloud.					
SC2	Security culture can support government agency decision.					
SC3	Security culture affect the execution of information security policies within the government organisations.					
PR1	A critical risk that affects the decision to use cloud services is privacy.					
PR2	Your government agency would use cloud services if the privacy to the information is guaranteed.					
PR3	My personal information in the cloud may be exposed to other parties without my knowledge.					
SS1	Smart scalable to multiple locations security benefit is an important driver to adopt the cloud.					
SS2	The ability to extend the security features in edges networks, is an important benefit to adopt the cloud. Timeless of response is importance smart scalable security benefits to adopt cloud.					
SS3	Smart scalable security benefits help my government agency to make decision adopting cloud.					
CE1	Cutting-edge cloud security market is important feature to secure the assets when adopt cloud.					
CE2	One of the top benefits to adopt the cloud is cutting edge in cloud security.					
AS1	Cloud provider can provide centralised security as service patches to help my government agency adopting cloud.					

AS2	In advance security mechanism, updates for the stakeholders more efficient than traditional organization security capability.					
AS3	To protect the assets, should implement advanced security mechanisms feature when adopting cloud.					
SSI1	Standardised security interfaces can ease any government's ability to change from provider to other in a short period.					
SSI2	Standardised security interfaces help to reduce a cost when the government using cloud.					
SSI3	It is importance to consider standardised security interfaces feature when making the decision to adopt cloud.					
CS1	Can be better organised auditing security benefit if the government wish to adopt cloud.					
CS2	Security auditing benefit allow to pay as you go for auditing when implementing the cloud.					
SLA1	Service level agreement audit enforcement considered of the top benefits because the provider have to comply with audit demands stated in the service level agreements.					
SLA2	Should consider the service level agreement audit enforcement when adopting cloud.					
RC1	Resource concentration benefit can adequately protecting government's data.					
RC2	Resource concentration benefit should consider as important factor when adopting cloud.					

Thanks you very much for your time.

B.1 Questionnaire Frequencies

Frequency Table of Questionnaire

II1

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	1	3.1	3.1	3.1
	3	1	3.1	3.1	6.3
	4	10	31.3	31.3	37.5
	5	20	62.5	62.5	100.0
	Total	32	100.0	100.0	

II2

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	3	2	6.3	6.3	6.3
	4	11	34.4	34.4	40.6
	5	19	59.4	59.4	100.0
	Total	32	100.0	100.0	

II3

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	3	2	6.3	6.3	6.3
	4	11	34.4	34.4	40.6
	5	19	59.4	59.4	100.0
	Total	32	100.0	100.0	

ST1

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	3	1	3.1	3.1	3.1
	4	11	34.4	34.4	37.5
	5	20	62.5	62.5	100.0
	Total	32	100.0	100.0	

ST2

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	5	15.6	15.6	15.6
	3	5	15.6	15.6	31.3
	4	10	31.3	31.3	62.5

5	12	37.5	37.5	100.0
Total	32	100.0	100.0	

AH1

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid 1	2	6.3	6.3	6.3
3	6	18.8	18.8	25.0
4	8	25.0	25.0	50.0
5	16	50.0	50.0	100.0
Total	32	100.0	100.0	

AH2

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid 1	4	12.5	12.5	12.5
3	3	9.4	9.4	21.9
4	13	40.6	40.6	62.5
5	12	37.5	37.5	100.0
Total	32	100.0	100.0	

AH3

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid 1	4	12.5	12.5	12.5
3	5	15.6	15.6	28.1
4	10	31.3	31.3	59.4
5	13	40.6	40.6	100.0
Total	32	100.0	100.0	

MI1

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid 1	2	6.3	6.3	6.3
3	3	9.4	9.4	15.6
4	11	34.4	34.4	50.0
5	16	50.0	50.0	100.0
Total	32	100.0	100.0	

MI2

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid 3	2	6.3	6.3	6.3
4	10	31.3	31.3	37.5
5	20	62.5	62.5	100.0
Total	32	100.0	100.0	

MI3

	Frequency	Percent	Valid Percent	Cumulative Percent
--	-----------	---------	---------------	--------------------

Valid	4	11	34.4	34.4	34.4
	5	21	65.6	65.6	100.0
Total		32	100.0	100.0	

CR1

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	2	6.3	6.3	6.3
	2	1	3.1	3.1	9.4
	3	7	21.9	21.9	31.3
	4	10	31.3	31.3	62.5
	5	12	37.5	37.5	100.0
Total		32	100.0	100.0	

CR2

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	2	6.3	6.3	6.3
	3	2	6.3	6.3	12.5
	4	15	46.9	46.9	59.4
	5	13	40.6	40.6	100.0
Total		32	100.0	100.0	

CR3

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	3	9.4	9.4	9.4
	3	2	6.3	6.3	15.6
	4	14	43.8	43.8	59.4
	5	13	40.6	40.6	100.0
Total		32	100.0	100.0	

CR4

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	3	2	6.3	6.3	6.3
	4	11	34.4	34.4	40.6
	5	19	59.4	59.4	100.0
Total		32	100.0	100.0	

DO1

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	3	2	6.3	6.3	6.3
	4	13	40.6	40.6	46.9
	5	17	53.1	53.1	100.0

Total	32	100.0	100.0	
-------	----	-------	-------	--

DO2

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid 1	2	6.3	6.3	6.3
3	3	9.4	9.4	15.6
4	11	34.4	34.4	50.0
5	16	50.0	50.0	100.0
Total	32	100.0	100.0	

DO3

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid 1	3	9.4	9.4	9.4
3	4	12.5	12.5	21.9
4	11	34.4	34.4	56.3
5	14	43.8	43.8	100.0
Total	32	100.0	100.0	

SDI1

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid 3	1	3.1	3.1	3.1
4	12	37.5	37.5	40.6
5	19	59.4	59.4	100.0
Total	32	100.0	100.0	

SDI2

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid 1	2	6.3	6.3	6.3
2	1	3.1	3.1	9.4
3	3	9.4	9.4	18.8
4	12	37.5	37.5	56.3
5	14	43.8	43.8	100.0
Total	32	100.0	100.0	

SDI3

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid 1	2	6.3	6.3	6.3
3	1	3.1	3.1	9.4
4	16	50.0	50.0	59.4
5	13	40.6	40.6	100.0
Total	32	100.0	100.0	

TR1

	Frequency	Percent	Valid Percent	Cumulative Percent
--	-----------	---------	---------------	--------------------

Valid	1	3	9.4	9.4	9.4
	3	2	6.3	6.3	15.6
	4	16	50.0	50.0	65.6
	5	11	34.4	34.4	100.0
	Total	32	100.0	100.0	

TR2

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	3	2	6.3	6.3	6.3
	4	15	46.9	46.9	53.1
	5	15	46.9	46.9	100.0
	Total	32	100.0	100.0	

TR3

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	5	15.6	15.6	15.6
	2	3	9.4	9.4	25.0
	3	2	6.3	6.3	31.3
	4	17	53.1	53.1	84.4
	5	5	15.6	15.6	100.0
	Total	32	100.0	100.0	

B.2 Questionnaire Reliability by Cronbach's Alpha

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardised Items	N of Items
.756	.796	51

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardised Items	N of Items
.716	.736	3

Item Statistics

	Mean	Std. Deviation	N
II1	4.50	.842	32
II2	4.53	.621	32
II3	4.53	.621	32

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardised Items	N of Items
.636	.696	2

Item Statistics

	Mean	Std. Deviation	N
ST1	4.59	.560	32
ST2	3.75	1.391	32

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardised Items	N of Items
.848	.849	3

Item Statistics			
	Mean	Std. Deviation	N
AH1	4.13	1.129	32
AH2	3.91	1.279	32
AH3	3.88	1.314	32

B.3 Questionnaire Analysis

One-Sample Statistics of the security risk questionnaire				
	N	Mean	Std. Deviation	Std. Error Mean
II1	32	4.50	.842	.149
II2	32	4.53	.621	.110
II3	32	4.53	.621	.110
ST1	32	4.59	.860	.099
ST2	32	3.75	1.391	.246
AH1	32	4.13	1.129	.200
AH2	32	3.91	1.279	.226
AH3	32	3.88	1.314	.232
MI1	32	4.22	1.070	.189
MI2	32	4.56	.619	.109
MI3	32	4.66	.783	.085
CR1	32	3.91	1.146	.203
CR2	32	4.16	1.019	.180
CR3	32	4.06	1.162	.205
CR4	32	4.53	.621	.110
DO1	32	4.47	.621	.110
DO2	32	4.22	1.070	.189
DO3	32	4.03	1.204	.213
SDI1	32	4.56	.564	.100
SDI2	32	4.09	1.118	.198
SDI3	32	4.19	.998	.176
DL1	32	4.25	.916	.162
DL2	32	3.97	1.092	.193
DL3	32	4.06	1.105	.195
One-Sample Statistics of the security social factors questionnaire				
	N	Mean	Std. Deviation	Std. Error Mean
TR1	32	4.00	1.136	.201
TR2	32	4.41	.615	.109
TR3	32	3.44	1.318	.233
SC1	32	4.19	.998	.176
SC2	32	4.19	.931	.165
SC3	32	4.25	.950	.168
PR1	32	4.50	.718	.127
PR2	32	4.25	1.016	.180
PR3	32	3.41	1.266	.224
One-Sample Statistics of the security benefits factors questionnaire				
	N	Mean	Std. Deviation	Std. Error Mean
SS1	32	4.16	.674	.101
SS2	32	4.09	.641	.113
SS3	32	4.16	.677	.120
SS4	32	4.00	1.016	.180
CE1	32	4.31	.693	.122
CE2	32	4.31	.592	.105
AS1	32	4.19	.738	.130
AS2	32	4.34	.845	.096
AS3	32	4.34	.602	.106

One-Sample Statistics of the security risk questionnaire				
	N	Mean	Std. Deviation	Std. Error Mean
SSI1	32	4.16	.884	.156
SSI2	32	4.34	.701	.124
SSI3	32	4.41	.615	.109
CS1	32	4.19	.693	.122
CS2	32	4.06	.716	.127
SLA1	32	4.03	.695	.123
SLA2	32	4.25	.880	.156
RC1	32	4.00	.718	.127
RC2	32	3.97	.740	.131

One-Sample Test of the Questionnaire for Security Risks Category

Test Value = 3

	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
II1	10.072	31	.001	1.500	1.20	1.80
II2	13.940	31	.001	1.531	1.31	1.76
II3	13.940	31	.001	1.531	1.31	1.76
ST1	16.102	31	.001	1.594	1.39	1.80
ST2	3.050	31	.005	.750	.25	1.25
AH1	5.638	31	.001	1.125	.72	1.53
AH2	4.008	31	.001	.906	.45	1.37
AH3	3.768	31	.001	.875	.40	1.35
MI1	6.445	31	.001	1.219	.83	1.60
MI2	14.281	31	.001	1.563	1.34	1.79
MI3	19.416	31	.001	1.656	1.48	1.83
CR1	4.473	31	.001	.906	.49	1.32
CR2	6.416	31	.001	1.156	.79	1.52
CR3	5.171	31	.001	1.063	.64	1.48
CR4	13.940	31	.001	1.531	1.31	1.76
DO1	13.371	31	.001	1.469	1.24	1.69
DO2	6.445	31	.001	1.219	.83	1.60
DO3	4.844	31	.001	1.031	.60	1.47
SDI1	15.661	31	.001	1.563	1.36	1.77
SDI2	5.536	31	.001	1.094	.69	1.50
SDI3	6.731	31	.001	1.188	.83	1.55
DL1	7.721	31	.001	1.250	.92	1.58
DL2	5.018	31	.001	.969	.58	1.36
DL3	5.438	31	.001	1.063	.66	1.46

One-Sample Test of the Questionnaire for Security Social Factors Category

Test Value = 3

	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
TR1	4.980	31	.001	1.000	.59	1.41
TR2	12.938	31	.001	1.406	1.18	1.63
TR3	1.877	31	.070	.438	-.04	.91
SC1	6.731	31	.001	1.188	.83	1.55
SC2	7.215	31	.001	1.188	.85	1.52
SC3	7.440	31	.001	1.250	.91	1.59
PR1	11.811	31	.001	1.500	1.24	1.76
PR2	6.960	31	.001	1.250	.88	1.62
PR3	1.815	31	.079	.406	-.05	.86

One-Sample Test of the Questionnaire for Security Benefits Category

Test Value = 3

	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
SS1	11.392	31	.001	1.156	.95	1.36
SS2	9.659	31	.001	1.094	.86	1.32
SS3	9.658	31	.001	1.156	.91	1.40
SS4	5.568	31	.001	1.000	.63	1.37
CE1	10.718	31	.001	1.313	1.06	1.56
CE2	12.535	31	.001	1.313	1.10	1.53
AS1	9.105	31	.001	1.188	.92	1.45
AS2	13.939	31	.001	1.344	1.15	1.54
AS3	12.636	31	.001	1.344	1.13	1.56
SSI1	7.400	31	.001	1.156	.84	1.47
SSI2	10.849	31	.001	1.344	1.09	1.60
SSI3	12.938	31	.001	1.406	1.18	1.63
CS1	9.698	31	.001	1.188	.94	1.44
CS2	8.399	31	.001	1.063	.80	1.32
SLA1	8.395	31	.001	1.031	.78	1.28
SLA2	8.036	31	.001	1.250	.93	1.57
RC1	7.874	31	.001	1.000	.74	1.26
RC2	7.407	31	.001	.969	.70	1.24

Appendix C Validation Study (Questionnaire)

C.1 Initial Instrument

Cloud Security Adoption Model for Government Organisations in Kingdom of Saudi Arabia

I am a PhD research student at University of Southampton, Southampton, UK. As part of my thesis, I am conducting a survey to investigate the security factor that might affect the Saudi government organisation to adopt cloud services.

The questionnaire designed for this research consists of two parts. The first part asks about the respondent's demographics. The second part asks about is the main study about the cloud security adoption of the government organisations.

If you are expert on IT and security in Saudi government organisation, I would be grateful if you fill out this survey. Your participant is voluntary and all responses will be anonymous and treated as completely confidential and it will be not be possible for anyone to identify the information you supply.

The questionnaire will only take 15 – 20 minutes of your time and it is recommended not to spend too long on any question. Your first thoughts are usually your best. Your participation is voluntary, and you can withdraw at any time without consequence.

If you have any queries or would like further information about this research please feel free to contact me.

Please select the appropriate
<input type="checkbox"/> I have read and understood the above and agree to take part in the survey.
<input type="checkbox"/> I have read and understood the above and don't wish to take part in the survey.

Thank you

Madini Alassafi

Electronics and Computer Science

University of Southampton, United Kingdom

SO17 1BJ, UK

Email: moa2g15@soton.ac.uk

The aim of this research is to investigate the security factors that may influence the adoption of cloud computing in Saudi Arabia government organisations. Your expertise will play a major role in addressing and building a security model of cloud computing services for government organisations which may be implemented widely. All information provided will be used for research purposes only. Thank you very much for taking part in this study.

Part 1 Demographic Information (General Questions)

- 1- Have you ever worked on IT or security project in Saudi government organisation?
 - ☐ Yes
 - ☐ No
- 2- Have you ever used cloud services at your organisation?
 - ☐ Yes
 - ☐ No
- 3- Do you think security affects your organisation decision to adopt cloud services?
 - ☐ Yes
 - ☐ No
- 4- Does your organisation adopt cloud services yet?
 - ☐ Yes
 - ☐ No
- 5- How many years of experience do you have in IT or security project field?
 - ☐ 2 years
 - ☐ 3 – 5 years
 - ☐ 6 – 10 years
 - ☐ More than 10 years

Part 2 Study Questions

To what extent do you agree about the effect of the following statements on the adopting of cloud services in your government organisations?

(Strongly Agree = 5, Agree = 4, Neutral = 3, Disagree = 2, Strongly Disagree = 1)

Construct	Statements	Coding	5	4	3	2	1
Insecure interfaces	Insecure application interfaces have an impact on the decision to adopt cloud services.	II1	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
	By understanding the dependency chain associated with secure interfaces, you can reduce the risks in adopting cloud services.	II2	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
	Awareness of the risks of insecure application interfaces affects the decision of adopt cloud services.	II3	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Shared technology	Secure shared technology affect the adoption of cloud services.	ST1	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
	Having a high quality of service in sharing technology would encourage us to use cloud computing.	ST2	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

	Some applications may be designed without using trusted computing practices, depending on the type of risks associated with the shared technology which affect the organisation decision to adopt the cloud.	ST3	o	o	o	o	o	o
Account hijacking	It is important to be aware of account hijacking risks while adopting cloud services.	AH1	o	o	o	o	o	o
	Account hijacking is considered to be one of the major risks in cloud services that affect the decision to adopt the cloud.	AH2	o	o	o	o	o	o
	Stolen identities, one of the risks of service hijacking, may affect the decision to adopt cloud services.	AH3	o	o	o	o	o	o
	Service hijacking often comes with stolen identifications that affect the decision to adopt cloud.	AH4	o	o	o	o	o	o
Malicious insiders	Without full knowledge and control, government organisations will be at risk with malicious insider attacks.	MI1	o	o	o	o	o	o
	Malicious insider risks can affect the confidentiality, integrity, and availability of the government organisation data.	MI2	o	o	o	o	o	o
	Saudi organisations should have knowledge about cloud providers' measures to avoid risk of malicious insider.	MI3	o	o	o	o	o	o
Failure to Comply with Regulations	Compliance with regulations affects Saudi government decision to use cloud services.	CR1	o	o	o	o	o	o
	Current Laws and regulations in Saudi government organisation are not sufficient to protect information stored in the cloud.	CR2	o	o	o	o	o	o
	It is necessary that cloud computing regulations comply with Saudi Arabia laws.	CR3	o	o	o	o	o	o
	Failure to Comply with Regulations is an effective factor that can make a secure reluctant transferring to the cloud.	CR4	o	o	o	o	o	o
Data ownership	Data ownership affects Saudi government decision to use cloud services.	DO1	o	o	o	o	o	o
	In order to reduce risks associated with Data Ownership, ownership of data should be authorised while adopting cloud services.	DO2	o	o	o	o	o	o
	The ownership of data should be exclusive when adopting cloud.	DO3	o	o	o	o	o	o
	Data ownership terms should be clearly stated in services level agreement.	DO4	o	o	o	o	o	o
	Data ownership is critical factor in cloud security that my government agency require to take it in consideration.	DO5	o	o	o	o	o	o
Service and data integration	Data integration affects Saudi government decision to adopt cloud services.	SDI1	o	o	o	o	o	o
	Integration of Saudi government applications with cloud services is causing a challenge to adopt the cloud.	SDI2	o	o	o	o	o	o
	Unsecured data is more susceptible to interception while being transmitted in the cloud.	SDI3	o	o	o	o	o	o

Data leakage	The fear of leaking Saudi government data affects the decision to adopt the cloud.	DL1	o	o	o	o	o
	Non-disclosed of data leakage events on the cloud provider raise concerns in Saudi government organisations.	DL2	o	o	o	o	o
	In general, data leakage risk hinders Saudi organisations' adoption of the cloud.	DL3	o	o	o	o	o
	Data leakages are weakness of physical transport system for cloud data and backups.	DL4	o	o	o	o	o
Failure of Client-side encryption	Client-side encryption affects Saudi government decision to use cloud services.	CSE1	o	o	o	o	o
	Saudi organisations should be aware about Client-side encryption while it plays in an important role in data protection.	CSE2	o	o	o	o	o
	The organisations feel that the client-side encryption risks outweigh the benefits of adopting the cloud services.	CSE3	o	o	o	o	o
Trust	Trust affects Saudi government decision use cloud services.	TR1	o	o	o	o	o
	Access of third-parties to an organisation's data may raise security concerns and affects the adoption of the cloud.	TR2	o	o	o	o	o
	Storing our organisation's data under third-party control is one of our concerns to adopt the cloud.	TR3	o	o	o	o	o
Security Culture	Security culture affects Saudi government decision use cloud services.	SC1	o	o	o	o	o
	Security culture affects the execution of information security policies within government organisations.	SC2	o	o	o	o	o
	Organisations would be more confident in using cloud services if the provider was based in Saudi Arabia.	SC3	o	o	o	o	o
Privacy	Privacy concerns affect the government organisation decision to use cloud services.	PR1	o	o	o	o	o
	Government organisations would be more confident to use cloud services if the privacy of the information was guaranteed.	PR2	o	o	o	o	o
	Access to personal information by third-party organisations may raise privacy concerns and affect the decision to use the cloud.	PR3	o	o	o	o	o
Smart Scalable security benefits	Smart scalable security benefits affect government organisations' decision to adopt cloud services.	SS1	o	o	o	o	o
	The ability to extend the security features in edges network promote the government organisation to adopt the cloud.	SS2	o	o	o	o	o
	Smart scalable to multiple locations security benefit is driven the government organisation to adopt the cloud.	SS3	o	o	o	o	o

	Timeless of response is importance smart scalable security benefits to adopt cloud.	SS4	o	o	o	o	o	o
Cutting-edge security market	Cutting edge cloud security marketing affects government organisations' decision to adopt cloud services.	CE1	o	o	o	o	o	o
	Saudi organisations should consider the cutting-edge benefits in cloud security marketing while adopting the cloud services.	CE2	o	o	o	o	o	o
	Cloud security marketing services affect the adoption of the cloud as it provides solutions to critical problems facing organisations and support remote workforces.	CE3	o	o	o	o	o	o
Advanced security mechanism	Advanced security mechanisms benefits affect government organisations' decision to adopt cloud services.	AS1	o	o	o	o	o	o
	Having sufficient support from the cloud provider in advance security mechanism would encourage organisation to use cloud services.	AS2	o	o	o	o	o	o
	With advance security mechanism it is necessary to have adequate technical support from the cloud provider before and after adopting cloud services.	AS3	o	o	o	o	o	o
Standardised security interfaces	Implementation of the standardised security interface features affects government organisations' decision to adopt cloud services.	SSI1	o	o	o	o	o	o
	Saudi organisations awareness about cloud interfaces security standards benefits (cost reduction), would encourage them to adopt the cloud.	SSI2	o	o	o	o	o	o
	Standardised security interfaces influence the adoption of cloud since it can ease the organisations' ability to change from one provider to another quickly.	SSI3	o	o	o	o	o	o
	It is importance to consider standardised security interface features when adopting the cloud.	SSI4	o	o	o	o	o	o
Cloud security auditing	Cloud security auditing affects government organisations' decision to adopt cloud services.	CS1	o	o	o	o	o	o
	Saudi organisations knowledge about cloud security auditing benefits such as pay as you go auditing drive them to adopt the cloud.	CS2	o	o	o	o	o	o
	Cloud scalable auditing feature, influence the decision to adopt the cloud in Saudi organisations.	CS3	o	o	o	o	o	o
SLA audit enforcement	Enforcing audit terms and conditions in the service level agreement by Saudi organisations would promote the cloud adoption decision.	SLA1	o	o	o	o	o	o
	Cloud providers' compliance to Saudi regulations audit requirements, helps the Saudi organisations to adopt their cloud services.	SLA2	o	o	o	o	o	o

	Clear stating of audit responsibilities of both Saudi organisation and the cloud provider, influence the decision of adopting the cloud.	SLA3	o	o	o	o	o
Resource concentration	Resource concentration benefits affect government organisations' decision to adopt cloud services.	RC1	o	o	o	o	o
	Saudi organisations awareness of cloud resource concentration (pool of security protection features), can accelerate the decision to adopt the cloud.	RC2	o	o	o	o	o
	Comprehensive security policy, advanced data management controls and up to date patches in resource concentration approach, would encourage the adoption decision.	RC3	o	o	o	o	o
Decision to adopt the cloud	It is likely that Saudi organisations will take steps to adopt cloud computing in the future.	DAC1	o	o	o	o	o
	Saudi organisations decide to adopt cloud computing.	DAC2	o	o	o	o	o
	I think, in the near future, most of the Saudi government organisations are going to decide to adopt the cloud services.	DAC3	o	o	o	o	o
	I feel comfortable recommending the adoption of cloud to my organisation.	DAC4	o	o	o	o	o

C.2 Expert Evaluation Feedback

Note to Experts for Evaluation Purposes

Greeting,

I am a PhD research student at University of Southampton, Southampton, UK. As part of my thesis, I am conducting evaluation feedback from your expertise in order to evaluate the questions for security factor that might affect the Saudi government organisation to adopt cloud services.

Please evaluate this instrument using the evaluation criteria as below:

Evaluation Criteria of the Items/ Scales	Definition
Essential	The question is necessary to define the security factors in cloud computing adoption. It needed be involved and if not involved would affect the factors negatively.
Useful but NOT essential	The question may be valuable but NOT necessary to define the factors in cloud computing adoption
NOT essential	The question is NOT necessary to define the security factors in cloud computing adoption. It is NOT needed be involved and if involved would NOT affect the factors.

This evaluation is to get the understanding if the questions are important or not and whether the scales appropriately measuring the question or not. If you are expert on IT and security in Saudi government organisation, I would be grateful if you fill out this survey. Your participant is voluntary and all responses will be anonymous and treated as completely confidential and it will be not be possible for anyone to identify the information you supply.

Please evaluate the item by placing a tick (✓) in appropriate part of the evaluation criteria

Thank you

Madini Alassafi

Electronics and Computer Science

University of Southampton, United Kingdom SO17 1BJ, UK

Email: moa2g15@soton.ac.uk

Evaluation Criteria of the Items				
Security Factor	Item Number	Essential	Useful but NOT essential	NOT essential
Insecure interfaces	II1	○	○	○
	II2	○	○	○
	II3	○	○	○
Shared technology	ST1	○	○	○
	ST2	○	○	○
	ST3	○	○	○
Account hijacking	AH1	○	○	○
	AH2	○	○	○
	AH3	○	○	○
Malicious insiders	MI1	○	○	○
	MI2	○	○	○
	MI3	○	○	○
Failure to Comply with Regulations	CR1	○	○	○
	CR2	○	○	○
	CR3	○	○	○
Data ownership	DO1	○	○	○
	DO2	○	○	○
	DO3	○	○	○
Service and data integration	DO4	○	○	○
	SDI1	○	○	○
	SDI2	○	○	○
Data leakage	SDI3	○	○	○
	DL1	○	○	○
	DL2	○	○	○
Failure of Client-side encryption	DL3	○	○	○
	CSE1	○	○	○
	CSE2	○	○	○
Trust	CSE3	○	○	○
	TR1	○	○	○
	TR2	○	○	○
Security Culture	TR3	○	○	○
	SC1	○	○	○
	SC2	○	○	○
Privacy	SC3	○	○	○
	PR1	○	○	○
	PR2	○	○	○
Smart Scalable security benefits	PR3	○	○	○
	SS1	○	○	○
	SS2	○	○	○
Cutting-edge security market	SS3	○	○	○
	CE1	○	○	○

Evaluation Criteria of the Items				
Security Factor	Item Number	Essential	Useful but NOT essential	NOT essential
	CE2	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
	CE3	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Advanced security mechanism	AS1	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
	AS2	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
	AS3	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Standardised security interfaces	SSI1	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
	SSI2	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
	SSI3	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cloud security auditing	CS1	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
	CS2	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
	CS3	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
SLA audit enforcement	SLA1	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
	SLA2	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
	SLA3	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Resource concentration	RC1	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
	RC2	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
	RC3	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Decision to adopt the cloud	DAC1	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
	DAC2	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
	DAC3	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
	DAC4	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Thanks you very much for your time.

C.3 Content Validity Ratio Analysis

Content Validity Ratio (CVR) Among Factors with its Items					
Items	Important	Neither Important nor Unimportant	Unimportant	CVR	CVR Average
II1	6	1	0	0.71	0.90
II2	7	0	0	1.00	
II3	7	0	0	1.00	
ST1	6	0	1	0.71	0.81
ST2	7	0	0	1.00	
ST3	6	1	0	0.71	
AH1	6	1	0	0.71	0.71
AH2	7	0	0	1.00	
AH3	6	0	1	0.71	
AH4	5	1	1	0.43	0.71
MI1	6	1	0	0.71	
MI2	6	0	1	0.71	
MI3	6	0	1	0.71	0.90
CR1	7	0	0	1.00	
CR2	7	0	0	1.00	
CR3	6	1	0	0.71	0.77
CR4	4	2	1	0.14	
DO1	6	0	1	0.71	
DO2	7	0	0	1.00	0.71
DO3	7	0	0	1.00	
DO4	7	0	0	1.00	
DO5	4	2	1	0.14	0.71
SDI1	6	0	1	0.71	
SDI2	6	1	0	0.71	
SDI3	6	1	0	0.71	0.86
DL1	7	0	0	1.00	
DL2	7	0	0	1.00	
DL3	6	0	1	1.00	0.43
DL4	5	1	1	0.43	
CSE1	6	1	0	0.71	
CSE2	7	0	0	1.00	0.81
CSE3	6	1	0	0.71	
TR1	6	1	0	0.71	
TR2	6	1	0	0.71	1.00
TR3	7	0	0	1.00	
SC1	7	0	0	1.00	

Content Validity Ratio (CVR) Among Factors with its Items					
Items	Important	Neither Important nor Unimportant	Unimportant	CVR	CVR Average
SC2	7	0	0	1.00	0.71
SC3	6	0	1	0.71	
PR1	6	1	0	0.71	
PR2	6	0	1	0.71	
PR3	6	0	1	0.71	0.64
SS1	7	0	0	1.00	
SS2	6	0	1	0.71	
SS3	6	0	1	0.71	
SSI4	4	2	1	0.14	0.81
CE1	6	0	1	0.71	
CE2	6	0	1	0.71	
CE3	7	0	0	1.00	
AS1	7	0	0	1.00	0.90
AS2	7	0	0	1.00	
AS3	6	1	0	0.71	
SSI1	6	0	1	0.71	
SSI2	7	0	2	1.00	0.90
SSI3	7	0	0	1.00	
CS1	6	0	1	0.71	
CS2	7	0	0	1.00	
CS3	7	0	0	1.00	0.81
SLA1	7	0	0	1.00	
SLA2	6	1	0	0.71	
SLA3	6	1	0	0.71	
RC1	6	1	0	0.71	0.71
RC2	6	0	1	0.71	
RC3	6	0	1	0.71	
DAC1	6	1	0	0.71	
DAC2	7	0	0	1.00	0.86
DAC3	6	0	1	0.71	
DAC4	7	0	0	1.00	

C.4 Content Validity Ratio Analysis for 67 Items

Factor	Total of items	Significant Items	CVR item 1	CVR item 2	CVR item 3	CRV item 4	CVR item 5	Average CVR
II	3 items	3 items	0.7	1.00	1.00	-	-	0.90
ST	3 items	3 items	0.7	1.00	0.7.6	-	-	0.81
AH	4 items	3 items	0.7	1.00	0.7	0.4	-	0.71
MI	3 items	3 items	0.7	0.7	0.7	-	-	0.71
CR	4 items	3 items	1.00	1.00	0.7	0.1	-	0.90
DO	5 items	4 items	0.7	1.00	1.00	1.00	0.1	0.77
SDI	3 items	3 items	0.7	0.7	0.7	-	-	0.71
DL	4 items	3 items	1.00	1.00	1.00	0.4	-	0.86
CSE	3 items	3 items	0.7	1.00	0.7	-	-	0.81
TR	3 items	3 items	0.7	0.7	1.00	-	-	0.81
SC	3 items	3 items	1.00	1.00	0.7	-	-	0.90
PR	3 items	3 items	0.7	0.7	0.7	-	-	0.71
SS	4 items	3 items	1.00	0.7	0.7	0.1	0.4	0.64
CE	3 items	3 items	0.7	0.7	1.00	-	-	0.81
AS	3 items	3 items	1.00	1.00	0.7	-	-	0.90
SSI	4 items	3 items	1.00	0.7	0.7	0.1	-	0.64
CS	3 items	3 items	0.7	0.7	1.00	-	-	0.90
SLA	3 items	3 items	1.00	0.7	0.7	-	-	0.81
RC	3 items	3 items	0.7	0.7	0.7	-	-	0.71
DAC	4 items	4 items	0.7	1.00	0.7	1.00	-	0.86
Total	67	62						

C.5 Correlations Matrix

Correlations																				
		II	ST	AH	MI	CR	DO	SDI	DL	CSE	TR	SC	PR	SS	CE	AS	SSI	CS	SLA	RC
II	Pearson Correlation	1	.646**	.160	.348	.228	.076	.467**	.216	.135	-.054	.067	.272	.020	.011	.171	-.146	-.249	-.064	-.053
	Sig. (2-tailed)		.000	.397	.060	.227	.690	.009	.251	.477	.778	.723	.145	.917	.953	.366	.441	.184	.735	.782
	N	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30
ST	Pearson Correlation	.646**	1	.335	.296	.435*	.200	.446*	.186	.433*	.083	.119	.355	.081	.168	.169	.063	-.152	.054	.104
	Sig. (2-tailed)	.000		.071	.112	.016	.289	.013	.325	.017	.662	.530	.055	.669	.374	.371	.740	.423	.775	.584
	N	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30
AH	Pearson Correlation	.160	.335	1	.189	.214	.630*	.484*	.493*	.706*	.419*	.479*	.571*	.395*	.329	.420*	.441*	.259	.346	.299
	Sig. (2-tailed)	.397	.071		.316	.257	.000	.007	.006	.000	.021	.007	.001	.031	.076	.021	.015	.168	.061	.108
	N	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30
MI	Pearson Correlation	.348	.296	.189	1	.112	.212	.366*	.234	.190	-.068	-.049	.216	.095	.000	.144	.086	-.142	-.123	-.049
	Sig. (2-tailed)	.060	.112	.316		.556	.260	.047	.214	.315	.720	.797	.251	.617	1.000	.447	.651	.453	.519	.798
	N	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30
CR	Pearson Correlation	.228	.435*	.214	.112	1	.425*	.464*	.402*	.398*	.425*	.188	.290	.527*	.306	.590*	.430*	.313	.414*	.270
	Sig. (2-tailed)	.227	.016	.257	.556		.019	.010	.028	.029	.019	.320	.119	.003	.100	.001	.018	.092	.023	.150
	N	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30
DO	Pearson Correlation	.076	.200	.630**	.212	.425*	1	.510**	.648**	.505**	.358	.470**	.384*	.426*	.217	.376*	.348	.273	.296	.192
	Sig. (2-tailed)	.690	.289	.000	.260	.019		.004	.000	.004	.052	.009	.036	.019	.250	.040	.059	.145	.112	.310
	N	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30
SDI	Pearson Correlation	.467**	.446*	.484**	.366*	.464**	.510**	1	.540**	.506**	.213	.420*	.517**	.364*	.371*	.377*	.334	.169	.213	.199
	Sig. (2-tailed)	.009	.013	.007	.047	.010	.004		.002	.004	.258	.021	.003	.048	.044	.040	.071	.372	.259	.292
	N	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30
DL	Pearson Correlation	.216	.186	.493**	.234	.402*	.648**	.540**	1	.259	.595**	.491**	.552**	.427*	.187	.609**	.462*	.213	.487**	.306
	Sig. (2-tailed)	.251	.325	.006	.214	.028	.000	.002		.167	.001	.006	.002	.018	.323	.000	.010	.259	.006	.100
	N	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30
CSE	Pearson Correlation	.135	.433*	.706**	.190	.398*	.505**	.506**	.259	1	.405*	.307	.280	.428*	.346	.319	.428*	.139	.359	.335
	Sig. (2-tailed)	.477	.017	.000	.315	.029	.004	.004	.167		.026	.099	.134	.018	.061	.086	.018	.462	.051	.070
	N	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30
TR	Pearson Correlation	-.054	.083	.419*	-.068	.425*	.358	.213	.595**	.405*	1	.281	.251	.497**	.339	.662**	.679**	.267	.728**	.568**
	Sig. (2-tailed)	.778	.662	.021	.720	.019	.052	.258	.001	.026		.133	.180	.005	.067	.000	.000	.154	.000	.001
	N	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30
SC	Pearson Correlation	.067	.119	.479**	-.049	.188	.470**	.420*	.491**	.307	.281	1	.212	.349	.347	.346	.497**	.448*	.467**	.308

	Sig. (2-tailed)	.723	.530	.007	.797	.320	.009	.021	.006	.099	.133		.260	.058	.060	.061	.005	.013	.009	.098
	N	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30
PR	Pearson Correlation	.272	.355	.571**	.216	.290	.384*	.517**	.552**	.280	.251	.212	1	.129	.049	.390*	.252	.113	.193	.105
	Sig. (2-tailed)	.145	.055	.001	.251	.119	.036	.003	.002	.134	.180	.260		.498	.795	.033	.180	.553	.307	.579
	N	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30
SS	Pearson Correlation	.020	.081	.395*	.095	.527**	.426*	.364*	.427*	.428*	.497**	.349	.129	1	.592**	.746**	.753**	.654**	.790**	.793**
	Sig. (2-tailed)	.917	.669	.031	.617	.003	.019	.048	.018	.018	.005	.058	.498		.001	.000	.000	.000	.000	.000
	N	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30
CE	Pearson Correlation	.011	.168	.329	.000	.306	.217	.371*	.187	.346	.339	.347	.049	.592**	1	.494**	.615**	.509**	.534**	.494**
	Sig. (2-tailed)	.953	.374	.076	1.000	.100	.250	.044	.323	.061	.067	.060	.795	.001		.006	.000	.004	.002	.006
	N	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30
AS	Pearson Correlation	.171	.169	.420*	.144	.590**	.376*	.377*	.609**	.319	.662**	.346	.390*	.746**	.494**	1	.781**	.456*	.741**	.572**
	Sig. (2-tailed)	.366	.371	.021	.447	.001	.040	.040	.000	.086	.000	.061	.033	.000	.006		.000	.011	.000	.001
	N	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30
SSI	Pearson Correlation	-.146	.063	.441*	.086	.430*	.348	.334	.462*	.428*	.679**	.497**	.252	.753**	.615**	.781**	1	.569**	.847**	.726**
	Sig. (2-tailed)	.441	.740	.015	.651	.018	.059	.071	.010	.018	.000	.005	.180	.000	.000	.000		.001	.000	.000
	N	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30
CS	Pearson Correlation	-.249	-.152	.259	-.142	.313	.273	.169	.213	.139	.267	.448*	.113	.654**	.509**	.456*	.569**	1	.578**	.510**
	Sig. (2-tailed)	.184	.423	.168	.453	.092	.145	.372	.259	.462	.154	.013	.553	.000	.004	.011	.001		.001	.004
	N	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30
SLA	Pearson Correlation	-.064	.054	.346	-.123	.414*	.296	.213	.487**	.359	.728**	.467**	.193	.790**	.534**	.741**	.847**	.578**	1	.860**
	Sig. (2-tailed)	.735	.775	.061	.519	.023	.112	.259	.006	.051	.000	.009	.307	.000	.002	.000	.000	.001		.000
	N	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30
RC	Pearson Correlation	-.053	.104	.299	-.049	.270	.192	.199	.306	.335	.568**	.308	.105	.793**	.494**	.572**	.726**	.510**	.860**	1
	Sig. (2-tailed)	.782	.584	.108	.798	.150	.310	.292	.100	.070	.001	.098	.579	.000	.006	.001	.000	.004	.000	
	N	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30
DAC	Pearson Correlation	.052	.111	.319	.076	.587*	.294	.527*	.178	.598*	.301	.431*	.093	.701*	.490*	.468*	.515*	.460*	.553*	.551**
	Sig. (2-tailed)	.785	.560	.086	.689	.001	.115	.003	.346	.000	.107	.017	.626	.000	.006	.009	.004	.010	.002	.002
	N	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30
**. Correlation is significant at the 0.01 level (2-tailed).																				
*. Correlation is significant at the 0.05 level (2-tailed).																				

C.6 Reliability

Reliability Statistics All Items

Cronbach's Alpha	Cronbach's Alpha Based on Standardised Items	N of Items
.945	.948	62

Reliability Statistics of Security Risk Factors

Cronbach's Alpha	Cronbach's Alpha Based on Standardised Items	N of Items
.839	.837	9

Inter-Item Correlation Matrix

	II	ST	AH	MI	CR	DO	SDI	DL	CSE
II	1.000	.646	.160	.348	.228	.076	.467	.216	.135
ST	.646	1.000	.335	.296	.435	.200	.446	.186	.433
AH	.160	.335	1.000	.189	.214	.630	.484	.493	.706
MI	.348	.296	.189	1.000	.112	.212	.366	.234	.190
CR	.228	.435	.214	.112	1.000	.425	.464	.402	.398
DO	.076	.200	.630	.212	.425	1.000	.510	.648	.505
SDI	.467	.446	.484	.366	.464	.510	1.000	.540	.506
DL	.216	.186	.493	.234	.402	.648	.540	1.000	.259
CSE	.135	.433	.706	.190	.398	.505	.506	.259	1.000

Reliability Statistics of Security Social Factors

Cronbach's Alpha	Cronbach's Alpha Based on Standardised Items	N of Items
.730	.726	3

Inter-Item Correlation Matrix

	TR	SC	PR
TR	1.000	.281	.251
SC	.281	1.000	.212
PR	.251	.212	1.000

Reliability Statistics of Security Benefit Factors

Cronbach's Alpha	Cronbach's Alpha Based on Standardised Items	N of Items
.927	.928	7

Inter-Item Correlation Matrix

	SS	CE	AS	SSI	CS	SLA	RC
SS	1.000	.592	.746	.753	.654	.790	.793
CE	.592	1.000	.494	.615	.509	.534	.494
AS	.746	.494	1.000	.781	.456	.741	.572
SSI	.753	.615	.781	1.000	.569	.847	.726
CS	.654	.509	.456	.569	1.000	.578	.510
SLA	.790	.534	.741	.847	.578	1.000	.860
RC	.793	.494	.572	.726	.510	.860	1.000

C.7 Improved Instrument

Practitioners Survey

Security Factors that Influence Cloud Computing Adoption in Saudi Government Organisations

I am a PhD research student at University of Southampton, Southampton, UK. As part of my thesis, I am conducting a survey to investigate the security factor that might affect the Saudi government organisation to adopt cloud services.

The aim of this research is to investigate the security factors that may influence the adoption of cloud computing in Saudi Arabia government organisations. Your expertise will play a major role in addressing and building a security model of cloud computing services for government organisations which may be implemented widely. All information provided will be used for research purposes only. Thank you very much for taking part in this study.

The questionnaire designed for this research consists of two parts. The first part asks about the respondent's demographics. The second part asks about is the main study about the cloud security adoption of the government organisations.

If you are expert on IT and security in Saudi government organisation, I would be grateful if you fill out this survey. Your participant is voluntary and all responses will be anonymous and treated as completely confidential and it will be not be possible for anyone to identify the information you supply.

The questionnaire will only take 15 – 20 minutes of your time and it is recommended not to spend too long on any question. Your first thoughts are usually your best. Your participation is voluntary, and you can withdraw at any time without consequence.

If you have any queries or would like further information about this research please feel free to contact me.

Please select the appropriate
<input type="checkbox"/> I have read and understood the above and agree to take part in the survey.
<input type="checkbox"/> I have read and understood the above and don't wish to take part in the survey.

Thank you

Madini Alassafi

Electronics and Computer Science

University of Southampton, United Kingdom

SO17 1BJ, UK

Email: moa2g15@soton.ac.uk

Part 1: General Questions

1. Have you worked in an IT or security project in Saudi government organisation?
 - ☐ Yes
 - ☐ No
2. Have you ever used cloud services at your organisation?
 - ☐ Yes
 - ☐ No
3. Does your organisation adopt cloud services yet?
 - ☐ Yes
 - ☐ No
4. Do you think security affects your organisation's decision to adopt the cloud?
 - ☐ Yes
 - ☐ No
5. Choose the option that best reflects your years of experience in the IT or security field:
 - ☐ 2 years
 - ☐ 3 – 5 years
 - ☐ 6 – 10 years
 - ☐ More than 10 years

Part 2: Study Questions (Security Risks, Social, and Benefits of Security in the Cloud)

The proposed model consists of three categories, the Security Social Category, the Cloud Security Risks Category and the Cloud Security Benefits Category.

The Main question in this survey:

6. To what extent do you agree about the effect of the following statements on the adopting of cloud services in your government organisations?

Strongly Agree = 5, Agree = 4, Neutral = 3, Disagree = 2, Strongly Disagree= 1

Factor	Statements	Coding	5	4	3	2	1
Insecure interfaces	Insecure application interfaces have an impact on the decision to adopt cloud services.	II1	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
	By understanding the dependency chain associated with secure interfaces, you can reduce the risks in adopting cloud services.	II2	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
	Awareness of the risks of insecure application interfaces affects the decision of adopt cloud services.	II3	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Shared technology	Secure shared technology affect the adoption of cloud services.	ST1	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
	Having a high quality of service in sharing technology would encourage us to use cloud computing.	ST2	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
	Some applications may be designed without using trusted computing practices, depending on the type of risks associated with the shared technology which affect the organisation decision to adopt the cloud.	ST3	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Account hijacking	It is important to be aware of account hijacking risks while adopting cloud services.	AH1	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
	Account hijacking is considered to be one of the major risks in cloud services that affect the decision to adopt the cloud.	AH2	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

	Stolen identities, one of the risks of service hijacking, may affect the decision to adopt cloud services.	AH3	o	o	o	o	o	o
Malicious insiders	Without full knowledge and control, government organisations will be at risk with malicious insider attacks.	MI1	o	o	o	o	o	o
	Malicious insider risks can affect the confidentiality, integrity, and availability of the government organisation data.	MI2	o	o	o	o	o	o
	Saudi organisations should have knowledge about cloud providers' measures to avoid risk of malicious insider.	MI3	o	o	o	o	o	o
Failure to Comply with Regulations	Compliance with regulations affects Saudi government decision to use cloud services.	CR1	o	o	o	o	o	o
	Current Laws and regulations in Saudi government organisation are not sufficient to protect information stored in the cloud.	CR2	o	o	o	o	o	o
	It is necessary that cloud computing regulations comply with Saudi Arabia laws.	CR3	o	o	o	o	o	o
Data ownership	Data ownership affects Saudi government decision to use cloud services.	DO1	o	o	o	o	o	o
	In order to reduce risks associated with Data Ownership, ownership of data should be authorised while adopting cloud services.	DO2	o	o	o	o	o	o
	The ownership of data should be exclusive when adopting cloud.	DO3	o	o	o	o	o	o
	Data ownership terms should be clearly stated in services level agreement.	DO4	o	o	o	o	o	o
Service and data integration	Data integration affects Saudi government decision to adopt cloud services.	SDI1	o	o	o	o	o	o
	Integration of Saudi government applications with cloud services is causing a challenge to adopt the cloud.	SDI2	o	o	o	o	o	o
	Unsecured data is more susceptible to interception while being transmitted in the cloud.	SDI3	o	o	o	o	o	o
Data leakage	The fear of leaking Saudi government data affects the decision to adopt the cloud.	DL1	o	o	o	o	o	o
	Non-disclosed of data leakage events on the cloud provider raise concerns in Saudi government organisations.	DL2	o	o	o	o	o	o
	In general, data leakage risk hinder Saudi organisation to adopt the cloud.	DL3	o	o	o	o	o	o
Failure of Client-side encryption	Client-side encryption affects Saudi government decision to use cloud services.	CSE1	o	o	o	o	o	o
	Saudi organisations should be aware about Client-side encryption while it plays in an important role in data protection.	CSE2	o	o	o	o	o	o
	The organisations feel that the client-side encryption risks outweigh the benefits of adopting the cloud services.	CSE3	o	o	o	o	o	o
Trust	Trust affects Saudi government decision use cloud services.	TR1	o	o	o	o	o	o
	Access of third-parties to an organisation's data may raise security concerns and affects the adoption of the cloud.	TR2	o	o	o	o	o	o
	Storing our organisation's data under third-party control is one of our concerns to adopt the cloud.	TR3	o	o	o	o	o	o
Security Culture	Security culture affects Saudi government decision use cloud services.	SC1	o	o	o	o	o	o

	Security culture affects the execution of information security policies within government organisations.	SC2	o	o	o	o	o	o
	Organisations would be more confident in using cloud services if the provider was based in Saudi Arabia.	SC3	o	o	o	o	o	o
Privacy	Privacy concerns affect the government organisation decision to use cloud services.	PR1	o	o	o	o	o	o
	Government organisations would be more confident to use cloud services if the privacy of the information was guaranteed.	PR2	o	o	o	o	o	o
	Access to personal information by third-party organisations may raise privacy concerns and affect the decision to use the cloud.	PR3	o	o	o	o	o	o
Smart Scalable security benefits	Smart scalable security benefits affect government organisations' decision to adopt cloud services.	SS1	o	o	o	o	o	o
	The ability to extend the security features in edges network promote the government organisation to adopt the cloud.	SS2	o	o	o	o	o	o
	Smart scalable to multiple locations security benefit is driven the government organisation to adopt the cloud.	SS3	o	o	o	o	o	o
Cutting-edge security market	Cutting-edge cloud security marketing affects government organisations' decision to adopt cloud services.	CE1	o	o	o	o	o	o
	Saudi organisations should consider the cutting-edge benefits in cloud security marketing while adopting the cloud services.	CE2	o	o	o	o	o	o
	Cloud security marketing services affect the adoption of the cloud as it provides solutions to critical problems facing organisations and support remote workforces.	CE3	o	o	o	o	o	o
Advanced security mechanism	Advanced security mechanisms benefits affect government organisations' decision to adopt cloud services.	AS1	o	o	o	o	o	o
	Having sufficient support from the cloud provider in advance security mechanism would encourage organisation to use cloud services.	AS2	o	o	o	o	o	o
	With advance security mechanism it is necessary to have adequate technical support from the cloud provider before and after adopting cloud services.	AS3	o	o	o	o	o	o
Standardised security interfaces	Implementation of the standardised security interface features affects government organisations' decision to adopt cloud services.	SSI1	o	o	o	o	o	o
	Saudi organisations awareness about cloud interfaces security standards benefits (cost reduction), would encourage them to adopt the cloud.	SSI2	o	o	o	o	o	o
	Standardised security interfaces influence the adoption of cloud since it can ease the organisations' ability to change from one provider to another quickly.	SSI3	o	o	o	o	o	o
Cloud security auditing	Cloud security auditing affects government organisations' decision to adopt cloud services.	CS1	o	o	o	o	o	o
	Saudi organisations knowledge about cloud security auditing benefits such as pay as you go auditing drive them to adopt the cloud.	CS2	o	o	o	o	o	o

	Cloud scalable auditing feature, influence the decision to adopt the cloud in Saudi organisations.	CS3	o	o	o	o	o	o
SLA audit enforcement	Enforcing audit terms and conditions in the service level agreement by Saudi organisations would promote the cloud adoption decision.	SLA1	o	o	o	o	o	o
	Cloud providers' compliance to Saudi regulations audit requirements, helps the Saudi organisations to adopt their cloud services.	SLA2	o	o	o	o	o	o
	Clear stating of audit responsibilities of both Saudi organisation and the cloud provider, influence the decision of adopting the cloud.	SLA3	o	o	o	o	o	o
Resource concentration	Resource concentration benefits affect government organisations' decision to adopt cloud services.	RC1	o	o	o	o	o	o
	Saudi organisations awareness of cloud resource concentration (pool of security protection features), can accelerate the decision to adopt the cloud.	RC2	o	o	o	o	o	o
	Comprehensive security policy, advanced data management controls and up to date patches in resource concentration approach, would encourage the adoption decision.	RC3	o	o	o	o	o	o
Decision to adopt the cloud	It is likely that Saudi organisations will take steps to adopt cloud computing in the future.	DAC1	o	o	o	o	o	o
	Saudi organisations decide to adopt cloud computing.	DAC2	o	o	o	o	o	o
	I think, in the near future, most of the Saudi government organisations are going to decide to adopt the cloud services.	DAC3	o	o	o	o	o	o
	I feel comfortable recommending the adoption of cloud to my organisation.	DAC4	o	o	o	o	o	o

C.8 Exploratory Factor Analysis Results

C.8.1 Reliability among Security Factors

Reliability Statistics Among Security Factors

Cronbach's Alpha	Cronbach's Alpha Based on Standardised Items	N of Items
.865	.842	20

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted	N
II	82.3926	44.957	.873	.946	215
ST	82.3523	44.729	.770	.945	215
AH	82.3973	44.642	.789	.946	215
MI	82.2143	45.293	.692	.946	215
CR	82.5012	42.837	.757	.942	215
DO	82.3147	43.302	.675	.944	215
SDI	82.2686	44.032	.657	.944	215
DL	82.4283	45.116	.854	.947	215
CSE	82.3554	42.130	.706	.943	215
TR	82.4547	43.525	.651	.944	215
SC	82.3244	43.609	.620	.944	215
PR	82.3461	44.962	.819	.947	215
SS	82.6081	39.687	.849	.940	215
CE	82.5756	40.505	.789	.941	215
AS	82.4205	40.180	.844	.940	215
SSI	82.6578	40.410	.833	.940	215
CS	82.5244	41.004	.777	.942	215
SLA	82.4919	40.257	.865	.940	215
RC	82.6578	40.547	.796	.941	215
DAC	82.8578	40.747	.701	.941	215

C.8.2 Correlations among Security Factors in the Instrument

Inter-Item Correlation Matrix																				
Construct	II	ST	AH	MI	CR	DO	SDI	DL	CSE	TR	SC	PR	SS	CE	AS	SSI	CS	SLA	RC	DAC
II	1	.646**	.160	.348	.228	.076	.467**	.216	.135	-.054	.067	.272	.020	.011	.171	-.146	-.249	-.064	-.053	.552**
ST	.646**	1	.335	.296	.435*	.200	.446*	.186	.433*	.083	.119	.355	.081	.168	.169	.063	-.152	.054	.104	.411*
AH	.160	.335	1	.189	.214	.630**	.484**	.493**	.706**	.419*	.479**	.571**	.395*	.329	.420*	.441*	.259	.346	.299	.319*
MI	.348	.296	.189	1	.112	.212	.366*	.234	.190	-.068	-.049	.216	.095	.000	.144	.086	-.142	-.123	-.049	.576**
CR	.228	.435*	.214	.112	1	.425*	.464**	.402*	.398*	.425*	.188	.290	.527**	.306	.590**	.430*	.313	.414*	.270	.587**
DO	.076	.200	.630**	.212	.425*	1	.510**	.648**	.505**	.358	.470**	.384*	.426*	.217	.376*	.348	.273	.296	.192	.494*
SDI	.467**	.446*	.484**	.366*	.464**	.510**	1	.540**	.506**	.213	.420*	.517**	.364*	.371*	.377*	.334	.169	.213	.199	.527**
DL	.216	.186	.493**	.234	.402*	.648**	.540**	1	.259	.595**	.491**	.552**	.427*	.187	.609**	.462*	.213	.487**	.306	.578**
CSE	.135	.433*	.706**	.190	.398*	.505**	.506**	.259	1	.405*	.307	.280	.428*	.346	.319	.428*	.139	.359	.335	.598**
TR	-.054	.083	.419*	-.068	.425*	.358	.213	.595**	.405*	1	.281	.251	.497**	.339	.662**	.679**	.267	.728**	.568**	.301*
SC	.067	.119	.479**	-.049	.188	.470**	.420*	.491**	.307	.281	1	.212	.349	.347	.346	.497**	.448*	.467**	.308	.431*
PR	.272	.355	.571**	.216	.290	.384*	.517**	.552**	.280	.251	.212	1	.129	.049	.390*	.252	.113	.193	.105	.493*
SS	.020	.081	.395*	.095	.527**	.426*	.364*	.427*	.428*	.497**	.349	.129	1	.592**	.746**	.753**	.654**	.790**	.793**	.701**
CE	.011	.168	.329	.000	.306	.217	.371*	.187	.346	.339	.347	.049	.592**	1	.494**	.615**	.509**	.534**	.494**	.490**

AS	.171	.169	.420*	.144	.590**	.376*	.377*	.609**	.319	.662**	.346	.390*	.746**	.494**	1	.781**	.456*	.741**	.572**	.468**
SSI	-.146	.063	.441*	.086	.430*	.348	.334	.462*	.428*	.679**	.497**	.252	.753**	.615**	.781**	1	.569**	.847**	.726**	.515**
CS	-.249	-.152	.259	-.142	.313	.273	.169	.213	.139	.267	.448*	.113	.654**	.509**	.456*	.569**	1	.578**	.510**	.460*
SLA	-.064	.054	.346	-.123	.414*	.296	.213	.487**	.359	.728**	.467**	.193	.790**	.534**	.741**	.847**	.578**	1	.860**	.553**
RC	-.053	.104	.299	-.049	.270	.192	.199	.306	.335	.568**	.308	.105	.793**	.494**	.572**	.726**	.510**	.860**	1	.551**
DAC	.552**	.411*	.319*	.576**	.587**	.494*	.527**	.578**	.598**	.301*	.431*	.493*	.701**	.490**	.468**	.515**	.460*	.553**	.551**	1
**. Correlation is significant at the 0.01 level (2-tailed).																				
*. Correlation is significant at the 0.05 level (2-tailed).																				

C.8.3 KMO and Bartlett's Test

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.881
Bartlett's Test of Sphericity	Approx. Chi-Square	4128.125
	df	171
	Sig.	.001

C.8.4 Communalities

Communalities		
	Initial	Extraction
II	1.000	.505
ST	1.000	.602
AH	1.000	.612
MI	1.000	.595
CR	1.000	.664
DO	1.000	.710
SDI	1.000	.751
DL	1.000	.644
CSE	1.000	.770
TR	1.000	.632
SC	1.000	.564
PR	1.000	.827
SS	1.000	.903
CE	1.000	.802
AS	1.000	.829
SSI	1.000	.872
CS	1.000	.815
SLA	1.000	.878
RC	1.000	.829
DAC	1.000	.862

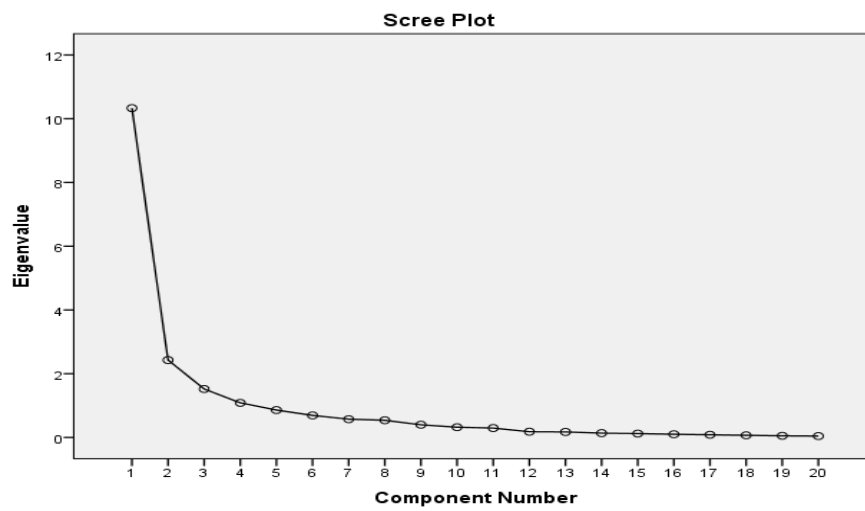
Extraction Method: Principal

Component Analysis.

C.8.5 Total Variance Explained

Total Variance Explained									
Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	9.802	51.588	51.588	9.802	51.588	51.588	6.510	34.263	34.263
2	2.391	12.585	64.173	2.391	12.585	64.173	4.387	23.090	57.353
3	1.310	6.892	71.065	1.310	6.892	71.065	2.605	13.712	71.065
4	.998	5.254	76.319						
5	.859	4.516	80.835						
6	.858	4.396	81.133						
7	.680	3.581	84.415						
8	.556	2.928	87.344						
9	.521	2.742	90.085						
10	.398	2.094	92.179						
11	.311	1.639	93.818						
12	.295	1.551	95.369						
13	.180	.947	96.316						
14	.160	.842	97.158						
15	.136	.715	97.872						
16	.107	.566	98.438						
17	.098	.514	98.952						
18	.081	.428	99.380						
19	.067	.353	99.732						
20	.051	.268	100.000						
Extraction Method: Principal Component Analysis.									

C.8.6 Scree Plot



C.8.7 Rotated Component Matrix

Rotated Component Matrix^a

	Component		
	1	2	3
SS	.903		
RC	.829		
SSI	.872		
SLA	.878		
CS	.815		
AS	.829		
CE	.802		
CR	.664		.443
TR	.632		.544
DAC	.862		
CSE		.770	
MI		.595	
SDI		.751	
DO		.710	
II		.505	
ST		.602	
SC		.564	
PR			.827
AH			.612
DL			.644

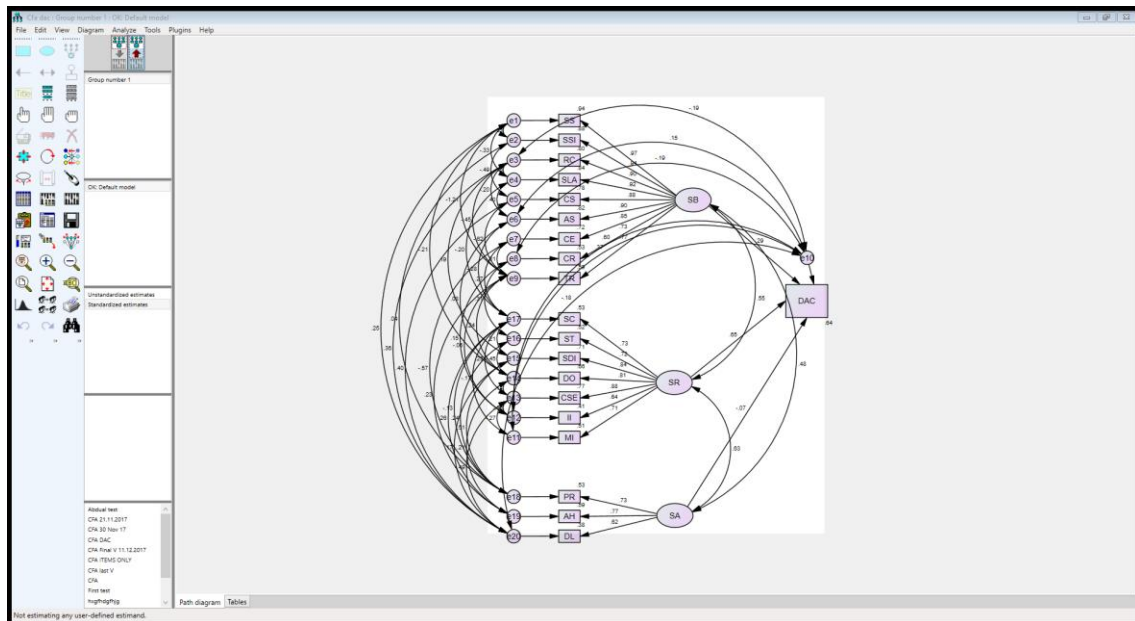
C.9 Confirmatory Factor Analysis Results

C.9.1 Construct Reliability

Construct Reliability (CR)						
Constructs			Loadings	Error	(SUM(loadings))^2	CR
TR	<--- -	SB	0.657	0.108	59.305401	0.987873
CR	<--- -	SB	0.735	0.091		
CE	<--- -	SB	0.852	0.115		
AS	<--- -	SB	0.91	0.070		
CS	<--- -	SB	0.869	0.091		
SLA	<--- -	SB	0.938	0.046		
SSI	<--- -	SB	0.907	0.070		
RC	<--- -	SB	0.892	0.084		
SS	<--- -	SB	0.941	0.053		
CSE	<--- -	SR	0.871	0.072	27.321529	0.983265
MI	<--- -	SR	0.658	0.055		
SDI	<--- -	SR	0.83	0.044		
DO	<--- -	SR	0.843	0.057		
II	<--- -	SR	0.609	0.082		
ST	<--- -	SR	0.693	0.061		
SC	<--- -	SR	0.723	0.094		
PR	<--- -	SA	0.687	0.090	4	0.94162
AH	<--- -	SA	0.78	0.064		
DL	<--- -	SA	0.533	0.094		
DAC	<--- -	SA	0.640	0.038		

C.9.2 Measurement Model with Modifications Indices

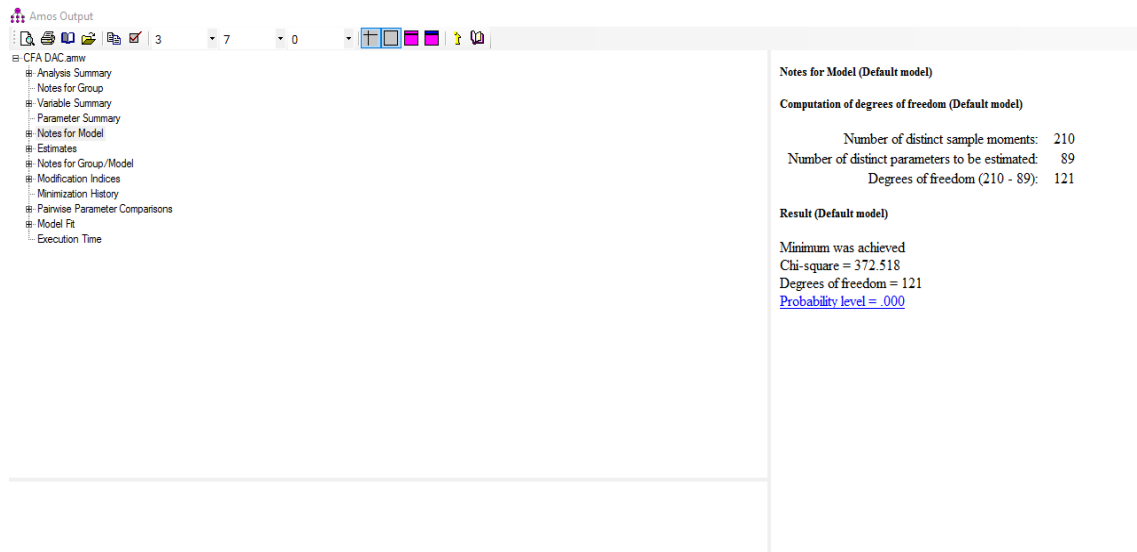
Unstandardized estimates



C.9.3 Standardized Regression Weights: (Group number 1 - Default model)

			Estimate
SS	<---	SB	.941
RC	<---	SB	.895
SSI	<---	SB	.902
SLA	<---	SB	.952
CS	<---	SB	.846
AS	<---	SB	.936
CE	<---	SB	.817
SC	<---	SR	.684
ST	<---	SR	.747
II	<---	SR	.622
DO	<---	SR	.874
SDI	<---	SR	.819
MI	<---	SR	.674
CSE	<---	SR	.860
DL	<---	SA	.534
AH	<---	SA	.774
PR	<---	SA	.696
TR	<---	SB	.693
CR	<---	SB	.770
DAC	<---	SR	.516

C.9.5 Model Fit Summary



The screenshot shows the Amos Output window for a CFA model. The left pane lists the following sections: Analysis Summary, Notes for Group, Variable Summary, Parameter Summary, Notes for Model, Estimates, Notes for Group/Model, Modification Indices, Minimization History, Pairwise Parameter Comparisons, Model Fit, and Execution Time. The right pane displays the following information:

Notes for Model (Default model)

Computation of degrees of freedom (Default model)

Number of distinct sample moments:	210
Number of distinct parameters to be estimated:	89
Degrees of freedom (210 - 89):	121

Result (Default model)

Minimum was achieved
 Chi-square = 372.518
 Degrees of freedom = 121
[Probability level = .000](#)

CMIN

Model	NPAR	CMIN	DF	P	CMIN/DF
Default model	51	800.821	139	.000	5.761
Saturated model	190	.000	0		
Independence model	19	4271.162	171	.000	24.978

RMR, GFI

Model	RMR	GFI	AGFI	PGFI
Default model	.013	.923	.630	.730
Saturated model	.000	1.000		
Independence model	.145	.178	.087	.160

Baseline Comparisons

Model	NFI Delta1	RFI rho1	IFI Delta2	TLI rho2	CFI
Default model	.813	.869	.840	.918	.945
Saturated model	1.000		1.000		1.000
Independence model	.000	.000	.000	.000	.000

NCP

Model	NCP	LO 90	HI 90
Default model	661.821	576.570	754.571
Saturated model	.000	.000	.000
Independence model	4100.162	3890.880	4316.715

RMSEA

Model	RMSEA	LO 90	HI 90	PCLOSE
Default model	.096	.084	.108	.100
Independence model	.335	.326	.343	.000

HOELTER

Model	HOELTER	HOELTER
	.05	.01
Default model	45	49
Independence model	11	11

Standardized RMR (SRAR)