Factors Determining E-Government Security

A Thesis Submitted for the Degree of Doctor of Philosophy

By

Hasan Ali Razzaqi

School of Information Systems, Computing and Mathematics

Department of Information Systems and Computing

Brunel University

2013

PhD Abstract

E-Government security is a major area of concern that has the potential to affect the success of e-Government services across the world. Much of the literature has addressed this phenomenon by applying principles of computer science or engineering which tend to be objective. User concern of e-Government service security has not been addressed applying social science principles or management that tend to be subjective and have not been addressed in the literature. Objective research outcomes are unfortunately not suitable to address subjective factors. Further, user centric approach has not been adopted in most of the empirical studies that have dealt with e-Government security leading to lack of an understanding of how users perceive or feel or comprehend about e-Government services, particularly e-Government service security. Most of the research efforts addressing e-Government security have focused on either technological issues or engineering issues neglecting user perceptions and behavioural aspects. This disadvantage has led to possible reduction in the up-take of e-Government services. There was a need to have an in-depth understanding of user centric e-Government security and user centric factors that affect it as its antecedents addressing which it is possible to enhance user confidence in e-Government and hence its success. This research has addressed this partially.

While addressing the concerns raised above, this research has defined and identified certain user centric factors that are required to examine the user centric nature of e-Government service security from the management and social sciences perspective. E-Government literature was critically reviewed to determine the user centric factors and their relationship to user centric e-Government security with the help of theories, models, concepts and frameworks that have not been applied so far. Contextual factors have been identified as important user centric ones that affect user centric e-Government security with e-Government technology chosen as the main contextual determinant of user centric e-Government security. User trust and user felt risk in using e-Government services were brought in as mediators of this relationship due to the prime importance these two user centric factors carry with regard to affecting the relationship between technology and user centric e-Government security. In addition demographic factors and culture (nationality) as a factor were applied to test their influence on the relationship between user trust and user centric e-Government security mediated by user felt risk to find whether they have any impact. Moderators (Human Computer Interaction (HCI), user privacy and web design quality) of this relationship were added to the investigation as literature showed that e-Government technology could not operate in isolation. Finally empirical outcomes of testing the above relationships were practically tested by examining the influence of perceived ease of use and

usefulness on the relationship between user trust and user centric e-Government security mediated by user felt risk to find whether technology impacted users in reality. Theoretical framework was drawn from the literature review leading to a conceptual model that was used to answer the research question. 12 hypotheses were tested in all.

The research was conducted in the Kingdom of Bahrain which ranks high in the implementation of e-Government (e.g. 14th ranked in the world in implementing e-participation in 2014 ranked by UN). The country offered a fertile ground for conducting research as the e-Government service provided were updated technologically constantly with the latest technological advancement cloud computing introduced in e-Government service provision. Most government services were offered now through e-Government services. The population was cosmopolitan and education levels of the users of e-Government were reasonably high providing a strong basis for conducting this research.

Quantitative research method and survey questionnaire strategy were used. Users of e-Government services were the target population. Sampling procedure yielded 309 valid responses. Rigourous statistical analysis provided the findings. Except for 2 hypotheses the remaining were verified and established. Technology was found to determine user centric e-Government security with the mediation by trust being stronger than risk. HCI and web design quality moderated the relationship between technology and user centric e-Government security significantly. User education and experience were found to influence user trust and user centric e-Government security. User privacy and nationality were not found to be statistically significant. Perceived ease of use and usefulness of the technology were found to influence e-Government security mediated by trust and risk. This research was perhaps one of the first to have been conducted in a context where e-Government technology used cloud computing.

The research contributed to the growing body of knowledge in the field of e-Government security that has viewed this phenomenon from the lens of social sciences and management. Theoretical contribution showed how the operationalization and relationship amongst the factors could be explained by expanding the application of theories including socio-technical, behavioural, managerial, technology adoption, organiational and HCI. Practical implications showed the usefulness of this research to users, service providers and policy makers involved with e-Government services. Methodologically this research has introduced a verification stage by which it has verified the theoretical results using practical outcomes.

Acknowledgements

Praise Allah, the Almighty and merciful, in whom every being on earth owes its existence and pray to the Almighty and His Prophet Mohammed (S.A.W.A).

Foremost I would like to express my deepest gratitude to Prof. Abdulla Al-Hawaj, President, Ahlia University, for his continuous encouragement, support and inspiration, which enabled me to complete this thesis.

In the same vein, I would like to my sincere thanks and appreciation to Dr. Ramzi El-Haddadeh, my academic supervisor at Brunel University for his excellent supervision, positive criticism and valuable feedback. At the same time, I wish to thank my co-supervisor at Ahlia University Dr. Masaud Jahromi, for his constant support and encouragement.

In addition, I would like to thank and appreciate the constant support provided by Dr. Tillal Eldabi of Brunel University who provided timely advice when needed during my journey through the PhD.

Last but not the least, my deepest gratitude and thanks go to my beloved wife and family members, who bore the brunt of the effects of my journey through the PhD and for their patience, moral support and continued encouragement without which I could not have completed this thesis.

Table of Contents

PhD Abstract ii
Acknowledgements iv
Chapter 1: Introduction 1
1.1 Current Status of E-Government 2
1.2 E-Government in Bahrain 4
1.3 Problems in E-Government Services Security 6
1.4 Problem Statement 6
1.5 Research Questions 7
1.6 Aim of the Research 7
1.7 Objectives 8
1.8 Significance of Study 8
1.9 Thesis Structure 9
1.10 Summary 9
Chapter 2: Literature Review 10
2.1 Introduction 10
2.2 E-Government 12
2.3 E-Government Security 15
2.4 Synthesis of Theories Affecting E-Government Security 16
2.5 Context of E-Government 20
2.6 Contextual Factors Affecting E-Government 24
2.6.1 Demographic Factors 26
2.6.2 Technology 28
2.6.3 Nationality as a Cultural Contextual Factor Affecting E-Government 31
2.7 Antecedents of E-Government Security that Affect Citizens 32
2.7.1 Technology as an Antecedent of E-Government Services Security 33
2.7.2 Moderators of Technology, an Antecedent of E-Government Security 34
2.7.3 Trust as an Antecedent of E-Government Services Security 35
2.8. Factors Affecting the Relationship between Trust and E-Government Services Security 38
2.8.1 Perceived Ease of Use (PEOU) and Perceived Usefulness (PU) as Antecedents of Trust in E-Government Technology 38
2.8.2 Demographic Factors as Antecedents of Trust in E-Government Technology 40
2.9 Risk as an Antecedent of E-Government Services Security 40
2.10 Factors Affecting the Relationship between Technology and E-Government Security 42
2.10.1 Human Computer Interaction (HCI) 43
2.10.2 Privacy of Users 44

2.10.3 Quality of Web Design 45
2.11 Gaps in the literature 46
2.12 Conclusion 48
Chapter 3: Theoretical Framework 49
3.1 Introduction 49
3.2 Research Context 49
3.3 E-Government Security and User Centricity 49
3.3.1 Relationship between Risk and User Centric E-Government Security 50
3.3.2 Relationship between Trust of Users and User Centric E-Government Security 51
3.3.3 Relationship between Technology and User Centric E-Government Security 52
3.4 Moderators of Technology 53
3.4.1 Influence of HCI on the Relationship between E-Government Technology and User Centric E-Government Security 53
3.4.2 Influence of User Privacy on the Relationship between-Government Technology and User Centric E-Government Security 54
3.4.3 Influence of Web Design Quality on the Relationship between E-Government Technology and User Centric E-Government Security 55
3.5 Impact of Contextual Factors on Trust of Users of E-Government Services 56
3.6 Impact of Perceived Ease of Use and Usefulness on Trust of Users of E-Government Services 57
3.7 Conclusion 59
Chapter 4: Research Methodology 60
4.1 Introduction 60
4.2 Research Background 60
4.3 Research Methodology 60
4.4 Research Philosophy 61
4.4.1 Positivism 62
4.4.2 Interpretivism 63
4.5 Choice of the Research Philosophy 64
4.6 Research Methods 65
4.6.1 Choice of the Type of Research Method 69
4.6.1.1 Use of Descriptive Study - Survey Method 70
4.7 Research Design 72
4.7.1 The Type of Investigation 73
4.7.2 The Research Setting 73
4.7.3 Unit of Analysis 73
4.7.4 Time Horizon of the Research 73
4.7.5 Extent of Researcher Interference with the Research 73

4.7.6 Data Collection 74
4.7.7 Data Analysis 74
4.8 Research Strategy 74
4.9 Data Collection 75
4.10 Data Analysis 75
4.10.1 Validity 77
4.10.2 Content Validity 78
4.10.3 Convergent Validity 78
4.10.4 Construct Validity 78
4.10.5 Main Survey Data Analysis 78
4.10.6 Missing Data 79
4.10.7 Outliers 79
4.10.8 Multivariate Normality 80
4.10.9 Multicollinearity 81
4.10.10 Structural Equation Modeling 81
4.10.11 Factor Analysis 81
4.11 Ethical Consideration 82
4.12 Methodology Outline 83
4.13 Summary 84
Chapter 5: Empirical Research: Data Collection and Analysis 85
5.1 Introduction 85
5.2 Questionnaire as the Method for the Main Survey 85
5.2.1 Development of the Questionnaire 86
5.2.2 Questionnaire Design 86
5.2.3 Questionnaire Validation 87
5.3 Pilot Study 87
5.3.1 Reliability 89
5.3.2 Validity 90
5.4 Main Survey 92
5.4.1 Population 92
5.4.2 Sample Size 92
5.4.3 Data Collection 94
5.4.4 Data Analysis 94
5.4.5 Outliers 95
5.4.6 Multicollinearity 96
5.5 Confirmatory Factor Analysis (CFA) 96

5.5.1 Construct Reliability 98
5.5.2 Discriminant Validity 98
5.6 Structure Equation Modelling (SEM) 102
5.6.1 Model Specification 102
5.6.1.1 SEM1 104
5.6.1.2 Model identification of SEM1 108
5.6.1.3 Measure Selection to Data Preparation 108
5.6.1.4 Model Evaluation (Model fit) 108
5.6.1.5 Test of Parsimony 109
5.6.1.6 Testing the Minimum Sample Discrepancy Function for Acceptability of the Model Fit 109
5.6.1.7 Assessing Population Discrepancy Measures 110
5.6.1.8 Comparing Baseline Model 110
5.6.1.9 Checking the Goodness of Fit Index 110
5.6.1.10 Model Analysis (Model Estimation) 110
5.7 Path Analysis 113
5.7.1 Effect of moderators on SEM1 116
5.7.2 Model Identification 120
5.7.3 Path Analysis of SEM1.0 123
5.7.4 SEM2 126
5.7.5 Model Identification 129
5.7.6 Model Fit 130
5.7.8 Path Analysis of SEM2 132
5.8 Unidimensionality 135
5.9 Common Method Bias 136
5.9 Summary 137
Chapter 6: Discussion 138
6.1 Introduction 138
6.2 Research Question RQ1: What are the Factors that can be Considered as User-Centric and Affect E-Government Services Security? 138
6.3 Research Question RQ2: How Those Factors Affect E-Government Services Security when there is a Change in Technology? 143
6.4 Analysis of the Relationship Technology–ET-ER-User-Centric e-Government Services Security 143
6.5 Analysis of the Relationship (HCI, EP, Service Quality)-Technology–ET-ER-User Centric e-Government Services Security 145
6.6 Relationship between User Experience, Education and Nationality and E-Government Security 146

6.7 Relationship between Perceived Ease of Use, Perceived Usefulness and E-Government Security 146
6.8 Summary 148
Chapter 7: Conclusion 149
7.1 Introduction 149
7.2 Study Context 149
7.3 The Aim 150
7.4 Contribution to Knowledge 154
7.5 Contribution to Theory 161
7.6 Contribution to Methodology 164
7.7 Contribution to Practice 164
7.8 Limitations of Research 165
7.9 Recommendations for Future Research 166
References 167
Appendix A: Literature Review Chapter Support Document 189
Appendix B: Research Ethics 190
Appendix C: Questions Survey and Statistical Analysis Tables 192

List of Tables

Table 1.1: World E-Government Leaders (Very High EGDI) in 2014....4
Table 2.1: Factors Contributing To the Development of E-Government 22
Table 2.2: Some of The Contextual Factors that are Found to Influence E-Government....25
Table 2.3: Example of Adoption Model 29
Table 2.4: Most Common Factors Affecting Different Users of E-Government Where Cloud Computing is Deployed 30
Table 4.1: Comparative Overview of Some of Major IS Research Paradigms....64
Table 4.2: Example of IS Security Research Methods 66
Table 4.3: Comparative Overview of Quantitative and Qualitative Research Methods....67
Table 4.3: Summary of Strengths And Weaknesses of The Quantitative and Qualitative Methods 68
Table 5.1: Descriptive of Demographic and Contextual Variables 88
Table 5.2: Pilot Survey Finding Summary....89
Table 5.3: SMC for Model SEM1.1....106
Table 5.4: CMIN for Model SEM1.1....107
Table 5.5: Bollen-Stine Bootstrap....107
Table 5.6: Regression Weights for Model SEM1.1 (Without Moderators)....108
Table 5.7: Parsimony 109
Table 5.8: Baseline Comparisons....110
Table 5.9: RMSEA....110
Table 5.10: Regression Weights for SEM1.1 113
Table 5.11: SMC, SEM1.1 (Constructs)....113
Table 5.12: Summary of results of SEM1.1 (Summary of the Significant Influence of Determinant on e-Government security)....116
Table 5.13: SMC for Model SEM1.0....118
Table 5.14: CMIN, AMOS-SEM1.0-Initial Model-after deleting EP....119
Table 5.15: Standardized Regression Weights SEM1.0 120
Table 5.16: Parsimony of SEM1.0....120
Table 5.17: Baseline Comparisons SEM1.0 121
Table 5.18: RMSEA SEM1.0 121
Table 5.19: Baseline Comparisons SEM1.0 121
Table 5.20: SMC, SEM1.0 (Constructs)....123
Table 5.21: Summary of the Significant Influence of Determinant on e-Government Security....125
Table 5.22: Correlations HCI and Service Quality 126
Table 5.23: SEM2, SMC....129
Table 5.24: Chi-square test 129
Table 5.25: Standardized Regression Weights SEM2 129

Table 5.26: Baseline comparison SEM2 130
Table 5.27: RMSEA SEM2 130
Table 5.28: SMC, SEM2 (constructs) 133
Table 5.29: Summary of Results of SEM2 134
Table 5:30: Covariance PEOU and PU 135
Table 5.31: AVE (Average Variance Extracted) 136
Table 6.1, Standardized Total Effects (SEM1) 143
Table 6.2 Standardized Indirect Effects 144
Table 6.3, Final List of Hypotheses Accepted and Rejected 148
Table C1: Questionnaire for Measuring the Security of E-Government Services 192
Table C2: Pilot Study Data Correlation 198
Table C3: Descriptive data Analysis (From Main Survey) 200
Table C4: Maximum Percentage of Outliers 202
Table C5: Squared Multiple Correlations 203
Table C6: Residual Covariances (Group number 1 - Default model) 205
Table C7: Standardized Residual Covariances (Group number 1 - Default model) 206
Table C8: Sample Correlation 208
Table C9: Variance Extracted (Variable and Items code) 210
Table C10: Sample Correlation for SEM1.0 212
Table C11: Sample Correlations – Estimates for SEM1.1 214
Table C12: Residual Covariances for SEM1.1 215
Table C13: Standardized Residual Covariance for SEM1.1 216
Table C14, Baseline Comparisons 219
Table C15, RMR, GFI 219
Table C16, RMSEA 219
Table C17: Residual Covariances for SEM1.0 after deleting EP1, EP2, EP3, EP4 and EP5 220
Table C18: Standardized Residual Covariances for SEM1.0 after deleting EP1, EP2, EP3, EP4 and EP5 221
Table C19, RMR, GFI for Model SEM1.0-Initial model-after deleting EP 224
Table C20, Baseline Comparisons for Model SEM1.0-Initial model-after deleting EP 224
Table C21, RMSEA for Model SEM1.0-Initial model-after deleting EP 224
Table C22: Sample Correlations - Estimates 225
Table C23: Variance Extracted AVE for SEM 1.0 226
Table C24: Variance Extracted AVE for SEM 2.0 227

List of Figures

Figure 1.1: E-Government Portal of Government of Sweden, Showing Social Media Networking 3
Figure 1.2: E-Government Portal of the Government of UK Showing Multiple Services Offered....3
Figure 1.3: E-Government Portal of Government of Bahrain (e-Government, 2015) 5
Figure 2.1: Literature Review Structure 11
Figure 2.2: Four Stage Model of E-Government Online Service Index 21
Figure 3.1: Research Model 59
Figure 4.1: Research Methodology Outline 83
Figure 5.1: Contextual, Relationship between Contextual Factors and Trust as an Antecedent of e-Government Security 91
Figure 5.2, Specified CFA model 97
Figure 5.3: CFA Model after Deleting Items (HCI11, EU2, ER2, ER7, ET5 and ESec4) 99
Figure 5.4: Discriminant Analysis of Five Latent Variables 101
Figure 5.5 Discriminant Analysis of Six Latent Variables 102
Figure 5.6: SEM1 for Analyzing Influence of Technology on E-Government Security. 104
Figure 5.7: SEM2 for Analyzing Perception of Users of E-Government Security Characterized by Cloud Computing....104
Figure 5.8: SEM1 without Moderators 105
Figure 5.9: SEM1.1 without Moderators (Standardized)....106
Figure 5.10: SEM1.1 Unstandardized Model 111
Figure 5.11: SEM1.1 Standardized Model....112
Figure 5.12: (Final SEM1.1) 116
Figure 5.13: SEM1.0-Initial Model, Moderators of Technology-e-Government Security 117
Figure 5.14: AMOS-SEM1.0-Initial Model-after Deleting EP....119
Figure 5.15: SEM 1.0 (Unstandardised) 122
Figure 5.16: SEM 1.0 (Standardised)....122
Figure 5.17: SEM 1.0 (Final Model)....126
Figure 5.18: SEM2 For Analyzing Perception of Users of E-Government Security Characterized by Cloud Computing....127
Figure 5.19: SEM2....128
Figure 5.20: SEM2 (Unstandardized) 131
Figure 5.21: SEM2 (Standardized) 132
Figure 5.22: SEM2 (Final Model)....135
Figure 7.1: E-Government Portal of the Kingdom of Bahrain....159
Figure C1: SEM1 213

LIST OF ABBREVIATIONS

Cobit	Control Objectives for Information and Related Technology
EHCII	Construct used to represent the HCI index variable
EPOUI	Construct used to represent perceived ease of use index
EPUI	Construct used to represent perceived usefulness index
ERI	Construct used to represent risk index
ESeI	Construct used to represent security index
ETI	Construct used to represent trust index
HCI / EHCI	Construct used to represent the Human computer Interaction
ISO	International Organization for Standardization
PEOU / EPEOU	Construct used to represent perceived ease of use in e-Government services
Privacy / EP	Construct used to represent the privacy in e-Government services
PU / EPU	Construct used to represent perceived usefulness in e-Government services
Quality / EQ	Construct used to represent website quality in e-Government services
Risk / ER	Construct used to represent risk in e-Government services
Trust / ET	Construct used to represent trust in e-Government services

Chapter 1: Introduction

Rapid development of e-Government services is revolutionising the way government services are being delivered to the people. In line with this argument, Ihmouda et al. (2015) assert that e-Government is the reason for the reforms taking place in the public sector policies around the world. Further, Ihmouda et al. (2015) claim that public sector organisations want to leverage the benefits offered by the computer-based information and communication technologies (ICTs) in making public sectors innovative while offering e-Government services. Echoing similar sentiments Ouyang and Lee (2015) argue that internet-based e-business and e-Government services are linking businesses, households and governments at rapid pace. ICTs contribute significantly to e-Government service provision in terms of providing easy access to government information, increasing the quality of government services and reducing the cost of government services. In such a situation organisations, including government organisations, use communication networks to exchange data to work with their business partners and clients (Ihmouda et al., 2015). Where there is data exchange through a network, security problems invariably surface.

Another phenomenon observed is that while governments want to achieve efficiency and effectiveness in their administrative and business processes as well as e-Government operations, they have to keep abreast of the fast paced developments taking place in the e-Government sector and adopt latest developments and e-Government applications (Ojo et al., 2011; Schwester, 2009). In this process if e-Government implementation has to be successful, then users of e-Government services must be given confidence that they would realize fewer risks and more benefits (Srivastava and Teo, 2009). In addition continuous developments taking place in the field of e-Government enable governments to increase the number of services leading to the e-Government service provision reaching advanced stages. In such a situation security is considered the most important factor by researchers and it is argued that higher level of security is required as the number of services is increased (Ihmouda et al., 2014; Ihmouda and Alwi, 2013). Thus security aspects of e-Government services that have bearing on users gain currency.

Ensuring security while users transact through e-Government, an important expectation of users, is considered a major challenge to providing successful, efficient and transparent e-Government services (Al-Shafi and Weerakkody, 2010). This argument leads to an important inference that the fundamental essence of e-Government value is the necessity for governments to focus on its citizens (Shareef et al., 2011). However current literature on online security, including e-

Government security, although showing it as a critical user factor by many researchers Berthon et al., 2008; Chang and Chen, 2008, 2009; Peikari, 2010c; Peterson et al., 2007), much less research appears to have been conducted on factors that determine online security or antecedents of online security viewed from the social science and management perspective that is a subjective perspective (Shah et al., 2014). Current literature shows that much of the research efforts have gone to address aspects concerning computer science and engineering, which are objective in nature thus ignoring user perspective or user centricity (Shah et al., 2014). Although user centricity can be described in a number of ways, the one that provides a parsimonious definition is the one given by van Velsen et al. (2009) who say that user centred approach should comply with the needs and wishes of citizens or users of e-Government within a context. At a minimum, it is necessary that any e-Government service and all aspects that concern e-Government satisfy this definition. Further to the brief discussion on e-Government and e-Government security, the next section discusses the current status of the e-Government services, user centric e-Government security and unresolved problems of e-Government concerning citizen centric e-Government services security.

1.1 Current Status of E-Government

E-Government is rapidly growing. New developments in and applications of e-Government are regularly appearing. Many governments are embracing and adopting latest developments in e-Government. For instance modern day e-Government portals are utilizing social media network as part of their service provision e.g. e-Government portal of Government of Sweden (see Figure 1.1).

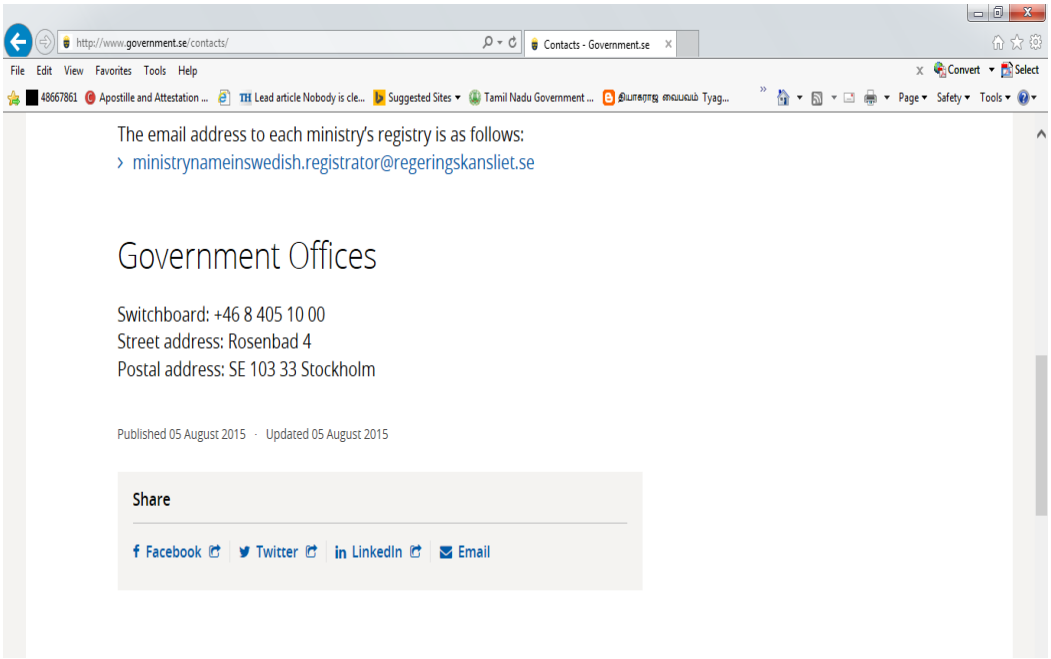

Figure 1.1: E-Government Portal of Government of Sweden, Showing Social Media Networking (http://www.government.se/contacts/)

More and more services are brought under e-Government (Figure 1.2).

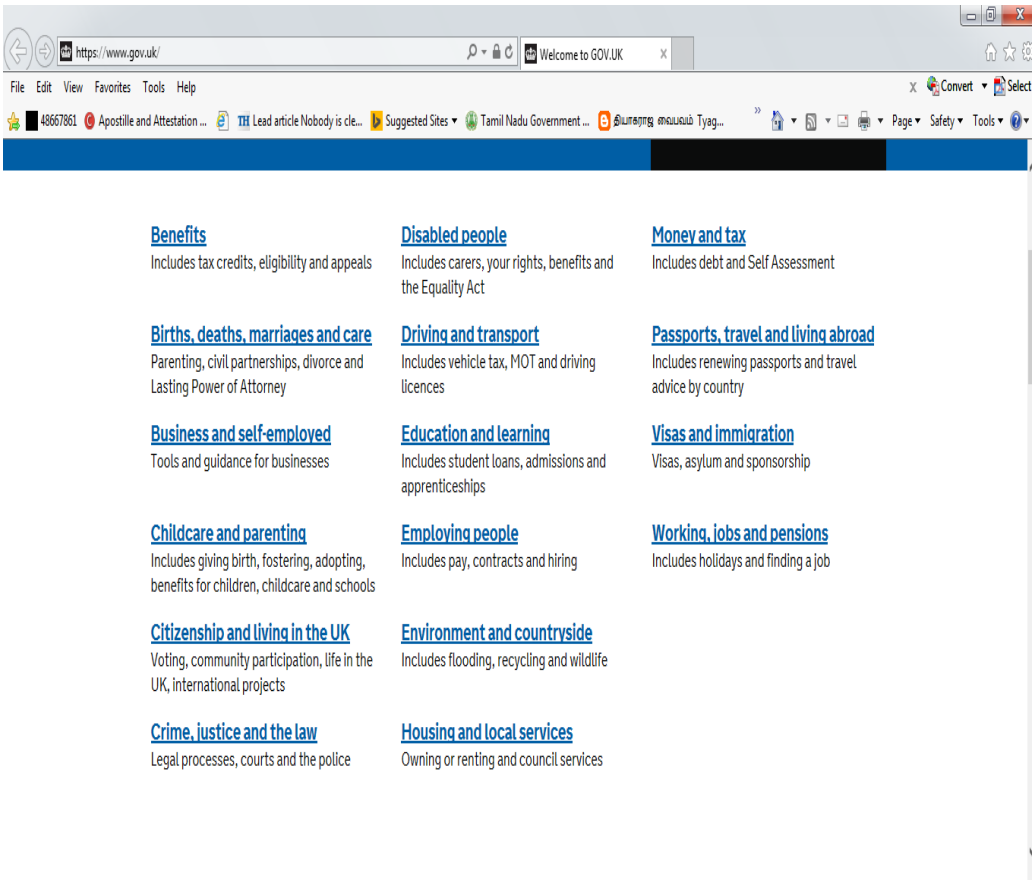

Figure 1.2: E-Government Portal of the Government of UK Showing Multiple Services Offered

E-Government is able to make available many different services to the users at their doorsteps. For instance birth certificates, driving licenses, passports and visas can now be obtained through e-Government services from wherever the user is and is able to access the e-Government portal (see Figure 1.2). Modern gadgets like tablets, smart phones, notebook, touch screen devices and personal digital assistants (PDAs) are changing the way people access e-Government services (Nosrati et al. 2012). Similarly new technologies like cloud computing, Bluetooth, Wi-fi, 4G technology and 5 G technologies and RFID (radio frequency identification device) have made inroads into the users of e-Government services (Brown, 2015). Today, e-Government services are available at the touch of a button or an icon on a touch screen device. Despite such progress made in the e-Government services across the world, still a number of challenges exist and the number of people adopting e-Government is not increasing. According to one report only 42% of the EU population used online public services in 2011, a reduction from a growth of 21-71%

achieved between 2000 and 2009 (Gonçalves, 2013). Problems exist. Chief amongst them is the e-Government security that is user centric (Shah et al., 2014). Thus there is a need to know what afflicts user centric e-Government services security discussions about which are given in Sections 1.2 that follow. In the meanwhile the next section discusses the e-Government context in Bahrain where the research was conducted.

1.2 E-Government in Bahrain

One of the most advanced e-Government services are provided in the Kingdom of Bahrain evidenced by its high rank in the UN survey provided in Table 1.1. The Table 1.1 indicates the World e-Government leaders (Very High EGDI) in 2014. The table shows that Bahrain has climbed 18 ranks from 36 in 2012 to 18 in 2014 and has been found ahead of countries like Germany.

Country	*Region*	*2014 EGDI*	*2014 Rank*	*2012 Rank*	*Change in Rank (2012–2014)*
Republic of Korea	Asia	0.9462	1	1	-
Australia	Oceania	0.9103	2	12	↑ 10
Singapore	Asia	0.9076	3	10	↑ 7
France	Europe	0.8938	4	6	↑ 2
Netherlands	Europe	0.8897	5	2	↓ 3
Japan	Asia	0.8874	6	18	↑ 12
United States of America	Americas	0.8748	7	5	↓ 2
United Kingdom	Europe	0.8695	8	3	↓ 5
New Zealand	Oceania	0.8644	9	13	↑ 4
Finland	Europe	0.8449	10	9	↓ 1
Canada	Americas	0.8418	11	11	-
Spain	Europe	0.8410	12	23	↑ 11
Norway	Europe	0.8357	13	8	↓ 5
Sweden	Europe	0.8225	14	7	↓ 7
Estonia	Europe	0.8180	15	20	↑ 5
Denmark	Europe	0.8162	16	4	↓ 12
Israel	Asia	0.8162	17	16	↓ 1
Bahrain	Asia	0.8089	18	36	↑ 18
Iceland	Europe	0.7970	19	22	↑ 3
Austria	Europe	0.7912	20	21	↑ 1
Germany	Europe	0.7864	21	17	↓ 4
Ireland	Europe	0.7810	22	34	↑ 12
Italy	Europe	0.7593	23	32	↑ 9
Luxembourg	Europe	0.7591	24	19	↓ 5
Belgium	Europe	0.7564	25	24	↓ 1
Very High EGDI Average		0.8368			
World Average		0.4712			

Table 1.1: World E-Government Leaders (Very High EGDI) in 2014

Although a developing nation, Bahrain boasts of a cosmopolitan culture. With a population of 1.2 million (approximately) the country consists of one of the most well educated populations in the region. Most of the services in the country have been brought under e-Government. A screenshot of Bahrain government's e-Government portal is provided in Figure 1.3. Figure

shows that many different government services have been integrated into the e-Government services as one stop shop in Bahrain and the figure shows that a security system in place (e.g. McAfee security services applied to the portal). This security is a technology based security and users usually do not understand what it is and what the implications are with and without the presence of those security systems.

Figure 1.3: E-Government Portal of Government of Bahrain (e-Government, 2015)

Another important point is that e-Government service providers in Bahrain seem to update their technology in line with the updates taking place in the information technology or computer science or engineering fields. For instance even though other advanced nations have hesitated at the introduction of cloud computing into e-Government services, Bahrain had introduced cloud computing as early as 2012, that is almost since the cloud computing was brought out by technologists for use by anyone. Thus e-Government service providers in Bahrain are at the forefront of introducing technological advances even when sometimes not much of their implications have been fully investigated, most importantly security issues. Bahrain context

therefore provided the most suitable context for conducting this research whose focus is user centric e-Government security, when technology changes. Needless to say the context also throws up other problems that are usually associated with user security for instance user trust and user felt risk. Hence the phenomenon of user centric e-Government services security required deeper study in the Bahrain context as it had the potential to bring out knowledge on how change in technology introduced in e-Government services in the context of cloud computing affected user centric security and how it can be managed. Such an effort was not found in the literature. There was a problem which is outlined next.

1.3 Problems in E-Government Services Security

Factors concerning users of e-Government are not well addressed in the e-Government literature, especially e-Government service security, when approached from the social science and management perspective (Shah et al., 2014). Even from the practical point of you e-Government portals do not seem to be concerned on informing users of the security aspects or educating them to be aware of security breaches. This is a major factor contributing to mismanagement of e-Government services. Lack of knowledge about user centric factors can affect the success of e-Government service providing agencies and users which includes e-Government service security (Shareef et al., 2011). Literature clearly shows that users are very concerned about security when e-Government technologies are implemented (Ihmouda et al., 2015; Jarvenpaa et al., 2000). Many researchers have asserted that e-Government security is a critical factor (Berthon et al., 2008; Chang and Chen, 2008, 2009; Peikari, 2010c; Peterson et al., 2007). While investigations into the e-Government services security have been conducted using computer science and engineering concepts, hardly any investigation has been conducted to address this issue as a factor concerning social science and management disciplines leaving a major gap in the literature (Shah et al., 2014). Lack of knowledge of how e-Government security affects government agencies and users and what user centric factors determine user centric e-Government security has the potential to affect the success of e-Government services. While literature points out that a number of factors can affect e-Government security, for instance contextual, technological, environmental, behavioural, organisational, technology adoption and management factors, empirical studies that have tested the influence of these factors on e-Government security are far and few (Shah et al., 2014). There was a need to understand this phenomenon. Thus the problem that emerges is detailed out next.

1.4 Problem Statement

From the literature it can be seen that contextual factors, particularly technological factors, constantly change forcing e-Government service providers to modify and adjust their infrastructure to adapt to the changes taking place in the context with an aim to offer better

services to the users (Cruz et al. 2015; Castells and Cardoso, 2005). However when each innovation is introduced in e-Government services, a host of challenges surface and chief amongst them is the user centric e-Government service security (AlKalbani et al., 2015). Other challenges that appear when new technologies are introduced in e-Government include distrust of users (Abu-Shanab and Al-Azzam, 2012), presence of risk factors associated with the new technologies, problems arising out of privacy issues (Lim et al., 2015), quality issues (Shanshan, 2014), human computer interaction issues (Gulliksen, 2014), perception of lack of ease of use of the technology, perception of lack of usefulness of the technology (Ayyash et al., 2013), cultural issues (Abunadi et al., 2008) and similar other issues. Such issues have the potential to impact the use of e-Government services by users resulting in reduced use of e-Government services, a problem that has been highlighted as highly concerning the service providers and others in the literature (Shah et al.,2014). Another important aspect that is of utmost concern to the users is the lack of research outcomes that have addressed user centricity in the field of e-Government (Elsheikh and Azzeh, 2014). A major lacuna in the literature is that much of the efforts within the research community has been focused on the technological issues concerning e-Government security rather than user centricity, a phenomenon that could be observed even with the service providers (Shah et al., 2014). Thus two important points emerge. One is the problem of technological changes that occur in the field of e-Government and the consequent security concerns it causes to the users and the second is the lack of user-centric approaches that are used to tackle those concerns. While there is an urgent need to address these points, it can be argued that till such time user-centric approaches are not the focus, it will be highly improbable that users will feel secure while using e-Government services and be motivated to transact through the e-Government portal. In order to overcome these problems the following research questions are set which need to be answered.

1.5 Research Questions

RQ1: What are the factors that can be considered as user-centric and affect e-Government services security?

RQ2: How those factors affect e-Government services security when there is a change in technology?

In order to address these research questions, the following aim was set.

1.6 Aim of the Research

The aim of the research is to examine how changing technology as a contextual factor is related to user centric e-Government security. Achieving this aim is expected to answer the research questions mentioned above. In order to achieve this aim following objectives are set.

1.7 Objectives

- To study the various factors concerning users in the field of e-Government in an environment characterized by changing technology.
- To elicit specific user-centric factors that could be related to e-Government security with the support of theories or models.
- To conceive a model using the factors elicited above that could relate those factors based on theories, concepts and models found in the extant literature.
- To derive findings by testing the model and achieve the aim set.

At this point it must be noted that in this research certain terms have been interchangeably used. For instance users and citizens imply users of e-Government services. Similarly e-Government security and e-Government services security have been synonymously used. Again terms user concern and user centric are used interchangeably. Trust signified user trust in e-Government services while risk signified user felt risk while using e-Government services. Technology implied any technology that affected or introduced or employed or used by e-Government service providers.

1.8 Significance of Study

The main significance of this study is that it was able to examine the concept of user centric e-Government services security and its relationship to various antecedents, mainly user trust, user felt risk and changing technology, with technology acting as the determinant, user trust and user felt risk acting as mediators of the relationship between technology and user centric e-Government services security. Such an examination revealed the need to manage effectively the new technology in a way user centric e-Government security is fully taken care of by taking into account user behavioural aspects such as effect of user trust and user felt risk with regard to e-Government security. The examination also involved how certain moderators affected the relationship between technology and user centric e-Government services security and included human computer interaction (HCI), user privacy and web design quality in the study. Moderators were found to be essential components whose presence affected the relationship between technology and user centric e-Government services security. Hence managing the moderators was shown to be imperative. Apart from these, the study tested the demographic factors' influence on the relationship between trust and user centric e-Government services security mediated by user felt risk. The examination showed that contextual factors affect the relationship. Again this aspect needs to be taken into account while managing the user centric e-Government services security. Finally this research significant as it has actually tested user perceptions of the change in the e-Government service technology by testing the influence of perceived ease of use and usefulness on the relationship between trust and user centric e-

Government services security mediated by user felt risk. This revealed that any empirical test that produces a conceptual model could be tested for its practical significance through this method adopted in this research where a second model was developed to test the practicality of the conceptual model. To achieve the above, this research has used appropriate concepts, theories, models and scientific outcomes as support thus expanding the application of those concepts, theories, models and scientific outcomes to address the research questions. Thus this research has significantly contributed to knowledge, theory, methodology and practice.

1.9 Thesis Structure

The thesis has been organized as follows:

Chapter 2 has delved into the literature and critically reviewed the different concepts that have bearing on the user centric factors including e-Government services security. User centric factors were identified and discussed. The chapter elicited the gap in the literature. Theoretical limitations to the concepts have been addressed and a section on the synthesis of various theories that apply to this research has been provided.

Chapter 3 provides the theoretical framework developed for this research that was used to answer the research questions. Hypotheses have been formulated to understand the meaningfulness of the relationship to this research. The chapter deals with the various relationships that need to be brought in using the user centric factors, to develop a conceptual model needed to answer the research questions and achievement of aims and objectives set for this research.

Chapter 4 provided the details regarding the methodology used in this research that provided the procedure to test the conceptual model and hence answer the research questions.

Chapter 5 dwelt on the data analysis using rigourous statistical methods that yielded the findings of this research including the verification of the hypotheses.

Chapter 6 discussed the findings and enabled the researcher to answer the research questions.

Chapter 7 concluded the research and discussed about the achievement of the aim and objectives set for this research, contributions to knowledge, theory, methodology and practice, limitations of research and recommendations for future research.

1.10 Summary

This chapter has provided an introduction to the current status of the e-Government literature and aspects concerning e-Government security. Problems affecting e-Government have been brought out. Research questions have been framed. Aim and objectives have been set. Significance of study has been explained and the thesis structure has been outlined. Thus this chapter takes the researcher to the next step of reviewing the e-Government literature.

Chapter 2: Literature Review

2.1 Introduction

E-Government has become more a necessity than an one off invention. In today's world most countries have implemented e-government technology and are able to provide many services to their citizens through online facilities. Alongside the implementation, technology is advancing rapidly necessitating both service provider and users to catch up with the advancing technology. This situation has led both service providers and citizens to understand and learn new aspects concerning both the technology and the e-government services. Often times this has led to problems of trust, risk, security and acceptance of the technology. In many contexts the technology introduced is virtual and not tangible to the users, for instance cloud computing, which has complicated the situation for the users and both researchers and service providers are struggling to crate user-centric facilities that are user friendly and trust worthy. Many factors have been identified for enhancement by the researchers involved in e-government research. However continuous advances made in the technological sphere has resulted in constant need to understand how the technology affects the users, in particular the security aspects. There is a need to identify those factors affected by technological change and also responsible for user felt security. In order to understand this complex situation, this chapter reviews the literature with a focus on technological change and user centric e-government security. The chapter has the following sections. This chapter starts by providing discussion about context of e-Government security, follows by context of e-Government. The researcher then discusses the various contextual factors affecting e-Government like demography, technology and nationality, then discusses about antecedents of e-Government security that affect users, follows by factors affecting the relationship between technology and e-Government security, ending with gaps in the literature and chapter summary. The structure of literature review chapter is outlined in Figure 2.1.

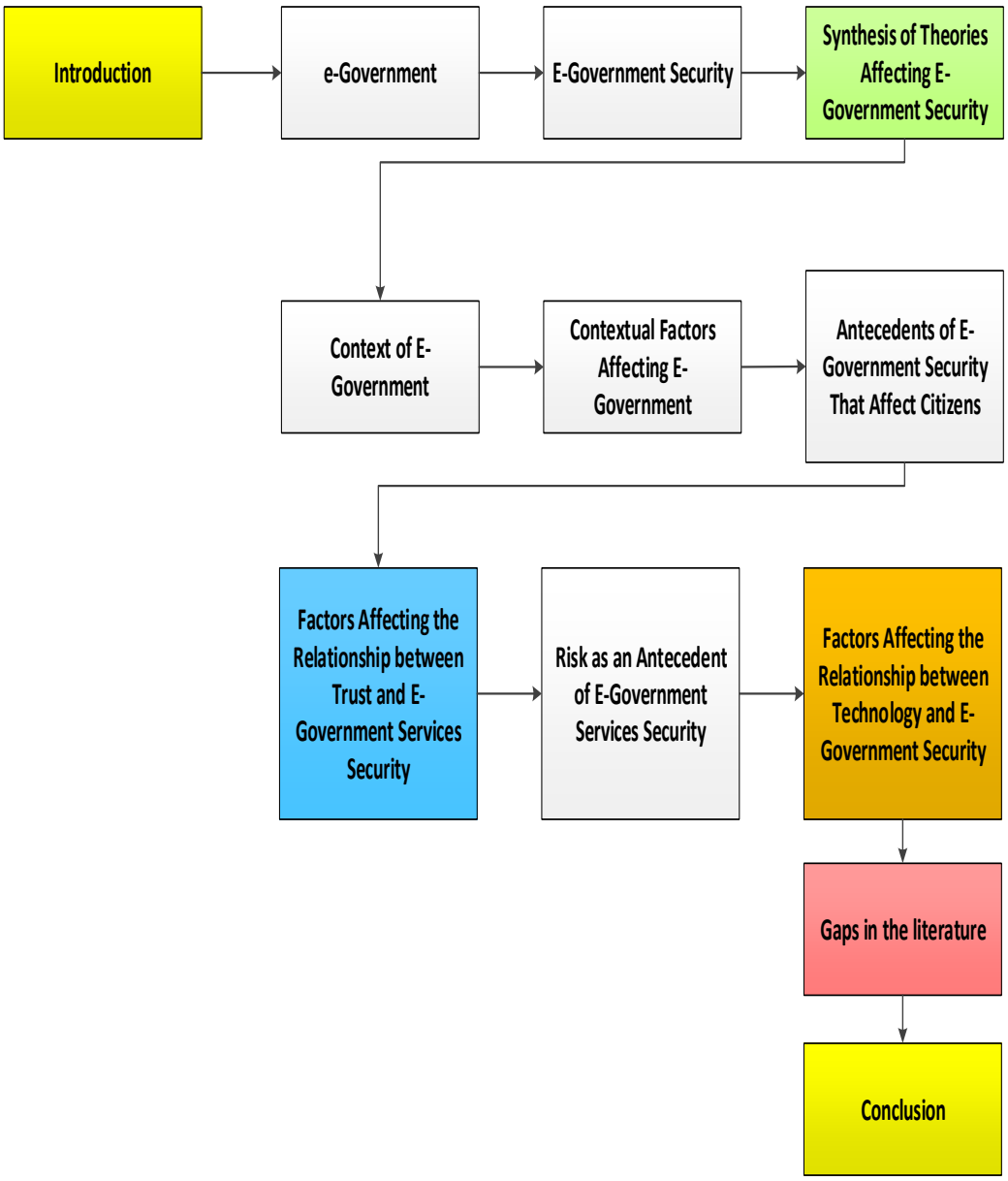

Figure 2.1: Literature Review Structure

2.2 E-Government

In the modern world, computer applications have found their way in every aspect of governance, business and individual use. Amongst many reasons that have driven the computer, applications to be adopted in government are the effectiveness and efficiency that could be engrained in government organizations (Brown and Thompson, 2011). Internet is one of the foremost computer applications that have revolutionized the world of governance because of its effectiveness and the efficiency. The need for using an effective and efficient computer application was that of the organizations' because of the primary concern of the organizations to provide improved services (Vassilakis et al., 2007). As a result of such a concern, organizations have set priorities and expectations to customize their services to fit into needs of their clients (Wei and Zhao, 2005). E-Government is a step in that direction by which governments aspire to provide transparent and people oriented services (Ong and Wang, 2009). Yet due to the fact that online services are not complying fully with clients' needs, there is a need to identify gaps in the provisioning of e-Government services (Wei and Zhao, 2005) so that reasons for non-compliance could be found and rectified. A study by West (2006) provides an idea about percentage of governments offering online services (Appendix A, Table A1) across different regions of the world, which indicates the steady increase in the implementation of e-Government services across the world.

Literature shows that definitions of e-Government vary, for instance Nawafleh et al. (2012) who explain that e-Government is a concept that is dependent on internet technology using which the government can play an important role in enabling the citizens, businesses and others in the private and public sectors to be efficient and effective. Abu-Shanab and Al-Azzam (2012) define e-Government as the delivery of information and services to its clients who are businesses and citizens through internet and information and communication technologies (ICTs). Kayrouz and Atala (2014) explain that e-Government is a phenomenon using which government organization's connect with people and aim to provide better services applying efficiently a wide range of different technologies. In yet another definition Al-Jamal and Abu-Shanab (2015) contend that it is a concept that uses and applies ICT tools in the processes of providing information and delivering government services to the users including citizens, businesses and other communities seeking government services in a more efficient, effective and improved manner but with the privacy of the information of the users of those services fully protected. As is common in many fields there are differences in the way e-Government has been visualized by researchers and no single definition seems to fit all contexts although there are common factors found in those definition that could be used in many contexts. Thus one

important common factor that could found in the different definitions is the use of internet and ICT in the delivery of government services using e-Government.

There are a number of advantages of using e-Government which include (Lee et al., 2011; Evans and Yen, 2006);

- Saving costs
- Ease of use
- Ease of usefulness
- Enhancement in the level of customer service
- Enable decision making by publishing compiled information
- Establish centralized decision making to ensure better efficiency
- Eliminate cost redundancies

However, the facilities that are needed to support provisioning of e-Government services is not growing in equal proportion leading to problems that are faced by end users. For instance a study by West (2006) in 2006 showed that only 29 percent of the government websites around the world offered fully executable services online with 14% offering just one service, 5% offering two services, 10% offering three or more services. This data shows that end users are unlikely to have the satisfaction of a full-fledged e-Government service and such a situation is likely to have inconsistencies. For instance, where e-Government is provided through a single point access, multiple online services are required to be made available to the users which if not made available users may have to resort to both manual and online services enabling possible errors to creep in due to manual intervention or the use of two different systems, one manual and the other electronic.

Furthermore, many challenges in implementing e-Government are seen to affect the users (Haider et al., 2016). For instance lack of appropriate ICT infrastructure, issues concerning security, privacy, cultural barriers, political willingness, issues related to design of e-Government portals, organisational issues, legal problems, overall environmental issues and issues at the government level have been identified as challenges in the literature (e.g. Alshehri and Drew, 2010; Helbig et al., 2009). In another instance a report published by US (General Accounting Office, 2001) has identified important challenges which include sustained and committed leadership, keeping citizen focus at all times, secure personal privacy, establish and operationalize necessary security controls, maintaining electronic records, ensure maintenance of a strong and reliable technical infrastructure, maintain uniform public service and ensure concerns related to IT human capital. Others have identified the need to build citizen centric e-

Government services, greater accessibility of government services, better usage of information and social inclusion as challenges (Burn and Robins, 2003). These aspects need to be addressed while implementing the e-Government operation especially due to the risks that could be introduced while transacting through the e-Government portal. These arguments imply that citizen centric aspects are considered important challenges by researchers and need specific attention because e-Government services are aimed at improving the government services provided to the citizens (Alshehri et al., 2012; Burn and Robins, 2003; General Accounting Office, 2001). Specific attention to citizen centric aspects may need to focus on factors that are not fully addressed. Those factors may need to include the ones that affect the e-Government services security needs of citizens as well. It is imperative that those factors are examined to identify the gaps that may exist in the literature and find ways to ensure delivery of secure and satisfactory e-Government services to the citizens (e.g. IBM, 2015; Duffany, 2012; Gharehchopogh and Hashemi, 2012; Curran et al., 2011; Wyld, 2010; Shareef et al., 2009; Heeks, 2003). Knowledge about these factors is expected to set the basis for understanding the security compliance issues related to the e-Government service vis-a-vis the citizens' needs an aspect that has attracted attention of researchers (Shah et al., 2014). However Shah et al. (2014) argue that the nature of online security perceived by citizens could be either subjective or objective. Shah et al. (2014) assert "although the antecedents of online security have been studied by the scholars in the field of computer science and engineering, their approach is from the technical and engineering perspective and not from the social science and management, which refer to security from the subjective perspective. Studying the antecedents of online security from the subjective perspective is important because the antecedents of security are different in subjective and objective perspective and the findings of each approach cannot be applied to the approach". Shah et al. (2014) further argue that outcomes produced by current investigations on a user's idea of security perception of online transactions focusing on the subjective side of online security have limitations with respect to their insight into the factors affecting perceived online security. The concept of online security perception of users is clearly not well investigated from the subjective perspective that concerns the management discipline. Knowledge on how the various factors that affect online security perception of individuals are related to online security as well as amongst themselves is limited and lack of such knowledge could seriously hamper the effective management of the provision of e-Government services. Thus there is a need to understand more about the online security perception of users including the online perception of e-Government and the factors that affect the online security perception of users, in other words, the user centric e-Government services security perception of users. The following sections discuss these aspects. In this literature review the word customer, citizen, or client are used synonymously.

2.3 E-Government Security

E-Government security is a major area of concern for users, service providers and researchers alike. e-Government security has been considered as a challenge in the e-Government literature by many (Lim et al., 2015; Alshehri et al., 2012; Irvine, 2000; Milner, 2000; Joshi et al., 2001; Holden et al., 2003; Luna-Reyes and Gil-Garcia, 2003; Roy, 2003). E-Government security as a user centric challenge appears to be an area that seems to have significant impact on the confidence of users in e-Government and is considered to be a cause of reduction in the number of users of e-Governments who trust the e-Government services (Hashim et al., 2015). While literature shows that many researchers (e.g. European Commission, 2013; Ayyash et al., 2013) have attempted to find out the factors that contribute to this loss of faith in the users arising out of e-Government security, the list of those factors does not seem to have covered or taken into account all the factors that contribute to the phenomenon of drop out of users of e-Government due to e-Government security issue. In addition contextual issues including changing technology, geography, demography and culture have been found to affect the users of e-Government by researchers with regard to some issues for instance adoption of e-Government as well as security and privacy concerns (Žilinskas and Gaulė, 2013). Although a number of researchers (e.g. Hasan, 2015, Omotayo and Adebayo, 2015; Alraja et al., 2015) have produced outcomes taking into account changing circumstances or contexts such as changing technology, demographic scenarios, change in user ability to use technology and change in social contexts like culture, those outcomes do not seem to be generalizable or consistent for application in different places in the world. Thus there is a need to know how user centric challenges pertaining to the e-Government could affect users of e-Government and could be successfully tackled for the benefit of users (European Commission, 2013).

Amongst the various challenges that have been related to contextual factors, the challenge pertaining to the e-Government security concerns of users has been identified by many researchers as a core issue and barrier perceived by citizens transacting through e-Government, that needs to be tackled (Alshehri et al., 2012). For instance West (2001) who argued that e-Government is unlikely to grow amongst citizens if security and privacy concerns of users are not addressed. This argument is confirmed by a study by Botterman et al. (2010) which shows that the trust in citizens with regard to e-Government is low because of worries of privacy and security. E-Government security concerns of users therefore attracts attention. In fact user centric e-Government security has been related to a number of factors by researchers in the past

but the attention given by researchers to the study of user centric e-Government security as a major dependent variable that affects secure transactions of e-Government users under multiple contexts appears to be very limited. Much of the work found in the literature has dealt with security from the perspective of technology and engineering (e.g. Shah et al., 2014) or as a factor that affects other variables for instance user adoption (Alrashedi et al., 2015) or a minor aspect of a larger variable for instance trustworthiness (e.g. Ranaweera, 2016). Seldom one comes across research efforts that have given prime of attention to user centric e-Government service security that it requires as a major concern of users and service providers. Besides, it seen that study of antecedents of user centric e-security in the field of e-Government is a neglected area although there are some examples of research conducted in the context of e-commerce (e.g. Shah et al., 2014). Research studies have at best treated user centric e-Government security either as a single item used to measure a construct for instance to measure trust in technology (Colesca, 2009) or part of a set of independent variables that are used to study other issues, for instance adoption of e-Government (e.g. Shareef et al., 2011) although without exception every research paper produced in the past argues that e-Government security viewed from user perspective is an essential aspect that cannot be ignored.

Furthermore, arguments in the literature point out that security features are one of the important factors that act as determinants of website success (Greunen et al., 2010), online satisfaction (Chang and Chen, 2009; Lee and Lin, 2005; Ribbink et al., 2004) and individual's online trust (Kim at al., 2010) an argument that could resonate in the context of e-Government portals. With governments across the world keen to involve citizens to participate in governance, e-Government as a tool is proving to be major area focus of governments (Botterman, et al., 2009). E-Government efforts are aiming to deliver personalized services to the citizens that satisfy their needs (Botterman, et al., 2009). More so when technological advances are slowly replacing older versions of the technology for instance the possibility that the letter "e" in e-Government by the letter "m" meaning m-government where "m" stands for mobile as mobile technology is sweeping across domains and is unleashing its power to change the world order with regard to electronic transactions. According to Dawes (2009) mobile government and multichannel service delivery by governments will be key contextual aspects that are expected to play an important role in satisfying user needs. On the one hand contextual factors are rapidly changing and on the other research is lagging behind in providing knowledge about how the different factors affect users whose trust levels are increasingly reducing in e-Government especially due to security concerns.

2.4 Synthesis of Theories Affecting E-Government Security

A number of theories have been applied to understand the security aspects pertaining to e-Government usage, online interaction aspects and internet aspects in the literature. Application of such theories can be classified under two aspects technological (and engineering) and managerial (Shah et al., 2014). The focus of this research is a combination of technology and management. However theoretical focus is less on technology and more on management aspects of e-Government as the research is dealing with e-Government services, a management aspect although technology is the basis because e-Government is based on internet technology. Specifically the focus of this research is users and their behavior.

One of the socio-technological theories well discussed in the literature is the MIS theory as part of which two other theories have been discussed. These two theories are Structuration theory and Actor-Network theory and are used in e-governance research (De, 2008). Structuration theory argues that observed social phenomena are not a result of one or the other but of both (Giddens, 1984) and is able to explain about issues related to use and management of information technology in organizations (De, 2008). Similarly Actor-Network theory is argued to be a theory that is addressing certain limitations of Structuration theory and is believed to give an explanation about what could be considered as technology. Both Structuration and Actor-Network theories deal with technology and human actors, and are considered duality theories. However both these theories have serious limitations and their application to situations that involve objective and material analysis is considered difficult (De, 2008).

With regard to managerial aspects a number of theories have been used by researchers to understand user behavior towards e-Government. Particularly theories and models that find place in the e-Government literature are those related to e-Government adoption, adoption compatibility variables, e-Government service quality (Shang, 2014), e-Government success factors, e-Government services security and management (Ziemba et al., 2015). The theories that have found application in those areas are grounded in technology adoption, public administration and organization, psychology, sociology, political science, culture, and marketing disciplines (Shareef et al., 2011).

One of the areas that has attracted wide attention in the e-Government research is the user acceptance of technology and a number of theories and models have been developed to explain the user behavior towards e-Government acceptance. These include:

- Roger's Diffusion of Innovation (DOI) (Rogers, 1995) and its derivatives. DOI deals with user perception of the characteristics of the technology with regard to the technology's influence on user behavior when information technology is delivered.

- Davis' Technology Acceptance Model (TAM) (Davis, 1989; Venkatesh and Davis, 2000) and its offshoots that explain the formation of user intention (personal beliefs and attitudes) to accept and adopt information systems. This model is one of the most widely used models although other theories and models that have addressed user adoption behaviour including Theory of Reasoned Action (TRA) (Fishbein and Ajzen, 1975) and Theory of Planed Behavior (TPB) (Ajzen, 1991) have also been used by researchers to understand the adoption and acceptance behavior.
- Variations of TAM that have been developed namely TAM2 (Venkatesh and Davis, 2000) and TAM3 (Venkatesh, 2000).
- Model developed by Taylor and Todd (1995a) that combines the principles of TAM and TPB.
- The Task-Technology Fit (TTF) model developed by Goodhue and Thompson (1995). According to this model task-technology fit is expected to affect the utilization of information system and the fit itself will be affected by task characteristics (TC) and technology characteristics (TNC).
- Unified Theory of Acceptance and Use of Technology (UTAUT) developed by Venkatesh et al. (2003). This was developed using a combination of eight models namely TRA, TAM, TPB, model developed by Taylor and Todd (1995a), TTF, DOI, the motivational model developed by Davis et al. (1992) and social cognitive theory (Compeau and Higgins, 1995). UTAUT is claimed to be the most comprehensive model that explains the variance in user intention to adopt and use a technology to a high percentage (Venkatesh et al., 2003; AlAwadhi and Morris, 2008; Colesca and Dobrica, 2008; and Loo et al., 2009).
- Socio-technical theory which argues that an organization is made up of a technical sub-system and social sub-system and there needs to be a fit between the two; and for systems to be successful technical, organizational, and social aspects of the system must be configured in parallel (Bostrom and Heinen, 1977). Literature shows that Socio-technical theory need to be used as extensions to acceptance models (e.g. TAM) to explain user behavior towards new technological innovations such as social network. Further Khan et al. (2010) argue that every aspect of e-Government including customer perspective of e-Government services and e-Government security could be understood using socio-technology theory although frameworks that have extended the application of socio-technical theory to e-Government services security by combining other models such as TAM are yet to be developed (Shipps, 2013). Thus in one way this theory could be used as an overarching theory to explain the behavior of users of e-Government.

- Human Computer Interaction (HCI): HCI in a way is not a theory as it is interdisciplinary and interrelates with a number of fields including psychology, computer science, cognitive psychology, engineering, artificial intelligence, ergonomics and recently other discipline are input as sociology, anthropology and art sciences (Fetaji et al., 2007). Definitions and models developed by researchers on HCI could themselves act as theories. Crucial to HCI design is the interrelation between psychology and computer science (Carroll and Thomas, 1982). Further, Iachello and Hong (2007) argue that in the design field HCI mostly deals information theory and information exchange. Information exchange is described using mathematics and has no reference to human user. Such a situation has forced the HCI community to focus on economic and behavioral models (Iachello and Hong, 2007).

  However in regard to e-Government adoption a notable omission that could be found in the literature is the lack of in-depth application of Human Computer Interaction (HCI) theory in research efforts that have investigated the human behavior in the field of e-Government. Although as early as 1987 Davis (1987) had predominantly used HCI theory in the original technology acceptance model (TAM) and brought out two important characteristics that influence technology acceptance namely perceived usefulness and perceived ease of use, research efforts that have used HCI theory in online research is only recent (Zhang et al., 2007; Corritore et al., 2003). The few research publications that are found in the literature grounding arguments in HCI and associated theories, have only addressed specific topics such as trust issues (Alsaghier et al., 2009), risk aspects (Featherman and Pavlou, 2003) and technology adoption issues in online transactions by users (Goswami, 2014), while there is hardly any research that has effectively used HCI theory alongside other theories with regard to e-Government issues and associated factors including user satisfaction as well as user recognition of systems (Keil et al., 1995; Legris et al., 2003; Venkatesh et al., 2000). There are growing calls by researchers to exploit HCI and related theories to understand the impact of MIS design features on the HCI of users (Axelsson and Melin, 2008; Zhang et al., 2007; Corritore et al., 2003).
- E-GovQual: e-GovQual (Papadomichelaki and Mentzas, 2012) is a derivative of the e-service quality concept postulated by Zeithaml et al. (2002). This idea was developed by Papadomichelaki and Mentzas (2012) which can be used to understand how users of e-Government service perceive and evaluate online services. A new concept needs empirical studies to assess and establish its reliability and validity.

The foregoing synthesis clearly points out that a number of theories could be used to understand how a host of factors operate and affect users of e-Government services and their belief in e-Government security. The factors addressed by those theories include contextual factors security, trust, privacy, quality of service provided by e-Government, perceived ease of use (Papadomichelaki and Mentzas, 2012), attitude toward technology, technological factors, perceived usefulness (Hashim et al., 2015), citizens centricity (Osman, 2013) and human computer interaction (Gulliksen, 2014). A notable argument found in the literature is that despite a plethora of papers being published on the various theories including those mentioned above and their usefulness in understanding the various behavioral, technological and organizational factors, still there are concerns voiced in the literature that changing technologies bring in new challenges that need to be explained as current theories may not address those challenges effectively (Al-Shafi and Weerakkody, 2008). For instance with the advent of new mobile applications, new facilities online and social media, there is a growing concern on whether existing theories could be applied to address user problems that arise out of changing technologies. Security, trust and privacy are some of the concerns of users that are frequently encountered when technology changes and even the most widely used model like TAM is found to be helpless in explaining some of the concepts applicable to acceptance of those technologies (Mathieson et al., 2001). The same argument could be applied to other theories and conceptualizations and their enhancements as every new situation unless explained by the existing theories and evidenced by empirical research, it is not possible to accept the reliability and validity of those theories. Each context and change in technology may require to be examined using existing theories to know how the change in context and technology affect users of e-Government. Thus this research aims to identify those theories that need to be applied to address the research gap existing in the literature with regard to user centric e-Government services security. Keeping the above arguments in view, this chapter embarks on critically reviewing the various factors that have not been either well addressed or not addressed in the literature as antecedents of e-Government security considered citizen centric and the usefulness of appropriate theories to address those factors. A critical review of the various concepts follows.

2.5 Context of E-Government

Electronic government (e-Government) is gaining significance steadily as an important tool to transform public governance. Many articles have been written over the years highlighting its potential in delivering services to the citizens. Initially the enthusiasm in E-Government was found to be very high in both the citizens and the service providers as a tool that can continuously transform public delivery system. A recent report of UN suggests that e-

Government has been adopted in as many as 193 countries (UNPAN, 2014) indicating the utility of e-Government as a tool for governance. Despite an overwhelming interest shown towards e-Government, some have argued that e-Government as a technological tool has not lived up to its potential (Teo et al., 2008). One statistic shows that in 2004 about 15% of all e-Government initiatives in the developing nations have only been successful (Heeks, 2004). Another recent survey of UN shows that majority of the 193 countries that have been surveyed in 2014 remain in the low and intermediate level of e-Government development (UN has identified a four stage model for evaluation, see Figure 2.2) (UNPAN, 2014).

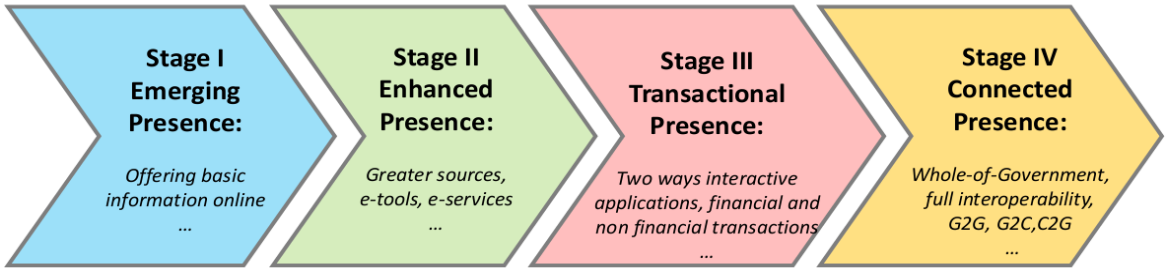

Figure 2.2: Four Stage Model of E-Government Online Service Index Developed by UN (UN, 2015)

Similar sentiments have been espoused by many authors who have cautioned about the declining trust of citizens in governments, in particular e-Governments due to privacy and security issues on the one hand and increased vulnerability of citizens to risks while transacting through e-Government portals on the other (Al-Adawi et al., 2005; Balasubramanian et al., 2003; Parent et al., 2005; Soat, 2003). The situation gets further aggravated when technological advances make transactions on e-Government portals prone to increased security threats. For instance, many countries (e.g. European Union countries) have recently thought of introducing cloud computing as a major technological innovation to make the e-Government operations efficient, effective and satisfactory (Tweneboah-Koduah et al., 2014) but had to be very careful about the prime vulnerability of users' information security risks and data privacy (Lim et al., 2015) although hardly any investigation has been conducted with secure transaction of users (e-Government security) as the determined factor and its antecedents. Use of cloud computing as technological factor has a major implication on security aspects concerning the user and in a context where e-Government service provider is using cloud computing investigations on user centric e-Government security has not been well investigated.

While there is no consensus amongst researchers on what can be considered as the most important factors that contribute to the achievement of the highest level of e-Government development (see Table 2.1) research shows that all factors contribute to the development.

No.	Factors Affecting e-Government	Authors
1.	Legislation and legal framework; human resistance to change, security and privacy issues; culture issues; trust in E-Government; usefulness and complexity issues; website design issues; access and IT skill issues; operational cost; organizational issues; technical infrastructure; usability, availability, and accessibility issues	Al -Shafi (2009); Majdalawi et al. (2015)
2.	Obstacle factors : infrastructure, political, economic, social, and legal and users' perspectives	Haider et al. (2016)
3.	National income, high-level political support and leadership, strengthened institutional capacity, public accountability and citizen engagement, as well as adequate e-Government programmes, ICT infrastructure and education.	UNPAN (2014)
4	Political factors, social factors, organizational factors, and technological factors	Weerakkody et al. 2011; Bonham et al. (2001)
	Demographic factor (gender, job, income, education, age, ethnicity, and frequency of Internet use)	Myeong et al. (2014)
5	Service (service support, efficiency), technology (infrastructure, data storage, security, alignment), employee readiness (ability, engagement), policy/management (budget, revenue, change management, decision making), social/economic responsibility (social, environment, economic), service performance (user take-up, user satisfaction)	Osman et al. (2013)
6	Online services, big data, social media, mobile apps, or cloud computing	UNPAN (2014)

Table 2.1: Factors Contributing To the Development of E-Government

But UN points out three major factors as contributing to the development of e-Government in all nations including those that are advanced in developing e-Government namely robust data protection, online payment systems, and secure data sharing across government institutions (UNPAN, 2014). One of the main reasons attributed by UN for this state of affairs is the continuous evolution of technology and technology is considered to be a major driver and critical enabler of e-Government development.

Further, contextually several technological innovations have significantly influenced the development of e-Government which include cloud computing, mobile technology, Internet, social media and space-based technologies such as Geographic Information Systems (GIS) (UNPAN, 2014). With continuous innovations taking place in the technology frontier, e-Government service providers are forced to continuously upgrade the technological aspects required to provide e-Government service. Up-gradations to technology usually bring with them changes in the way people could transact through the e-Government portal and the necessity to understand how they affect the users and what needs to be done. For instance one of the recent trends in the technology that has significantly changed the way people use services on the internet is the cloud computing. One report suggests that cloud computing could be likened to another industrial revolution (Alleweldt et al., 2012). Changes in technology form part of the context in e-Government research (Srivastava and Teo, 1998). Alongside change in technology come the challenges associated with the change that require investigation and to know how those challenges could be overcome. For instance in the context of an e-Government development that uses cloud computing, citizens are exposed to serious challenges related to information security while transacting business through the e-Government portal. Where users were conversant with using desktop personal computers, now people are able to use mobile devices to access e-Government services with applications provided by the service provider catering to needs of cloud computing. Thus users are introduced to new contextual factors including human computer interface, ease of use of the technology, usefulness, security, trust issues, risk, privacy issues and quality issues (Hashim et al., 2015; Alrashedi et al., 2015; Shah et al., 2014; Alateyah et al., 2013; Alshehri et al., 2012; Colesca, 2009; Al-Shafi and Weerakkody, 2010; AlAwadhi and Morris, 2009).

While a number of studies have been conducted in e-Government, such studies have not addressed emerging contextual issues related to e-Government such as technological factors; demographic and cultural aspects affected in a changing environment such as technology; and user centric security issues as a dependent variable in a changing environment. Thus contextual factors gain currency. With the advent of cloud computing there appears to be a new era of e-governance emerging and how this technology affects user centric contextual issues including demography, security, privacy, quality, trust, risk, human computer interface, ease of use, and usefulness is yet to be fully understood. For instance Facebook and Google maps are two excellent examples of cloud computing e-Government agencies are adopting through their services other than those dedicated cloud services such as online storage (IBM, 2015). Although cloud computing is still in its early stage of development, some countries including Kingdom of Bahrain have already started to take advantage of this technology (Tweneboah-Koduah et al., 2014; UNPAN, 2014). However not much is known about how contextual factors affect user

centric security in an e-Government environment that has implemented technological changes including introduction of cloud computing. Arguably user data security and privacy are two factors identified by researchers (e.g. IBM, 2015; Duffany, 2012; Gharehchopogh and Hashemi, 2012; Curran et al., 2011; Wyld, 2010) as having serious implications to citizens where technological changes including cloud computing have been introduced, especially when citizens consider security and privacy as barriers to transact on e-Government web portals. Lack of knowledge on how user data security and privacy are affected when they transact through the e-Government web portal characterized by changed contexts, could impact user trust on governments. There is a need for further investigation in this area. At this point it can be seen that the contextual aspects that influence e-Government users and their possible implications to user centric e-Government security have been critically reviewed. This sets the basis to review in greater detail some of the contextual aspects that have the potential to affect citizen centric data security issues pertaining to e-Government and its antecedents. While a critical review of the main contextual factors that affect citizen centric e-Government security follows next, the review of important antecedents that need to be considered alongside contextual factors follow later.

2.6 Contextual Factors Affecting E-Government

Overall focus of this research is the context of change affecting citizen centric e-Government security and falls under the business to consumer (B2C) context (Shah et al., 2014). Shah et al. (2014) conducted their study in the context of B2C with a focus on perceived security of websites of Malaysian consumers and justified the need to study in Malaysia in the context B2C relevant to e-commerce due to the following reasons which appear to be very similar to the e-Government context:

- Lack of studies in the developing nations' context as majority of the research is focused on the developed countries like USA (Alam and Yasin, 2010b).
- Adoption of e-commerce is considered to be in its early stages in developing nations leading to higher degree of security concerns in the minds of users (Alam and Yasin, 2010a; Hwang et al., 2006).
- Outcomes of research conducted using data collected in one nation differ with respect to another.

The above arguments clearly point out the need to conduct context based research. In addition that research outcomes and concepts pertaining to e-commerce can be extended to research in the context e-Government is an argument that finds agreement with many researchers (Bernhard, 2013; Alsaghier et al., 2009); Schneider, 2003; Fang, 2002) and hence it is

reasonable to argue that the concepts used and results reported in their study by Shah et al. (2014) can find application in any research pertaining to user centric e-Government security.

Furthermore, literature shows that changes triggered by technological, economical, political and social factors propel the attention of researchers to study those changes (Wischnevsky, 2004). Such triggers have the potential to disturb the established routines and stimulate the conscious thoughts of service providers of e-Government services and compel people's attention to be brought into the changes that occur due to those triggers (Isabella, 1992). It won't be an exaggeration to say that context of change and the kind of triggers of change stimulate the need to identify the overall components and results where the change is introduced. In fact offering justification to the need to gain an understanding of the nature of those triggers of change and finding out how the triggers mutually interact with organisational systems including e-Government systems can be vital to arriving at a complete picture about the change phenomena (Wischnevsky, 2004). Keeping this in view in this research certain important contextual issues that are purported to influence user centric e-Government security have been critically reviewed. While the list of contextual factors that have the potential to introduce change in organizations providing e-Government services is by no means small (see Table 2.2), covering all those factors in one research is near impossible task. Thus the contextual factors that were considered essential for an understanding of how change is brought in by those factors and influence the user centric e-Government security were demographic factors (experience, technology and culture), technological factors and human computer interface factors. The reasons for choosing those factors for investigation were:

1. Some argue (see Table 2.2) that in general the contextual factors vary from one country to another that affect e-Government.

Category	Components	Reference
Context	Social and organizational culture	Golipour & Pirannejhad (2009); Markellou et al (2009); Im & Seo (2005); Al-Saber (2007); Ciborra (2005); Davidrajuh (2004); Ho (2002); Cameron & Quinn (1999)
	Management maturity	Im & Seo (2005); Al-Saber (2007); Ciborra (2005); Davidrajuh (2004)
	Economic conditions	Lim (2003); Hughes (2002); Ho (2002); Im & Seo (2005); Al-Saber (2007); Ciborra (2005); Davidrajuh (2004)
	Electronic knowledge	Lim (2003); Hughes (2002); Carter & Belanger (2005); Im & Seo (2005); Al-Saber (2007); Ciborra (2005); Davidrajuh (2004)
	Demographic conditions	Ho (2002); Im & Seo (2005); Al-Saber (2007); Ciborra (2005); Davidrajuh (2004)
	Specialist human resources	Lim (2003); Hughes (2002); Bellamy (2000); Bozeman & Bretschneider (1986); Changalur & Duchessi (1999); Ho (2002)
	Technological infrastructures	Im & Seo (2005); Al-Saber (2007); Ciborra (2005); Davidrajuh (2004); Ho (2002); Ho (2002)

Table 2.2: Some of The Contextual Factors that are Found to Influence E-Government

(adopted from: Dehkordi et al., 2012)

It can be seen that the most common contextual factors identified by researchers in the field of e-Government is technology, demographic conditions and electronic knowledge (implies human computer interface in terms of the skill and ability of citizens working with electronic devices (Dehkordi et al., 2012).

2. Some argue context needs to be considered as the first category factor that must be used to realize e-Government and includes citizens' knowledge to use computers, demographic factors and technological aspects (Dehkordi et al., 2012).
3. Researchers (e.g. Al-Shafi and Weerakkody, 2009; Dwivedi and Irani, 2009; Carter and Weerakkody, 2008; Irani et al., 2008; Al-Shafi and Weerakkody, 2008; Carter and Bélanger, 2005; Thomas and Streib, 2003) believe that challenges that arise while e-Government is implemented in different nations are not the same and hence have attempted to provide insights into those challenges through research in different national contexts. Included in those challenges are technological factors, demographic factors and knowledge of citizens to use e-Government services (Al-Shafi and Weerakkody, 2009) without addressing which citizens may find it difficult to adopt e-Government.

Thus it is reasonable to infer that the three contextual factors can play an important role in understanding not only the implementation of e-Government by service providers' and citizens' intention to adopt e-Government but also the user centric e-Government security and secure transactions as user centric e-Government security and secure transaction are considered essential to any e-Government infrastructure. A critical review of each one of these factors follows.

2.6.1 Demographic Factors

Some of the demographic factors commonly examined in different contexts by researchers in the context of e-Government include age, gender, education, income, year of internet experience, employment status, knowledge of internet and use of social media (Alrashedi et al., 2015; Alateyah et al., 2013; Alshehri et al., 2012; Colesca, 2009). Demographic characteristic vary across nations. Researchers (e.g. Alrashedi et al. 2015; Alateyah et al., 2013; Alshehri et al., 2012; Colesca, 2009; Dwivedi and Lal, 2007; Choudrie and Papazafeiropoulou, 2006; Fu et al. 2006; Choudrie and Lee, 2004); Venkatesh et al., 2000; Burgess, 1986) have investigated the effects of demographic characteristic on many issues pertaining to e-Government as well as online factors that affect citizens. Studies have examined the influence of demography on user behavior towards e-Government under different contexts, for instance Al-Shafi and Weerakkody (2009) who investigated the influence of education level, gender and age on e-

Government use behavior of citizens of Qatar whereas Fu et al. (2006) examined the influence of demographic factors (age, gender, education, prior experience in using computers and internet and accessibility of Taiwanese taxpayers with regard to acceptance of e-Government initiatives in Taiwan. Similar examples of other researchers examining the influence of demographic factors on user or consumer or citizen behavior could be found in the extant literature. This clearly indicates that demographic factors affect user perception or behavior with regard to e-Government initiatives although variations in user behavior towards e-Government due to demographic factors are not generalizable across nations. For instance Alrashedi et al. (2015) did not find demographic factors education, income, and employment status of citizens of Saudi Arabia influencing e-participation. Thus it is meaningful to argue that demographic factors across nations vary and may or may not influence user behavior towards e-Government initiatives.

The above arguments imply that if any inference has to be drawn about the general impact of demographic factors on user behavior towards e-Government initiatives across the globe, it is necessary to study how different demographic factors affect citizens of a country in each national context so that it is possible to gain knowledge on how each of the factors affect the users towards e-Government initiatives. In addition, discussions above show that there is no consensus amongst researchers about the choice of any particular demographic factor or set of factors that must be investigated in any particular national context and there is no standardization on determining what demographic factors should be necessarily studied with regard to e-Government initiatives. However most researchers who have been cited above have chosen certain demographic factors for study in common which include age, income, internet experience, knowledge or awareness of internet or online usage, gender and employment related aspects. However hardly any study has considered nationality (considered as representing the concept of culture (Stoddard and Leibbrandt, 2014) as a demographic factor that affects user behavior towards e-Government initiatives, in particular user centric e-Government security or secure transaction through e-Government portals. In addition, literature shows that demographic factors have been identified varyingly as a determining or control or moderating factor of user behavior towards e-Government. For instance Al-Shafi and Weerakkody (2009) studied the influence of demographic factors on e-Government adoption in the context of Qatar as moderating factors while Alraja et al. (2015) examined the influence of demographic factors as control variables in the context of Oman and Fu et al. (2004) examined demographic factors as predictors of e-Government initiative in Taiwan. However majority of studies do not seem to investigate demographic factors as predictors and have either reported the effect of demographic factors on e-Government transactions conducted by users, through a description of those factors or as moderators with a few choosing to use them as control variables. Seldom one comes

across studies that have considered demographic factors as predictors of user behavior with regard to e-Government initiatives. Thus it is reasonable to conclude that demographic factors in general could be used in studies as control variables or moderators when the investigations are focusing on knowing how those factors impact e-Government security.

While addressing of issue of linking demographic factors to e-Government usage, it is seen from the extant literature researchers have used different ways, for instance, using the Unified Theory of acceptance and use of technology (UTAUT) model, Hashim et al. (2015) explained how demographic factors gender, age, experience and voluntariness moderate the relationship between user trust and user intention to adopt cloud computing services. Similar sentiments have been expressed by Alshehri et al. (2012) although in the context of e-Government. However researchers have attempted to use the demographic factors not only as moderators but also as others in different models as influencing on line transactions similar to e-Government (e.g. Mourao et al., 2015; Ibrahim and Pope, 2011; Ilias et al., 2009; Fu et al., 2006; Fu et al., 2004). For instance nationality as a factor representing cultural aspects of users has been argued to directly affect beliefs and trust of users in e-Government as a predictor (Abunadi et al., 2008). Thus while contradictions are seen in the way demographic factors are used in different models in the e-Government literature, at the same time it is also possible to infer that demographic factors can be conceptualized in multiple ways.

2.6.2 Technology

Technological aspects affect a number of user related factors and a number of theoretical propositions have been developed to explain how technology affects users although literature shows that there is no one theory that is sufficient to explain the various user behavioral aspects. For instance Davis (1989) postulated the TAM to explain why people accept or adopt new technologies in the context of information systems while Rogers (1995) attempted to explain how new technology diffuses and affects users. Many other theories have also been found in the literature details about some of which have been provided in Table (2.3).

No.	Theory/Model	Authors	What it explains
1.	Unified Theory of acceptance and use of technology (UTAUT)	Venkatesh et al. (2003)	Prediction of behavioral intention to use a technology and technology use primarily in organizational contexts (Venkatesh et al., 2012).
2.	Technology-organization-	Tornatzky and	Used to analyze adoption of

	environment (TOE)	Fleischer (1990)	technological innovations by firms and organizations (Melville and Ramirez, 2008)
3.	Theory of planned behavior (TPB)	Ajzen (1991)	Individuals make behavioral decisions based on careful consideration of available information (Conner and Armitage, 1998)

Table 2.3: Example of Adoption Model

While many of the aforementioned theories have been used by researchers to understand how technological innovations and inventions have been adopted and implemented by individuals and organizations, literature is silent on what theories could be applied to understand how user concern towards e-Government security issues are affected when any new technology is introduced. Although potentially many of the abovementioned theories could be used to understand how user concern towards e-Government security issues are affected when any new technology is introduced, by and large it can be seen that theories that explain user behavior including TAM, TRA, DOI and similar adoption theories have only been applied by researchers (see Hashim et al., 2015) to the context of e-Government. Seldom one sees the application of such theories as TOE or Human Computer Interaction (HCI) to understand concepts of e-Government including security concerns of users of e-Government although their potential to explain user behavior has been highlighted by some (e.g. Ahmad et al., 2015; Väätäjä, 2014).

That technological factors play a key role in successful adoption and acceptance by users of e-Government is widely acknowledged in the e-Government literature (Srivastava and Teo, 2005). For instance recent initiatives of introducing cloud computing in e-Government have been shown to be prone to security threats and some authors consider information security is a major issue where cloud computing is introduced in e-Government (Armbrust et al.,2010). The example of cloud computing, one of the recent developments in the field of IT, provides a basis to argue that it is reasonable to assume that technological advancements in IT such as cloud computing impact information security, an issue that must be of prime importance to all stakeholders associated with e-Government an argument that finds support from Armbrust et al. (2010). Thus technological factors can be construed to impact user perspective of e-Government security and every innovation or invention in IT when introduced in area like e-Government where user transactions are involved need scrutiny to gain knowledge on how they actually affect users, especially when user security issues are involved. In fact many researchers (Hashim et al., 2015; Myeong et al., 2014; Alrashedi et al., 2015) have called for investigations

into security issues with regard to e-Government whenever a new technological aspect is introduced, for instance introduction of cloud computing in e-Government. Further some argue that issues related to security and privacy can delay development of a technology due to purported lack of confidence in users and e-Government authorities (Fielder et al., 2012), aspects that become important in any investigation of e-Government. More importantly literature cautions that most studies that have investigated the influence of technology on e-Government have tended to focus on the technological aspects rather than examining the user needs pertaining to those technological factors (Alharbi and Kang, 2014; Persaud and Persaud, 2013). This implies that there is hardly any effort found amongst researchers involved in e-Government studies that have focused on the influence of technology on user needs an argument that could be extended to user needs of e-Government security.

While literature shows that technological innovations impact users, most often such literature focuses on certain factors that affect technology and those that get affected by technology. For instance Hashim et al. (2015) have argued that a number of user oriented factors have been identified in the extant literature as affecting users when technology changes (see Table 2.4). Table (2.4) shows that a set of user relevant factors that affect different users in an e-Government environment where the technology of cloud computing is deployed. Literature also shows that user trust, privacy and security are found to be the most commonly affected factors when new technology is introduced (Hashim et al., 2015).

Factor/ Area	Business	Education	IT professional	Users
Security and privacy	X	X	X	X
Relative advantage	X		X	
Compatibility	X		X	
Complexity	X		X	
Ease of use	X		X	
Risk		X		
Cost		X		
Performance expectancy		X		
Perceived usefulness			X	X
Availability				X

Table 2.4: Most Common Factors Affecting Different Users of E-Government Where Cloud Computing is Deployed (Adopted from Hashim et al., 2015)

Further to the above arguments, it is seen from literature that change in technology, innovations in technology and new technology have the potential to affect different users in different ways, for instance acceptance and adoption (Hashim et al., 2015) and hence technology becomes an important contextual factor that needs to be studied.

The foregoing arguments suggest that acceptance and adoption of technology itself gets affected by certain factors (e.g. ease of use and usefulness (Davis, 1989)) and technology affects users in terms of certain other factors including trust and security. In addition the foregoing discussions also point out that it is important to understand (a) how certain antecedents affect technology and therefore the users of such a technology in an e-Government environment as also (b) how technology affects some other factors that affect user behavior with regard to e-Government security, is worth investigating, an argument echoed in the literature (e.g. Shah et al., 2014).

A significant aspect of studying technology as a factor in the context of e-Government security is the maturity of a technology that comes into focus because emerging technologies are introduced into e-Government even before those technologies have matured, resulting in the possible use of incomplete technology and hence some risk (UNPAN, 2014). For instance, across the world introduction of cloud computing into e-Government is being contemplated although it is still considered to be in its early stage of development. Despite this apparent fact many leading countries have introduced cloud computing (UNPAN, 2014) and literature shows that cloud computing is prone to security problems. Such introduction of an evolving technology can have consequences for the users. Therefore it is essential to understand how users could react to the introduction of new technology in an e-Government environment using appropriate user behavior theories. In summary it can be inferred that from the foregoing arguments that there is a need to bring technology as a central factor for investigation into how it affects e-Government service security although such an investigation should focus on user perspective because much of the studies conducted until now focus only on technological factors and not user behavioral aspects.

2.6.3 Nationality as a Cultural Contextual Factor Affecting E-Government

Research on e-Government shows that culture is a factor that affects users with regard to adoption of e-Government (Al-Shafi and Weerakkody, 2010; AlAwadhi and Morris, 2009) and implementation e-Government (Reffat, 2003; Ebrahim and Irani, 2005; Halaris et al., 2007; Hung et al., 2009) although some disagree on the conclusion that culture is a factor that affects e-Government adoption. For instance AlShihi (2005) did not find evidence that culture affects e-Government adoption while studying development and adoption of e-Government services in Oman. Another important aspect that is observed in the literature is that culture has been shown to be represented in many forms including language, nationality, education, ethnicity, religion, family, gender, social class and organization (Usunier, 1993). This implies that culture as a variable could be tested or investigated in different ways one of which is nationality. Infact literature is replete with papers that have investigated the effect of nationality on different

aspects of e-Government including its adoption, implementation and influence on organisational performance (Alharbi et al., 2014; Al-Shehry, 2009; Chen and Dimitrova, 2006). However there has been consistent calls by researchers to investigate the influence of culture in association with such factors as trust (Al-Shafi and Weerakkody, 2010; AlAwadhi and Morris, 2009) in order to understand citizens' behavior in different cultures while encountering e-Government technology. What emerges from these discussions is that nationality as a cultural factor needs to be considered in any investigation concerning e-Government although such investigations may or may not add significantly to the existing body of knowledge if one considers the volume of investigations conducted on culture as a factor affecting e-Government already.

Theoretically literature shows that cultural aspects involving nation as a factor have used such theories as Social cognitive theory, Intrinsic and Extrinsic Motivation (IEM), Theory of Interpersonal Behaviour (TIB), TAM and DOI (Elsheikh and Azzeh, 2014) to understand how different contexts pertaining to different nations affect users of e-Government in those nations. While there is considerable debate on whether these theories can be applied to every context (Elsheikh and Azzeh, 2014) what emerges is that some aspects of the TAM like perceived ease of use or usefulness, appear to be a major concern of users of new technology, including e-Government technology, in making decisions on using the technology, in different nations (Gupta et al., 2015). It is therefore possible to infer that certain factors derived from the TAM can be useful in explaining the use of nationality as a cultural factor in research concerning e-Government, including user perspective of e-Government security.

While the foregoing discussions have delved on contextual factors, it is reasonable to state that the centrality of user centric e-Government security to users and e-Government service providers not only hinges upon the contextual factors but others that are crucial enablers of e-Government (e.g. trust of citizens) and prerequisites (e.g. need for the service and ability of the service to satisfy that need of the users) (Srivastava and Teo, 1998). Enablers could be antecedents of e-Government security aspects that affect users. Thus next section identifies some of the antecedents on which user centric e-Government service security depends.

2.7 Antecedents of E-Government Security that Affect Citizens

From Section 2.6.2 it can be seen that technology has been identified as an important contextual factor that has become central to a research on user centric e-Government services security. This implies that technology becomes an important antecedent of user centric e-Government services security. This argument is further justified by the examples of the introduction of such technology based services as Twitter, Facebook and LinkedIn in major e-Government portals

which create security hazards to users a phenomenon that has not been well studied (Dong, 2015). Introduction of social media technologies in e-Government services although have been argued to contribute to security hazards for users (Criado et al., 2013) how users are affected by those technologies with regard to e-Government security is an important area of concern in the literature. Hence it can be implied that introduction of new technology needs to be investigated as a major antecedent of user centric e-Government services security, especially when new technologies like cloud computing are introduced in e-Government and perhaps as the core determinant of user centric e-Government services security an argument supported by Shah et al. (2014). Other potential antecedents of user centric e-Government services security identified researchers as requiring further investigation include trust and risk propensity (Shah et al., 2014). While literature speaks of many factors as affecting security which include information security, awareness, privacy, availability, accessibility, culture (Alharbi et al., 2014), web design, authentication and internally and externally provided assurance (Shah et al., 2014) trust and risk appear to be two significant factors that have been highlighted in the literature as affecting the users of e-Government (Alharbi et al., 2014). This could be because trust is expected to enhance the users' interest in repeat use of e-Government whereas risk produces negative consequences in the minds of people leading to avoiding e-Government (Alharbi et al., 2014). Further, with every technological innovation, it is essential to understand the extent of trust and risk users could perceive as literature highlights that technological innovations bring with them security concerns regardless, for instance cloud computing in e-Government (Kemp Little, 2013). Thus this research focuses on three factors namely technology, trust and risk as antecedents of citizen centric e-Government security.

2.7.1 Technology as an Antecedent of E-Government Services Security

The importance of technology as a core factor affecting user centric e-Government services security has been explained in Section 2.6.2. Extending those arguments further it is can be seen that technological advances and innovations that have recently impacted e-Government include mobile-computing, I-pads, cloud computing and social media networking (see Section 2.5). Transactions by users through e-Government portals are now taking place using latest devices such as touch screen devices, 4G telecom technology that provide a high capability to the users in interacting using mobile devices, communication via social networking sites and using facilities offered by cloud computing which enable users to store and retrieve data using distributed systems. Unfortunately if there is one parameter that immediately affects users when technological innovations are introduced is the user security (Shah et al., 2014). Introduction of new technology or innovations in technology immediately affect users in many ways including how to interact with the technology, privacy issues, quality issues and security issues (see above). Besides, investigations into antecedents of user centric e-Government security have

been very limited and such investigations have not addressed the influence technology as a factor affecting user centric e-Government services security taking into account different factors (Shah et al., 2014), for instance trust and risk, in one model and also in a variety of contexts. For example the impact of the introduction of cloud computing on user centric e-Government services security is an area that has not been discussed well. From literature it can be seen that one of the major concerns of introducing cloud computing is the user security (Voorsluys et al., 2011; Ahmed and Hossain, 2014).

2.7.2 Moderators of Technology, an Antecedent of E-Government Security

While trust and risk have been identified in the literature as essential factors that need to be investigated in any research concerning technology and user security issues, it is important to understand what factors moderate the relationship between technology and e-Government security with regard to e-Government. The reason for brining in the concept of moderators is that the relationship between technology and e-Government security has been characterized in the literature as being influenced by certain factors and technology does not act in isolation (Elsheikh and Azzeh, 2014). For instance Elsheikh and Azzeh (2014) have identified quality of service, diffusion of innovation, computer and information literacy, culture, lack of awareness, technical infrastructure, website design, and security as affecting the decision of citizens to use e-Government out of which technology itself has been identified to be influenced by factors including privacy issues of users, computer and information literacy of users and quality of service of e-Government. If this is the case it is not possible to discuss any model that involves technology to overlook the influence of moderators of the relationship between e-Government technology and e-Government security. Such an argument finds support from theories such as TAM which argues that ease of use and usefulness of technology influence human behavior towards adopting that technology, information theory which states that disclosing less information increases privacy (Iachello and Hong, 2007) and HCI theory which explains a wide range of human-computer interaction aspects (see McCarthy et al., 2014) including technological aspects. Thus it is reasonable to argue that it is necessary to investigate the relationship between technology and e-Government security using useful moderators for instance privacy of users, web quality of e-Government and HCI. While it is possible to include more moderators in the investigation, it is also reasonable to limit the number of moderators in one PhD research in order to know how they impact the relationship between technology and e-Government security, so that the findings from such a research could be extended to other moderators. In addition there is no common set of variables identified by researchers as influence technology and each one of the researchers have examined different sets of variables as affecting technology. For instance when one considers the user perspective, use of e-Government technology was argued to be affected by demographic characteristics and personal

characteristics by Venkatesh et al. (2012). Similarly DeLone and McLean (2003) investigated the influence of information quality, system and service quality and user satisfaction on use of e-Government technology. In another instance in a study on e-Government technology effectiveness in Egypt, Abdelsalam et al. (2012) used management capacity, security and privacy, and collaboration as variables influencing the e-Government technology effectiveness, which brings out yet again the difference that persists amongst the different researchers on the set of variables that influence e-Government technology. In such a situation of flux it is perhaps not contentious to identify and investigate variables chosen in any specific research as long as there is support of the established theories for using those variables. The three variables HCI, privacy and web design quality identified in this research as affecting e-Government technology are separately reviewed critically in Sections 2.10 later.

2.7.3 Trust as an Antecedent of E-Government Services Security

The factor trust has been found to be an important component of e-Government (Warkentin et al., 2002). There is evidence in the e-Government literature to suggest that trust as a factor impacts citizens' adoption of e-Government. There is also evidence in the literature to point out that trust issues in the internet can be grouped together with factors such as security and privacy (Alomari et al., 2012). Besides, trust as a concept has been described in a number of ways in the literature and has been used in a variety of models (Gefen et al., 2003), a situation that has led to the possible derailment of a simple and useful understating of the concept of trust as applicable to the users of e-Government. For instance 'trust of the internet', 'trust of the government', 'trust of the Citizen Service Centres (CSCs)', 'party-based trust' or 'trust in government' and 'institutional trust' (Carter and Weerakkody, 2008; Carter and Bélanger, 2005; Gefen et al., 2003) are some of the ways trust has been depicted in the literature. This shows that there is a lack of agreement on what could really constitute trust and how to describe it. However if one restricts the focus on e-Government and its users, a description of trust that could be more suitable in this research is the one that should focus on users. There a few descriptions of trust that fit this argument which include:

Iachello and Hong (2007) argue that the concept of trust with regard to data originated in the government and referred to the accountability of the owners of data (meaning the government). In the context of changing technology (for instance cloud computing) trust is considered to be directly related to the security concerns of the users in terms of credibility and authenticity of the service provider (Ryan and Falvey, 2012; Ahmed and Hossain, 2014). In another instance Buyya et al. (2009) argue that trust of users towards the service providers is a basic need to ensure the expected level of privacy for the applications hosted by the service provider. Another

important aspect that needs to be considered is that trust as a concept is widely associated foremost with technology and then with user security, user risk, user privacy and adoption intentions of users (Voorsluys, et al., 2011; Ahmed and Hossain, 2014; Voutinioti, 2013). Although these arguments could lead to the inference that technology, user security, user privacy and adoption intentions of users are important factors that are related to trust of users as a concept in the e-Government literature, it is important to note that literature (e.g. Elsheikh and Azzeh, 2014) in general advocates further research to understand how user trust on e-Government services could be affected when technology changes. For instance Elsheikh and Azzeh (2014) argue that the effect of innovation in the IT sector, particularly on user centric security aspects in the e-Government domain, is an important area for future research in the context of developing nations. This could mean that other factors other than the ones identified here, could also play a role in understanding how trust affects e-Government services security, an aspect that needs further investigation. Thus it is useful to argue that there is a need to investigate how trust as a factor affects online security alongside other factors. Lack of user trust on e-Government services security can become a major barrier for users to use e-Government. Hence every effort to know more about how trust operates in the e-Government can reveal hitherto unknown facts.

Further, it can be seen that trust as a factor has been associated with other crucial factors including risk, technology, privacy, HCI and web design quality (e.g. Elsheikh and Azzeh, 2014; Iachello and Hong (2007). While literature shows that trust could be linked to security as an antecedent (e.g. AlKalbani et al., 2015) there is no agreement on how trust affects user centric e-Government security, for instance whether trust is directly linked to security or indirectly, an argument that gives rise to the speculation that there could be multiple ways by which trust could be liked to user centric e-Government service security. For instance AlKalbani et al. (2015) have argued that trust could be linked to information security compliance issues related to e-Government directly. However Elsheikh and Azzeh (2014) have argued that citizen trust in e-Government and perceived online safety and security are factors that together influence citizen centric delivery of e-Government services. In another instance Shah et al. (2014) argue that the effect of user trust and risk propensity need to be studied on overall security of e-Government as antecedents. Shah et al. (2014) argue current studies that have investigated online security fall into the category of computer science and engineering from the perspective of technology and engineering which is very objective in nature. However Shah et al. (2014) point out that hardly any study has been conducted to understand the influence of trust and risk propensity over security as antecedents of e-Government in the area of management sciences that address online security in a subjective manner.

As far as theoretical support to the concept of trust and its relationship to other factors in the field of e-Government services are concerned some have argued that the theory of Unified Theory of Acceptance and Use of Technology (UTAUT) can be applied to explain the concept of trust as a factor affecting user centric e-Government services security issues. In turn some theories applicable UTAUT namely 'Performance Expectancy' and 'Effort Expectancy (Rotter, 1967) have also been extended to explain trust in the field of user centric e-Government services in the extant literature. For instance expectancy theories have been used to define trust as "expectancy that the promise of an individual or group can be relied upon" (Voutinioti, 2013). Furthermore, some have used trust as a factor in models that have used the theories of TAM and DOI (Gefen, 2002; Pavlou, 2003; Warkentin et al., 2002). However Bélanger and Carter, 2008) have argued that few have used the above mentioned theories to explain the sole implication of trust on user related behavior in the e-Government domain, for instance e-Government adoption behavior. These arguments lead to the inference that there is a need to know how contemporary behavior theories could be applied to understand the usefulness of trust as a factor that affects user centric e-Government services security as an antecedent.

An important aspect that needs to be understood at this point is that if a technology like e-Government technology can affect trust as a factor, it is reasonable to worry how that trust manifests or can be verified to exist in a situation where technological changes take place. It is argued that trust evolves with changing technology (Giustiniano and Bolici, 2012). There are different ways by which this could be attempted. For instance when users transact through the government portal, the perceived ease of use and usefulness of transacting through the e-Government portal can be used as factors that could indicate that users feel comfortable in using the e-Government facility and hence would trust the e-Government services. Similar arguments could be put forth in the case of such factors as technology (see Section 2.6.2) and demographical aspects (see Section 2.6.1) as trust is argued to evolve continuously as a result of changing technology (Giustiniano and Bolici, 2012) as changing demographical aspects (Abunadi et al., 2008). It is therefore useful to understand how certain factors affect the trust of users when dealing with e-Government security. Two important factors that have been identified as not well studied in this regard are perceived ease of use of e-Government technology and perceived usefulness of e-Government technology (Ayyash et al., 2013). These two aspects have been argued to be under-investigated with regard to their ability to influence users to build trust in transacting securely through the e-Government facilities (Ayyash et al., 2013). Hence the next sections discuss how these some factors affect the relationship between user trust and their belief in e-Government security.

2.8. Factors Affecting the Relationship between Trust and E-Government Services Security

An important aspect that needs to be considered in an investigation on e-Government aspects is the assertion or confirmation of the users' trust and hence acceptance or adoption of the e-Government technology an important part of which is the user centric e-Government services security (Renny et al., 2013). In this context two factors appear to have been widely accepted in the literature that indicate user acceptance and usage of a technology namely perceived ease of use (PEOU and perceived usefulness (PU) of the technology. These two factors are extracted from the TAM of Davis (1989). The argument is that if e-Government technology is assumed to influence user centric e-Government services security, then how does it manifest or verified empirically. PEOU and PU are two constructs that have been used effectively by researchers to indicate that the intention to accept or adopt or use the technology is based on how easy it is use the technology and how useful it is to the user (Danila and Abdullah, 2014). However Ayyash et al. (2013) assert that literature is largely silent on how these two factors affect trust of users and not many investigations have been conducted to know how user trust is affected by PEOU and PU. Thus in the context of the current research it is possible to argue that empirical tests on how PEOU and PU affect the trust of users of e-Government technology. At the same time as a corollary it can be stated that if PEOU and PU could be used as predictors of trust of users, then these two constructs could also be used to understand how a relationship between users' trust and user centric e-Government services security is affected by PEOU and PU. These aspects of PEOU and PU are discussed later under Sections 2.81. However there is a third factor that has been considered to affect the users of e-Government technology and their trust which is the demographic factor (see Section 2.6.1). Demographic factors have been widely used to just understand how they interact with aspects affecting e-Government including trust and e-Government services security. Taking into account the above arguments the following discussions focus on the three factors namely PEOU, PU and demographic factors next.

2.8.1 Perceived Ease of Use (PEOU) and Perceived Usefulness (PU) as Antecedents of Trust in E-Government Technology

These two constructs have been derived from the theoretical model TAM. There is evidence in the literature show that PEOU and PU affect the perception of users of an information system technology with regard to the technology as well as their trust, risk and security issues (Gupta et al., 2015; Yan and Yang, 2015; Papadomichelaki and Mentzas, 2012). Perceived ease of use refers to the extent to which a user believes that using a new information system demands little or no effort; while perceived usefulness is the degree to which a user believes that using new information system would enhance task performance (Davis, 1989). That PEOU and PU

affects not only adoption and acceptance behavior of a technology is shown in the literature which shows that there is a close relationship between PEOU and PU on the one hand and technological aspects of an information technology artefact or an online technology artefact e.g. in terms of effectiveness of the technology (Thao and Trong, 2015), users' trust and user felt risk (Yan and Yang, 2015) on the other. These arguments can be extended to E-Government technology as well as e-Government technology is another IT and online artefact. However there are consistent calls in the literature which indicate that every time a new context or technological change occurs, there is a need to investigate the effect of PEOU and PU on acceptance and adoption of technologies by users as well as the trust factor affecting users. It is further important to understand that with regard to the core issue of user centric e-Government security on which this research is focused, it is also seen in the literature that PEOU and PU of e-Government technology affect user centric e-Government security although current evidence available suggests that such an influence of PEOU and PU of e-Government technology on user centric e-Government security is mostly seen through the adoption behavior of users (e.g. Renny et al., 2013). As far as theoretical support for PEOU and PU is concerned it can be seen that both are grounded in the TAM developed by Davis (1989). This theory has been extended extensively to explain many issues in both technological and social science fields. Hence any involvement of PEOU and PU is mostly grounded in TAM or one of its extensions like UTAUT.

In addition to the above arguments, it must be brought out that PEOU and PU have been almost always used to determine the technology acceptance and adoption behavior (see above). Hence it is implied that if there is an investigation that examines the relationship between the e-Government technology and user centric e-Government security, then it is reasonable to assume that linking PEOU and PU to technology could actually reveal the influence of PEOU and PU on the technology adoption behavior. But prior to attempting to use the technology literature shows that users tend to be cautious as far as trusting the technology is concerned (Ayyash et al., 2013). Lack of trust can reduce the usage of technology. Although researchers have investigated the influence of many factors on usage of technology only recently there has been efforts to understand how lack of trust can lead to failure of e-Government initiatives (Ayyash et al., 2013). This includes the factors PEOU and PU. Further only recently researchers have started to understand the role of trust in the acceptance of e-Government technology (Warkentin et al., 2002; Carter and Bélanger, 2005; Gefen et al., 2005; Welch et al., 2005; Bélanger and Hiller, 2006; Bélanger and Carter, 2008). Thus it is posited that testing the relationships PEOU to trust in e-Government technology and PU to trust in e-Government technology can enable an understanding whether users have really been affected by the changing technology artefact at all

and how does it affect the relationship between trust in e-Government technology and user centric e-Government security.

2.8.2 Demographic Factors as Antecedents of Trust in E-Government Technology

Demographic factors have been dealt with in the extant literature in different ways including as moderators (Hashim et al., 2015), controlling factors (Mourao et al., 2015) and not to mention of the few occasions where they have been used as predictors (Ibrahim and Pope 2011). In addition demographic factors have been used to just describe about the population under study (e.g. Rana et al., 2015). This indicates that demographic factors can be conceptualized in various ways and such conceptualizations depend on the aim of the research. For instance while using UTAUT for their study Hashim et al. (2015) investigated how demographic factors moderate the relationship between trust and adoption behavior of users of cloud computing. Here the primary aim of the research was to gain an understanding of the relationship between trust and adoption behavior of users of cloud computing not demographic factors. However Ibrahim and Pope (2011) studied the gender as a predictor of e-filing system which indicates that the primary purpose of the investigation was the demographic factors. These arguments point out how demographic factors could be useful in understanding behavioral aspects of populations, especially aspects related to their perception of, say, trust in e-Government, when technological changes occur.

The foregoing arguments have discussed how different factors can be linked to trust in e-Government technology and why there is a need to understand such linkages. It should be noted here that factors namely PEOU, PU and demographic factors have been discussed in order to limit the research to specific aspects as extending the research to many other factors affecting trust of users can make the scope of this research too large to be handled in one PhD research. Extending these arguments further it can be seen that a factor that closely works alongside trust as an antecedent of user centric e-Government services security is the factor risk, and has been identified by Shah et al. (2014) as requiring further investigation in the management sciences domain. This discussion is provided next.

2.9 Risk as an Antecedent of E-Government Services Security

Like trust, risk has been identified as a major factor that affects users of e-Government services in the literature especially when user security aspects are brought into focus (Shah et al., 2014). For instance risk comes into focus when users feel uncertain about the quality of services offered online, cost of learning about changing and advancing technology and the need for additional resources to transact effectively through the e-Government services so that full

benefits accruing through the e-Government are utilized (Lee et al.,2011). It won't be an exaggeration to state that every context including new technological context brings in a sense of risk in the minds of users when they encounter a change in the situation.

A broad definition of risk found in the literature is that a person who trusts a phenomenon also thinks about the possibility of gains and losses (Mayer et al., 1995; Pavlou, 2003; Warkentin et al., 2002). It is argued that when risk is felt, trust is mandatory (Corritore et al., 2003; Mayer et al., 1995; Pavlou, 2003). In another instance one researcher found trust as an important antecedent of perceived risk (Pavlou, 2003). It is also explained in literature that risk is not measurable objectively and hence the perception of risk is considered as meaningful. In fact perceived risk is defined as some kind of a subjective expectation a person has that is related to suffering a loss that may occur in pursuit of an outcome aimed to be achieved by that person (Warkentin et al., 2002). Thus it is clear that conceptually risk has been viewed differently by different authors in the literature and it is reasonable to argue that where one speaks of trust or technological changes, there could be a necessity to examine the extent of risk felt by users of such a technology and the trust they pose in that technology.

Despite the fact that user perception of risk has been well investigated from the point of view of user acceptance of e-Government (e.g. Lagzian and Naderi, 2015; Fang et al., 2005, 2006; Pavlou and Gefen, 2004), hardly any research has been conducted in understanding the influence of user felt risk on online security from the perspective of management which is subjective in nature (Shah et al., 2014). In fact Shah et al. (2014) argue that current research outcomes have addressed antecedents of online security only from the perspective of technology and engineering in an objective manner but not from the perspective of management which is more subjective. Considering the fact that the user centric online security needs to be addressed from the managerial perspective, user perception of risk needs to be examined as an antecedent of online security to understand how it influences the online security subjectively.

Apart from examining the influence of user perceived risk on online security as an antecedent of online security, it is also important to recognize that user perceived risk has been identified to affect online security not as a standalone factor but in combination with factors like technology, trust, IT attitudes, IT knowledge, IT experience, IT confidence, innovativeness and satisfaction (Bélanger and Carter, 2008; Elsheikh and Azzeh, 2014). Many models have been conceived that have explained how user perceived risk of using e-Government has impacted users. For instance Bélanger and Carter (2008) established a model of user adoption of e-Government which focused on trust and risk, thus risk was associated with trust. It was argued by Bélanger and Carter (2008) that higher the risk felt by users in using e-Government technology, lower is the

trust developed and adoption of e-Government. Burda and Teuteberg (2014) studied the role of trust and risk in the perception of adopting cloud storage by students in German universities. Iachello and Hong (2007) highlighted the risk of misuse of technology made possible due to new challenges that emerge from HCI and privacy issues when new online applications (e.g. new kinds of mobile and ubiquitous computing applications) crop up and are used in non-traditional settings. More examples could be cited from the extant literature on the different models that have been developed to understand the role of risk felt by users of online facilities including e-Government, all of which point towards the need to examine the concept of risk felt by users of online facilities under changing circumstances.

As far as theoretical support needed for understanding the concept of user felt risk is concerned, much of the theories used by researchers include theories that enable the anticipation and analysis of human behavior (Venkatesh et al., 2003). Thus theories such as the theory of Planned Behavior (Ajzen, 1991), the second model of Technology Acceptance (Venkatesh and Davis, 2000), and the Innovation Diffusion Theory (Rogers, 1983) are seen to be the most widely used to explain user behavior of online use (Lagzian and Naderi, 2015). Here the assumption is that acceptance of information technology by users is considered to be the principal factor in e-Government success in the literature (Lagzian and Naderi, 2015). However there are situations where users could feel threatened to interact with a new technology that emerges due to privacy and HCI aspects. In such situations some have advocated the development of a theory of technology acceptance (Iachello and Hong, 2007). Thus dominant theories cited above need to be examined for extending their application where the question of user felt risk needs to be understood in conditions where new technologies have emerged (the focus of this research) or contexts have changed. Further to an understanding of why user felt risk needs to be examined in this research as an antecedent of user centric e-Government security, the next section deals with the other aspects of technology (other than demographic and contextual factors) that could affect the influence of technology on user centric e-Government security as the core issue tackled in this research is the relationship between technology and user centric e-Government services security.

2.10 Factors Affecting the Relationship between Technology and E-Government Security

Amongst the different factors that have been argued to affect the relationship between technology and e-Government security in the literature some of the widely discussed factors in the literature include privacy of users, quality of web design, perceived ease of use of technology, perceived usefulness of technology, social pressure, attitude, subjective norm and

perceived behavioral control (AlKalbani et al., 2015; Danila and Abdullah, 2014; Alleweldt et al., 2012) to quote a few. Also discussed in the literature as a factor affecting e-Government technology or online technologies, is HCI although in a lesser measure. According to Gulliksen (2014) HCI has the potential to influence public policymaking and IT politics, an area that needs investigation as research in HCI, a multidisciplinary research covering fields like "technology, engineering and computer science, on one side and economics, behavior and social sciences on the other side, but also using design and other creative sciences" is not well addressed. Taking into account these arguments in this research following factors were chosen for critical review namely HCI, privacy of users and quality of web design.

There are two primary reasons for choosing the three factors. The first one is that the factors HCI, privacy of users and quality of web design have found to be closely associated with technological changes in the literature, especially when user behavior aspects are involved (see Sections 2.4 and 2.7.1). Thus any research wherein the core concept of investigation is technology and its relationship to e-Government services security, there is a need to necessarily consider these factors during the course of the investigation. The second reason is that theoretical conceptualizations have not yet been fully understood how users behave when new technological contexts appear necessitating the operationalization of important factors associated with technology (see Section 2.6.2). Thus these factors have been chosen for review in this research. However a word of caution is added here. Although these are not the only factors that have been identified in the extant literature as affecting users in a new technological context, it is important to understand that within the scope of one PhD research it is necessary to limit the number of factors that need to be considered for investigation failing which there is a risk of the research becoming unnecessarily complicated without focusing on the problem under consideration. Thus each one of these factors has been reviewed for understanding their conceptual aspects required for this research.

2.10.1 Human Computer Interaction (HCI)

HCI has been chosen as an important determinant of technology. The reason for choosing HCI is the important role it plays as the front end factor that enables a user to interact with e-Government. Further research on the relationship between HCI and technology is found to be a major area of concern in literature (Zhang et al., 2009). Researchers who have investigated the human behavior and interaction with respect to computers or technology have highlighted that a host of concepts are involved in this interaction, chief amongst them the recent advancement of technologies and relatively easy development of many sophisticated applications. Recent developments of technologies affect more and more people these days. Along with the

advancements come the bottlenecks of acceptance and deployment of those innovations because of user interface and human factors problem (Zhang et al., 2009). Investigation on how HCI contributes to acceptance and deployment of technology is a major concern that needs investigation. Technologies affecting e-Government are no exception to this as newer applications are being developed every day and each innovation needs to be investigated for its user acceptance promising technologies. As far as theoretical support for explaining the influence of HCI on technology it can be seen that a number of theories have been applied which include cognitive fit, task-technology fit, TAM, UTAUT, users with individual differences, users as economic agents, users as social actors, decision support systems and computer self-efficacy (Zhang et al., 2009). These theories cover a number aspects of the users. However as far as application of a theory or theories to HCI is concerned, UTAUT that is based on effort expectancy and performance expectancy has been used in the literature where research focuses on organizations, systems, users, and tasks although efforts until now have not enabled the application of such theories generalizable (Zhang et al., 2009).

2.10.2 Privacy of Users

Gulliksen (2014) argues that with the progress of the society from an information society to a networked society significant challenges arise; especially digitalization, a phenomenon associated with information and networked societies, has been found to cause concerns about employment and privacy alongside social isolation and alienation. It can be seen that when online trust and security is affected by cyber-attacks, privacy is breached (Gulliksen, 2014). Besides as far e-Government literature is concerned privacy issues have always been considered as a concern when contextual aspects especially when online technology changes. For instance Lagzian and Naderi (2015) argue that users generally feel as though they have low control on their privacy leading to mistrust on the online technology including e-Government technology. In a world where e-Government technology requires payments online and disclosure of private information, technological security is paramount and this aspect bothers the users (Abunadi, 2015). Thus studying the impact of privacy issues on the relationship between technology and e-Government services security assumes significance when contexts including technological contexts change.

As far as theoretical aspects are concerned, privacy issues are shown to be explained by largely adoption theories such as TAM, TRA, TPB, TOE, UTAUT and DOI (Sarabdeen and Ishak, 2015; Hashim et al., 2015). In addition some have proposed the application of social cognitive theory (Sarabdeen and Ishak, 2015). All these theories can be applied to explain individual behavior towards privacy aspects of users concerning e-Government. However in an ever

changing world of technology, extending the above mentioned theories to understand how privacy issues affect provision of e-Government technology is an important area that must be taken into account in any research involving privacy issues as a factor.

2.10.3 Quality of Web Design

After the discussions on privacy issues next the quality of e-Government technology in terms of web design was taken up for review as it was considered as a factor affecting e-Government technology. According to Papadomichelaki and Mentzas (2012) web design quality is an element of quality of e-services. Similar sentiments are echoed by other researchers (e.g. Ivory and Megraw, 2005; Iwaarden et al., 2003, 2004; Ivory and Hearst, 2002). A number of quality based research publications are found that have addressed many issues pertaining to quality including quality of e-Government services and quality of e-services (Papadomichelaki and Mentzas, 2012). In addition literature on dimensions of e-Government quality shows that a number of dimensions including functionality of the interaction environment, reliability, citizen support (interactivity), content and appearance, trust, privacy, security and ease of use (navigation, personalization, technical efficiency) (Papadomichelaki and Mentzas, 2012) have been addressed in the literature. Further Papadomichelaki and Mentzas (2012) while discussing their model of e-Government quality (e-GovQual) involving reliability, efficiency, citizen support, and trust have recommended that the knowledge gained about these factors need to be further extended e-Government websites to develop guidelines for future development of e-Government websites. Considering the importance of e-Government quality to users, and taking into account the arguments of Papadomichelaki and Mentzas (2012) and others (e.g. Chen et al., 2015) who argue that web design as a factor affects users and need to be studied further in order to identify any barrier that may crop up due to web design quality factors and make the e-Government effective. There is lack of generalizability on the operationalization of the outcomes of current research to different contexts which implies that every research on e-Government quality needs to investigate the implications of quality of website design in order to know whether it is making the e-Government technology effective and secure or not. This is evident from the variety of factors analyses in the e-quality literature that constitute quality of website design which are not having consensus (see Papadomichelaki and Mentzas, 2012). Thus quality of website design becomes an important factor that needs to be investigated for its influence on the e-Government technology especially under changing technological contexts.

Theoretical support for quality of web design can be seen to be largely grounded on a number of concepts such as SITEQUAL, SERVQUAL and TAM to quote a few (Halaris et al., 2007). For a more detailed elaboration of the approaches that have been applied to understand quality for the “e” channel of public services further reference to Halaris et al. (2007) is suggested.

However as is the case with the theoretical propositions and as suggested by Halaris et al. (2007) there needs to be a periodic review of the measure of quality to achieve continuous improvement. Quality of web design affects system performance (technology) and such an influence of quality of web design on system performance needs to be studied at various stages of the system evolution using appropriate theories including those existing and probably newer ones that may be conceived in future.

The foregoing discussions have provided a critical review on five important aspects that have been found to affect e-Government technology and user centric e-Government security. These are contextual aspects, antecedents of user centric e-Government security, e-Government technological aspects, user trust aspects and acceptance aspects, and user centric e-Government services security aspect. The core issue of e-Government technology has been reviewed as a contextual factor that affects users when technology change, for its influence on user centric e-Government services security. The discussions have shown that multiple factors play a role in understanding the relationship between e-Government technology and user centric e-Government security. The discussions also revealed that there are growing calls to study this phenomenon called "relationship between e-Government technology and user centric e-Government security". Theoretical propositions that could find application in this study have been discussed. Finally the discussions showed that serious gaps exist in the literature exist with regard to the current understanding of the "relationship between e-Government technology and user centric e-Government security" which need to be outlined. Thus as the outcome of this review, the next section discusses the gaps that have been found in the extant literature that need to be addressed.

2.11 Gaps in the literature

In the context of e-Government technology, security has taken a very important place due to a number of factors that constantly change which include contextual factors such as demography and technology, antecedents of user centric e-Government security including trust, risk and technology (incidentally a contextual factor) and user perception aspects including PEOU and PU (see Sections 2.8.1). Literature shows that users are concerned over rapid changes that take place on the e-Government technological front. From Section 2.6 and 2.10, it can be seen that such changes can affect a number of factors that have serious implications to the users and continuous investigations are being conducted in the field of e-Government to gain knowledge on how those factors come into play and affect users. For instance from Section 2.6.3, it can be seen that the ever changing contextual factors such as culture, education, and technology affect users and their concern for secure transactions through the e-Government. Thus it is reasonable

to argue that every time an investigation is conducted in a particular environment where e-Government is implemented, the outcomes obtained through such investigations on how changing contextual factors affect user centric e-Government security can produce new knowledge that can contribute to the growing body of e-Government related knowledge.

More importantly, since user centric e-Government security is paramount in any activity that is related to e-Government, literature shows that much of the study with regard to the antecedents of user centric e-Government security is restricted to technological aspects and not management sciences (Shah et al., 2014). Thus there is a gap in the literature that calls for more research to be conducted to be on the antecedents of user centric e-Government security to gain knowledge on how the relationship between those antecedents and user centric e-Government security can be dealt with to enhance useful user perceptions such as trust, risk on the one hand and contextual factors on the other. From these arguments and the review given above it is seen that there is a need to fill in this important gap. Further considering the fact that technology is the core issue that affects user centric e-Government security the most (see Section 2.6.2), it is reasonable to argue to that the most important gap that needs to be filled up is how technology affects user centric e-Government security. Since literature review shows that technology is not the lone antecedent of user centric e-Government security, other important factors need to be brought into the investigation as antecedents include trust and risk perceived by users (see Section 2.8 and 2.9). Trust appears to be a common factor that gets affected with any change that takes place in the technological front and most often trust is seen to be associated with risk as a factor alongside online security. Further literature shows that serious investigations on how trust affects user centric e-Government security have only been recently initiated without conclusive outcomes. Thus the gap in the literature concerning trust and risk as antecedents of user centric e-Government security needs to be filled.

While technology as an antecedent is found to be the core issue that affects user centric e-Government security, literature shows that as a stand along factor technology is itself affected by other components including HCI, privacy issues of users and web design quality of the e-Government portal (see Section 2.10). However how these components affect technology in its role as an antecedent of user centric e-Government security is an aspect not addressed in the literature. This is a major gap that needs to be addressed. Knowledge about how these antecedents of technology affect the overall relationship between technology and user centric e-Government security can provide a greater leverage to deal with a wider set of factors and enhance user centric e-Government security.

Arguing in a similar manner it is also seen that trust is affected by user perceived factors including PEOU and PU (see Section 2.8.1) and without understanding their influence on trust it is difficult to get a full picture of how trust affects user centric e-Government security and the outcome of such research would be incomplete. Hence it is necessary to include PEOU and PU in any investigation involving trust as an antecedent of user centric e-Government security thereby the gap left in the literature could be comprehensively addressed. Similar arguments could be made with regard to contextual factors as the first factor that gets affected by any change in any of the contextual factor namely technology, experience, education and culture is user trust in e-Government technology (see Section 2.6). Thus the investigation involving trust as an antecedent of user centric e-Government security should include the contextual factors while addressing the gap.

2.12 Conclusion

This chapter has critically reviewed the concept of e-Government and the core area of research namely user centric e-Government services security. Various theories and concepts postulated in the literature have been discussed. Different factors including demographic factors, user perceived e-Government security, antecedents of e-Government security, antecedents of technology and trust and their linkage have been critically discussed. The gap in the literature has been identified. This chapter provides the basis for drawing the theoretical framework for this research discussed in the following chapter.

Chapter 3: Theoretical Framework

3.1 Introduction

User centric e-Government services security is a major area of concern for both the users and the service provider. From Section 2.3, it can be seen that literature is silent on how users of e-Government understand security and what factors affect the e-Government services security, knowledge that is needed from the management point of view. Further it is not clear from the literature what antecedents affect e-Government services security and how the two are related. In order to address these gaps the following theoretical framework has been drawn based on the critical review provided in the previous chapter. However an important contextual definition needs to be added here as context in which e-Government technology operates is important to understand user beliefs and behavior with regard to security offered by the e-Government service provider.

3.2 Research Context

This research is aimed to be conducted in an environment where the e-Government service provider namely the Government of the Kingdom of Bahrain has introduced a change in the technological aspects supporting the e-Government operation. Recently Bahrain government introduced cloud computing in the e-Government services offered to the citizens of Bahrain (Supreme Committee for Information and Communication technology (SCICT), 2015). This is a major technological change. As explained in Section 2.5, one of the major concerns of cloud computing is the security aspect. Adding to this concern is that users will not be able to easily feel the introduction of cloud computing principles when they transact through the e-Government portal and hence will not able to understand how such a change affects their security concerns. Not many empirical evidence are available to establish that users are secured while operating through the e-Government portal that has employed cloud computing and what their feelings are with regard to security. Thus this research embarks on generating empirical evidence on how user centric e-Government service security is perceived by users in an environment characterized by change in technology. Through the next sections that follow a theoretical framework is drawn to empirically test this concept.

3.3 E-Government Security and User Centricity

From Section 2.3, it can be seen that e-Government security is an important topic that affects both the users and service providers. Literature shows that a number of user related factors influence e-Government security which includes contextual factors, trust and risk. Amongst the

contextual factors that affect e-Government security the one that is considered the most important is the technology factor (see Section 2.7.1). Shah et al. (2014) in their study in Malaysia found that technical protection, a factor that refers to the protection built on to the website by the online service provider in terms of integrity and confidentiality of customers' data, directly affects the overall security perceived by the users. Overall security meant financial information security including credit card information or online password. While the study of Shah et al. (2014) posits that technology provides protection to users' data information and positively influences user belief of security, it must be understood that such a position needs to be tested in the combination of other factors such as trust and risk a recommendation suggested by Shah et al. (2014). Technology's influence on user security as an antecedent of user perceived online security, although established by Shah et al. (2014), such a finding is incomplete without the inclusion of trust and privacy. This argument gains currency because changes in technology foremost impacts user behavior in terms of trust and risk perception an argument that is supported by literature (see Section 2.7.3, .8 and 2.7.9). Thus this research while relying upon the findings of Shah et al. (2014) partially, posits that the direct relationship between technology as a factor that affects e-Government security and user felt e-Government services security needs to be altered by introducing trust and risk. Theoretical support for establishing a relationship between technology, trust and risk on the one hand and user centric e-Government services security on the other is provided by socio-technical and adoption theories. While socio-technical theory argues that there needs to be a fit between technical sub-system and social sub-system and there needs to be a fit between the two (Bostrom and Heinen, 1977), adoption theories suggest that the attitude towards adoption is affected by a number of factors which include trust of the user and risk felt by the user. Thus taking support of the two theories (see Sec Sections 2.7.2 and 2.7.3) it is possible to establish a relationship between technology, trust and risk on the one hand and user centric e-Government services security on the other.

3.3.1 Relationship between Risk and User Centric E-Government Security

Literature shows that contradictory opinion prevails on the nature of the relationship between risk felt by users and the security perceived by them in transacting through the e-Government portal. For instance, Kumar et al. (2007) argue that perceived risk leads to security issues and discourages use of online services. However, Bwalya and Healy (2010) argued that both risk and security affect e-Government adoption as associates. In contrast, Shah et al. (2014) argue that risk felt by users should be considered as an antecedent of user centric e-Government security. These arguments lead to the inference that there is no consensus on how to conceptualize risk. Especially when technology changes whether risk precedes security or acts in association with it or determined by security is a matter that needs to be investigated.

However if one considers that users are forced to take risk when a new technology is implemented in e-Government, user security aspects such user information security, could be put to risk. This argument is supported in the literature (AlKalbani et al., 2015). Thus, it is posited that user felt risk influences user centric e-Government security directly. However it must be borne in mind that when risk is involved, lower will be the security felt by users and vice versa. This argument finds theoretical support from technology acceptance theories that state that users accept information technology despite security risks (see Section 2.4). The hypothesis that can then be formulated to verify this assumption is:

H4: User felt risk negatively influences user centric e-Government security

3.3.2 Relationship between Trust of Users and User Centric E-Government Security

Trust has been identified as a major factor associated with user acceptance of a technology, security aspects related to e-Government and risk felt by users in using e-Government technology (see Section 2.7.3). There are different ways by which trust has been conceptualized in the literature. For instance, AlKalbani et al. (2015) argue that when trust and confidence in users increase then users feel a sense of greater security while using online services including e-Government services.

However, Belanger and Carter (2008) argue that trust of the internet could be linked to perceived risk of the user of internet. In another instance Shah et al. (2014) suggest that trust should be considered as an antecedent of user centric online security but do not provide any recommendation how the two should be related. However, in the natural behavior of users, when a new technology emerges, users first pose trust in the technology and use it before recognizing the risks involved and the possible breach in the security aspects related to their privacy or personal information. This argument finds support from the literature. For instance, Lee and Rao (2007) established a relationship between disposition to trust and security risk on the internet. However, there is no clarity in the literature on whether trust as an antecedent of e-Government security is related to it directly or through any other construct like risk. But considering the evidence available in the literature that trust is related to risk and risk is directly related to user centric e-Government security (see Section 2.8) and taking into account the recommendations of Shah et al. (2014) of the need to investigate trust as an antecedent of user centric online security, it is argued that trust could be either directly linked to e-Government services security or through risk. That trust affects human behavior including user felt risk, is an argument that is supported by technology acceptance and adoption behavior theories (see Section 2.9). The hypothesis that could be formulated is:

H3a: User trust on e-Government negatively influences user centric e-Government security

H3b: User trust on e-Government negatively influences the risk felt by users of e-Government

This hypothesis leads to the linkage between trust and user centric e-Government security directly and in consonance with the hypothesis H4 through risk as an intervention. Further, since the objective is to know how technology interacts with user centric e-Government security in the presence of user trust and user felt risk, the next section investigates the relationship between technology and user centric e-Government security.

3.3.3 Relationship between Technology and User Centric E-Government Security

Technology has been identified in the literature as an important contextual factor that affects e-Government transactions made by users including user centric e-Government services security. (See Section 2.10). Ever since internet has been invented, technology, particularly ICT, has been found to be fundamental to any e-Government investigation. Much of the literature suggests technological infrastructure is a major factor that impacts user security. For instance, Lee and Rao (2007) argue that users feel protected if adequate technological structures are installed in the process of providing online services. This argument is further strengthened by the results achieved by Shah et al. (2014) who argued that technical protection affects overall online security of users. However, there are contrasting opinions voiced in the literature with regard to technological factors affecting online user security. For instance Hashim et al. (2015) identify security is an integral part of technology implying technology is represented by security as a factor. On the other hand, Shah et al. (2014) argue that overall online security perceived by users is determined by technical protection an argument supported by AlKalbani et al. (2015) who say that technological capability and compatibility determine adoption of information security compliance by government service providers. However, there are other arguments found in the literature that point out that technology affects a host of factors for instance trust. Abunadi (2015) argued that technology for instance electronic integrated systems including e-Government systems impact trust of users. These arguments point out to the need to understand how technology affects user centric e-Government services security, as there is no consensus on how technology affects e-Government services security. Considering the fact that much of the literature (e.g. Hashim et al., 2015; Magro, 2012; Kumar et al., 2007) has argued that technology indeed affects apart from user centric online security, a host of factors including adoption and acceptance of technology, it is reasonable to argue that the direct link between technology and user centric e-Government services technology needs to be re-examined. Such a re-examination may need to bring in user behavior factors, for instance trust. Trust is the most often cited factor in the literature as getting affected at the first instance when user comes into contact with technology. However, it must be noted that user trust in practice usually increases with a robust technology, for instance internet explorer. Hence while discussing the linkage

between technology and user centric online security, it is necessary to bring-in the concept of trust, which then leads to the following hypothesis:

H2: e-Government technology positively influences user trust in e-Government services.

Taking into account hypotheses H3 in which it has been assumed that user trust in e-Government services positively influences user centric e-Government security and H4 in which it has been assumed that user felt risk in e-Government services negatively influences user centric e-Government security, it is reasonable to assume an indirect relationship between e-Government technology and user centric e-Government security. That the assumption e-Government technology affects user perception of e-Government security is supported by both socio-technical theory and technology acceptance theories (see Section 2.4). Thus, it is reasonable to create a relationship between e-Government technology and user perception of e-Government security.

Further to drawing the relationship between e-Government technology, user trust in e-Government technology, risk felt by users in using e-Government services and user centric e-Government security, it is important to know how whether technology acts on user centric e-Government security in isolation or are there factors that moderate technology when it influences user centric e-Government security. This aspect is examined next. The reason for bringing this argument here is that literature clearly shows that technology is a factor that is affected by a number of factors that are both external (e.g. HCI and Privacy) and internal (e.g. web quality design) to the e-Government services provider but have the potential to affect the users. It is pertinent to examine the impact of those factors in a context of changing technological environment, which in this case is the introduction of cloud computing in e-Government. The following sections discuss this aspect.

3.4 Moderators of Technology

From Sections 2.7.2, it can be seen that HCI, privacy and web design quality play a leading role in deciding on e-Government technological structure. While the discussions in the preceding sections show that a number of factors can affect e-Government technology, what is important is to include some of the specific factors like HCI, privacy and web design quality that have significance in understanding how the relationship between technology and user centric e-Government security is affected by those factors.

3.4.1 Influence of HCI on the Relationship between E-Government Technology and User Centric E-Government Security

HCI gains importance because if one takes the example of a situation where in the modern world users can interact with e-Government portal using touch screens security comes into picture immediately as no two users can be assumed to have the same capability to understand and use the technology and this is a security hazard (Zhang et al., 2010). From Sections 2.10.1, it can be seen that every new innovation like cloud computing needs to be tested for security aspects by linking it to technology and HCI. It is seen from the literature that if HCI aspects are better designed, then users feel that the technology is better and develop trust with the technology and feel that security risk is lower (see Section 2.10.1). Literature supports the argument that user behavior with regard to how they interact with computers when technological changes take place and how technology affects their security needs to be examined with every innovation (see Section 2.10.1). Such an examination can be carried out by using socio-technical theory, HCI theory and acceptance theories (Zhang et al., 2010). These arguments are applicable to any online service including e-Government. From these arguments, it is possible to postulate the following hypothesis:

H1a: Human computer interaction positively influences the relationship between e-Government technology and user centric e-Government security.

3.4.2 Influence of User Privacy on the Relationship between-Government Technology and User Centric E-Government Security

In similar vein, it is argued that privacy of users alongside HCI acts as major concern of and challenge for users when technological innovations take place an argument supported by literature (see Section 2.10.2). Privacy has been identified as a major security factor in e-Government research. From Section 2.10.2, it is seen private user information can be compromised if technology is not robust. As one of the main factors, privacy issues have been argued to be major influencers of technological innovations and trust aspects and hence security risks (Gulliksen, 2014). Online service providers need to offer a technology that enables users to feel that privacy issues with regard to their personal data are secure when they use advance technology (see Section 2.10.2). Any examination of how technology is related to user centric e-Government security needs to necessarily include privacy as a construct an argument supported by literature especially when contextual factors change (Lagzian and Naderi, 2015). In addition, it can be seen from published material that higher the privacy, higher is the usage of technology an argument that could be tested to see whether a similar effect could be seen with regard to its impact on the relationship between e-Government technology and user centric e-Government security. Investigation into how privacy affects the relationship between e-Government technology and user centric e-Government security can be conducted using technology acceptance theories (see Section 2.10.2). Thus in order to verify whether user privacy affects the

relationship between e-Government technology and user centric e-Government security the following hypothesis is postulated:

H1b: User privacy positively influences the relationship between e-Government technology and user centric e-Government security.

3.4.3 Influence of Web Design Quality on the Relationship between E-Government Technology and User Centric E-Government Security

HCI is viewed in this research from the managerial angle more than the technical angle. However, that does not eliminate the involvement of technical aspects completely from the research. For instance, for any user of e-Government services, online payment when carried out, the quality of design of the website should ensure absolutely safe and secure user operations. Payment gateways always have contents and design of the webpage that conform to certain quality standards. Thus, web quality design carries importance in the relationship between e-Government technology and user centric e-Government security. From Section 2.10.2, it can be seen that In order to understand how web quality design affects the user behavior and its relationship between e-Government technology and user centric e-Government security service quality and adoption theories could be used. Already published material shows that higher the web quality design, higher is the acceptance of technology and hence greater trust in the technology and better is the feeling of security and risk. Thus in this research web quality design has been drafted in to investigate how it affects the relationship between e-Government technology and user centric e-Government security in association with HCI and privacy of users. In order to verify how web design quality impacts the relationship between-government technology and user centric e-Government security the following hypothesis is outlined.

H1c: Web design quality positively influences the relationship between e-Government technology and user centric e-Government security.

After having identified the factors that act as antecedents of user centric e-Government security and moderators of the relationship between e-Government technology and user centric e-Government security, the following sections discuss how contextual factors affect e-Government security and what user acceptance factors can be used to understand whether users have really trusted the change in e-Government technology. In the current research the researcher proposes to test this aspect in an environment wherein e-Government technology uses a newly invented technology namely cloud computing. The results of such testing is expected to yield findings about how technology really affects user centric e-Government security and what is the importance of antecedents with regard to user centric e-Government security.

3.5 Impact of Contextual Factors on Trust of Users of E-Government Services

While technology has been identified as the core construct (as antecedent of user centric e-Government security) affecting user centric e-Government security, the next most important factor that has been found to affect user centric e-Government security is the user trust in e-Government security. It is argued (see Section 2.8) that when users pose a high level of trust (one of the antecedents of user centric e-Government security) in e-Government, it implies that the user centric e-Government security is perceived to be high (Woodward, 2009). However from literature review (see Section 2.8.2) it can be seen that a number of contextual factors affect user trust in e-Government security, which include demographic factors. Amongst the demographic factors literature shows that age, gender, qualification, experience and cultural factors have been mainly analyzed by researchers (Myeong et al., 2014; Weerakkody et al., 2011; Bélanger and Carter, 2006; Bonham et al., 2001). Interest on how demographic factors impact trust and e-Government has been high amongst researchers involved in studying e-Government literature although studies that have assessed the influence of certain factors like nationality, education and experience of users on the relationship between trust and user centric e-Government security have viewed those factors variedly. For instance, Ibrahim and Pope (2011) have treated demographic factors as predictors in their study on e-Government whereas Hashim and Hassan (2015) have used demographic factors as moderators. There appears to be no clear understanding on how to deal with demographic factors in the extant literature. However, considering the fact that the main purpose of this research is to gain knowledge on how technology as a core concept and antecedent affects user centric e-Government security with the intervention of trust, as one of the intervening constructs, the focus on demographic factors is only academic. In fact, many researchers have just provided a report on how demographic factors operate in their investigations on e-Government aspects, for instance Fu et al. (2004), who just listed the profile of potential adopters of electronic taxpayers. While some useful information could be gained in relating demographic factors to trust as an antecedent of user centric e-Government security, such information only provides knowledge about population aspects but not conceptual aspects. Considering the importance of other conceptual factors to this research, it is proposed to just find out how certain demographic factors affect the antecedents of user centric e-Government security that will indicate about how the population under study is characterized. Thus three factors were chosen as representing the demographic aspects of the target population namely education, experience and nationality (cultural aspect). It is posited that if the relationship between these demographic factors and one of the antecedents namely trust is examined the outcomes of such an examination could be extended to other demographic factors not examined in this research and other antecedents of user centric e-

Government security as they have similarities. Further the research takes into account that two of the three demographic factors namely user education and experience affect user trust positively, meaning if education and experience are high, trust of users on e-Government is expected to be high, an argument that is supported by extant literature (Al Khattab et al., 2015). Similarly, nationality as a cultural factor has also been found to be affecting trust of users of e-Government services (Kearney, 2015). Thus keeping in view the main focus of this research intact, the three demographic factors are treated as control factors that affect the relationship between trust as an antecedent of user centric e-Government security and the outcome of the analysis will be just reported to know the effect of the demographic factors on the relationship between trust as an antecedent of user centric e-Government security and user centric e-Government security. Thus, the following hypotheses have been postulated in this research to verify the impact of education of users, experience of users in using e-Government and nationality of users on trust in e-Government:

H6a: Education level of users positively influences user trust in e-Government.

H6b: Experience of users in e-Government positively influences user trust in e-Government.

H6c: Nationality of users influences user trust in e-Government.

Further to identifying the purpose of using demographic factors to this research and relationship between demographic factors and user trust in e-Government, the next section discusses whether the impact of antecedents of user centric e-Government services security on user centric e-Government services security has in reality affected the users or not. From literature (see Section 2.8.1) it can be seen that two technology adoption factors namely perceived ease of use and perceived usefulness provide a way to understand how users have felt while adopting a new technology, in this instance cloud computing. One way to test this aspect is to verify whether PEU and PU of e-Government services has influenced the user trust or not. The following sections discuss this aspect.

3.6 Impact of Perceived Ease of Use and Usefulness on Trust of Users of E-Government Services

From Section 2.8.1, it can be seen that TAM provides theoretical support to understand whether PEU and PU can influence user trust and hence their attitude to accept a technology. Literature shows that when PEU and PU of e-Government services are high then user trust in e-Government is high (e.g. Ayyash et al., 2013). However, there is not much of an evidence to suggest in the literature that shows that researchers have investigated the relationship between PEU and PU of technology on the one hand and user trust on the other, the exception being the

research conducted by Ayyash et al. (2013). Ayyash et al. (2013) argued that researchers have just started to initiate investigations into the implications of trust issues in the domain of e-Government (Warkentin et al. 2002; Carter and Bélanger, 2005; Gefen et al., 2005; Welch et al., 2005; Belanger and Hiller, 2006; Bélanger and Carter, 2008). Much of research that have investigated user adoption of e-Government have treated user trust in e-Government, PEU and PU as associates and not as PEU and PU determining user trust, a lacuna in the research. Thus, on the one hand, there is not much of research that has investigated PEU and PU as determinants of user trust and on the other such an investigation can reveal how trust as an antecedent of user centric e-Government security is affected by PEU and PU of e-Government services. Outcomes through such an investigation has the potential to redefine the way models can be constructed by directly understanding the influence of PEU and PU on user trust which could then imply that technology acceptance behavior indeed could be understood by examining how user trust is affected by PEU and PU of e-Government services. Thus this research relies upon the model tested by Ayyash et al. (2013) and argues that when user perception on both ease of use and usefulness is high then user trust is high. In order to verify this argument the research uses the following hypothesis.

H5a: Perceived ease of use of e-Government services positively influences user trust in e-Government.

H5b: Perceived usefulness of e-Government services positively influences user trust in e-Government.

From the foregoing discussions a conceptual model could be drawn making use of the various hypothesis postulated above. The resulting model is provided in Figure 3.1.

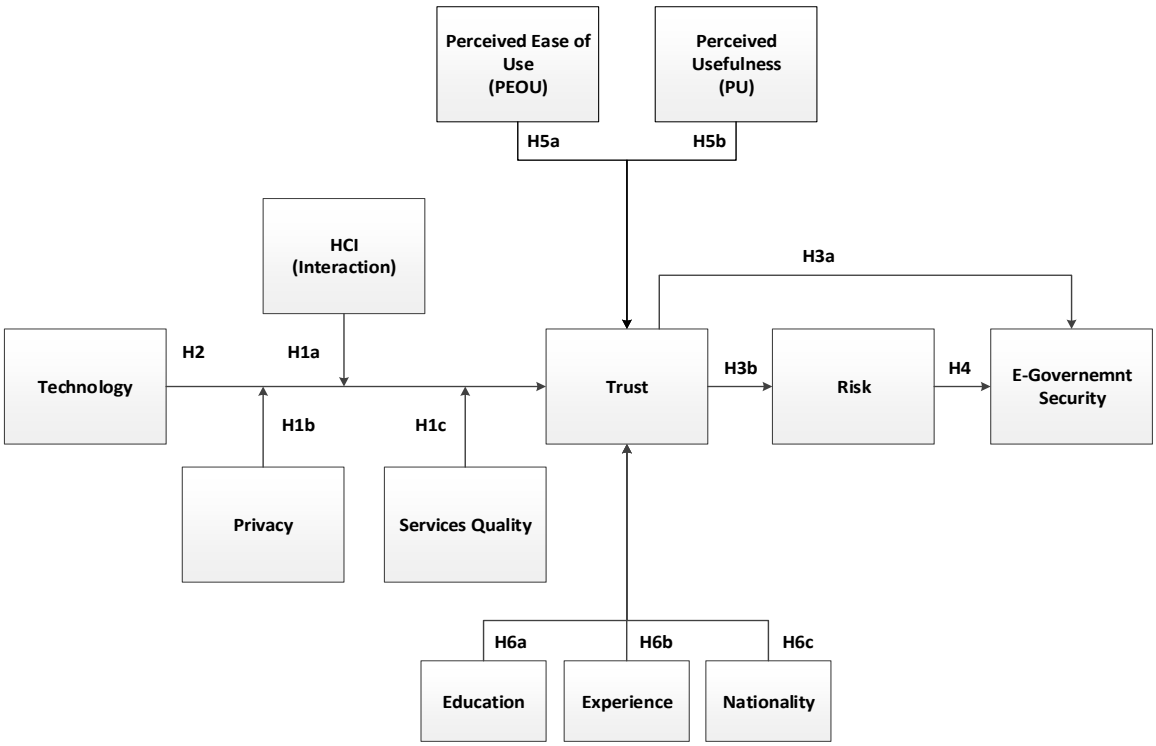

Figure 3.1: Research Model

This model will now be tested to verify each one of the hypotheses and hence the research questions formulated for this research (see Section 1.3) using the research methodology discussed in the next chapter.

3.7 Conclusion

The theoretical framework required to address the gap identified in Chapter 2 has been drawn in this chapter. Assumptions to test the different relationships established with the help of past research have been postulated in the form of hypotheses. Theoretical support for the various relationships has been provided which led to the creation of the conceptual model. Thus in the next chapter the methodology used to collect data for testing the conceptual model has been discussed.

Chapter 4: Research Methodology

4.1 Introduction

The previous chapter (Chapter 3) provided a discussion about the theories and concepts behind the development of the research model and hypothesis. This chapter delineates the research methodology in relation to the research study. This chapter starts by providing a background about the research followed by an explanation about the methodology, comprising the choice of the research philosophy, development of the research design and strategy, data collection aspects and data analysis process.

4.2 Research Background

An e-Government security model was developed to provide an overview of the level of security implemented in the e-Government services from user perspective. This model is not aimed to measure the level of security in e-Government services, rather it provides an insight of the security available with the e-Government portals, which could be used at later stage to increase the level of trust and satisfaction of users toward the e-Government services throughout they conduct e-Government services. Several researchers have developed research models that could be used by the users to comprehend the e-Government security aspects (Shah et al., 2014; Dally, 2006; Kim et al, 2010; Alfawaz et al., 2008; Blakemore and Lloyd, 2007; Accenture, 2005; Bevan, 2006; Johnston et al., 2003). In this context, it can be seen that researchers have used different methodologies to achieve their research aim and objectives set by them, leading to lack of consensus on a particular type of research methodology that could be used in every research. Thus, there is a need to identify the most appropriate methodology that could be used in this research. Further Saunders et al. (2007) suggest that it is necessary to gain knowledge on the research philosophies, which guide the choice of the research methodology. The research philosophies enable the researcher to determine the research approach and research method that need to be applied in this research prior to developing the research framework and design. In addition, the chapter discusses the details of data analysis that define the statistical tests that need to be conducted in this research.

4.3 Research Methodology

Literature shows that researchers including the ones involved in IS research begin their research methodology by explaining their belief about a phenomenon and the type of research philosophy or paradigm they may use to inquire into the phenomenon (Khazanchi and Munkvold, 2002). Using this research philosophy as the basis, researchers are able to identify

the type of data that needs to be collected to provide solutions to the problem statements as well as decide on the research methodology that needs to be employed in this research. In this context, developing a model related to e-Government security aspects requires data to be collected from such subjects who have significant role in both using the e-Government services as well providing service, in order to enable the researcher to acquire inputs for addressing the research question.

Literature review shows that research in the area on e-Government security aspects is inadequate. The type of research methodology developed for this research was based on the research questions to be addressed and the philosophy adopted by other researchers involved in similar topics and found in research publications in the literature relevant to the topic of this research. Additionally it was necessary to develop the research design to verify hypotheses that have been formulated to establish the relationship amongst the different variables based on collected data. These hypotheses were empirically tested to find answers to the research questions.

Furthermore, it was important to decide on the type of research method that was used in this research, to identify the data collection method, subjects, from whom data will be collected, sampling process, instrument design, data analysis methods, testing the reliability and validity of the relationship between variables and establish the hypotheses. Thus, this chapter discusses all the aforementioned aspects in detail to enable the researcher to systematically conduct the research as well as derive findings. To begin with, the following sections discuss the widely used research philosophies, research approaches and research methods in the e-Government literature so the researcher gains knowledge on choosing the most appropriate research philosophy, approach and method.

4.4 Research Philosophy

Literature shows that the widely used research philosophies in information system research are positivism and interpretivism (Orlikowski and Baroudi, 1989; Orlikowski and Baroudi, 1991). Though up to the early 90s of the last century about 96% of IS research adopted the positivist research philosophy, towards the end of the century the percentage of adoption of interpretive research philosophy by researchers had increased to 12%-17% (Walsham, 2006). It is important for researchers to identify the research philosophy they are going to adopt based on the research objectives to enable them achieve the objectives with minimum problems. Research philosophies play a leading role in the success of the research, as the research methodology will depend on the philosophy (Evely et al., 2008). Thus, a brief discussion on the two widely used

research philosophies namely positivism and interpretivism follows. This will enable the researcher to decide on the research philosophy that will be chosen for this research.

4.4.1 Positivism

According to Guba and Lincoln (1989), positivism assumes that an objective reality exists that can be empirically investigated systematically and rationally. Furthermore, Guba and Lincoln (1989) argue that the objective reality is driven by causal laws that apply to social behavior. Another important aspect of the positivist approach is that the researcher and the phenomenon that is under investigation are assumed to be independent, with the researcher remaining an outsider to the phenomenon, neutral and objective (Shanks and Parr, 2003). In addition positivism is built upon general theories that exist and such theories are used to formulate propositions leading to the operationalization of hypotheses that will be empirically tested using large number of samples selected randomly (Shanks and Parr, 2003; Easterby-Smith et al., 2002; Saunders et al., 2007). Chuairuang (2010) argues that the main focus of positivism is to research on a specific phenomenon through observations on social reality that are quantifiable and generalize the findings using statistical analysis. Literature indicates that positivism as a philosophy encompasses deductive approach and quantitative research method (Fitzgerald and Howcroft, 1998). While literature shows that there are number of advantages in using the positivist approach such as generalizability of findings, validating the results, establish the reliability, objectively test hypotheses and provide quantified findings, it is also beset with limitations (Evely et al., 2008). Some of the limitations of positivism include difficulties in quantifying behavior, feelings, perceptions, and attitudes of people and that the knowledge gained through positivist approach is shallow due to the lack of in-depth understanding of the phenomenon due to non-participative approach of the researcher. Further, the view of reality could be changed if the phenomenon is studied using qualitative methods leading to the conclusion that it is important to identify the research method based on the research philosophy so that the researcher attains the expected research outcomes (Moody, 2002). Thus, the researcher should select positivism as the philosophy keeping in view the pitfalls associated with the philosophy. As a next step, the following section provides a brief discussion about the interpretivist philosophy.

4.4.2 Interpretivism

The philosophy of interpretivism is developed on the principle that it is not possible to generalize all phenomena or make predictions but through interpretation and understanding of specific situations (Dahlbom and Mathiassen, 1995). In fact, Dahlbom and Mathiassen (1995) argue that true knowledge needs to be personal. Morgan and Smircich (1980) argue that human beings fix their relationship to the world through a process and interpretive philosophy enables an understanding of this. Kuhn (1977) and Dyson and Brown (2005) argue that the social world is in a state of continuous change as people tend to continue to find multiple realities in relation to an ongoing interchange of perceptions, meanings, feelings, emotions and motives. Thus, there is a need to understand the depth, variety and qualities of a human being's experience, feelings, perceptions and thought process. The researcher is in a position to interpret based on the personal interaction with the subject leading to a greater understanding of the human actions and choices. One of the important advantages of interpretive philosophy is the fact that it is able to study human actions and choices through induction process where prior knowledge to important questions to raise are not assumed (Evely et al., 2008). Furthermore, instead of creating a mechanistically dependent relationship the interpretive philosophy enables the researcher to investigate deep into the phenomenon and leading to development of new theories. Literature shows that interpretive philosophy encompasses the inductive research approach and qualitative research method (Fitzgerald and Howcroft, 1998).

Though interpretive philosophy can enable the researcher to gain an in-depth understanding of a phenomenon, it is criticized to achieve a result that are not independent of researcher bias created due to the proximity of the researcher to the subject and is a major problem that afflicts this philosophy (Parahoo, 1997).

The following Table (4.1) presents a summary of the comparative overview of some major ontological and epistemological philosophical approaches related to IS research paradigms.

Approach	Positivist	Interpretivist
Ontological Assumptions	"Naive Realism" in which an understandable reality is assumed to exist, driven by immutable natural laws. True nature of reality can only be obtained by testing theories about actual objects, processes or structures in the real	Relativist; the social world is produced and reinforced by humans through their action and interaction

	world.	
Epistemological Assumptions	Verification of hypothesis through rigorous empirical testing. Search for universal laws or principles. Tight coupling among explanation, prediction and control.	Understanding of the social world from the participants' perspective, through interpretation of their meanings and actions Researchers' prior assumptions, beliefs, values, and interests always intervene to shape their investigations
Relationship between Theory and Practice	It is possible to discover universal laws that govern the external world.	Generative mechanisms identified for phenomena in the social sciences should be viewed as 'tendencies', which are valuable in explanations of past data but not wholly predictive for future situations
Role of the researcher	Objective, impartial observer, passive, value-neutral.	Interactive; the researcher interacts with the human subjects of the enquiry, changing the perceptions of both parties

Table 4.1: Comparative Overview of Some of Major IS Research Paradigms

(Source: Adapted from Khazanchi and Munkvold (2002)

Table 4.1 shows that both positivist and interpretive philosophies have their own advantage and disadvantages. However, the choice of the research methodology that was chosen for this research has taken into account the above.

4.5 Choice of the Research Philosophy

In the case of the current research, the development of e-Government security model needs the study of the user perception with regard to the e-Government security at a stage prior to the development of their attitude to accept e-Government services. There is a growing body of knowledge, which has addressed the e-Government security aspects. However, the current knowledge available does not adequately address the issue of how users understand the security aspects related to e-Government services at the frontend, in particular when the focus is on HCI

and attitude to accept. A model was developed in this research to examine this issue. In order to the model, it was necessary to collect data from the users as well as service providers pointing towards the use of quantitative research methodology and sampling procedure for the collection of data from the subjects. Thus, positivist philosophy was found to be a more suitable philosophy that could be used in this research.

4.6 Research Methods

There are many types of research used by researchers namely applied and basic research, quantitative, qualitative, descriptive, analytical, predictive, inductive and deductive (Hussey and Hussey, 1997). The research objectives set for this research dictated the choice of a particular research method and the discussions provided in this chapter detail out the rationale behind the choice of the research method.

Majority of the researchers involved in research including e-Government research have used either the quantitative or qualitative research method in their research, although it is not uncommon to come across researchers who have used a combination of both quantitative and qualitative research methods (e.g. Collins, Onwuegbuzie and Sutton, 2006) (see Table 4.3). Much of the research publications found in the literature with regard to development and testing of information security model indicate that many researchers (see Table 4.2) and leading organizations such as the United Nations (UN) have used quantitative research method to collect data for their study like the annual e-Government Readiness report (UNDESA, 2004).

No.	Type of research	Researcher	Model	Type of Research	Year
1	E-Government evaluation: A framework and case study	Gupta and Debashish (2003)	Empirical	Qualitative	2006
2	Multiple behavior information fusion based quantitative threat evaluation	Chen et al., (2005).	Experimental	Quantitative	2005
3	Inclusive eGovernment: survey of status and baseline activities	Millard, J. (2007)	None	Quantitative	2007
4	e-Government Ranking	West (2001)	None	Quantitative	2006

5	Quantitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements	Patel et al. (2008)	Measurement	Quantitative	2008
6	Method for Evaluating the Security Risk of a Website Against Phishing Attacks	Kim et al. (2008)	Experimental	Quantitative	2008
7	A review of information security issues and respective research contributions	Siponen and Oinas-Kukkonen (2007)	Empirical	Quantitative	2008

Table 4.2: Example of IS Security Research Methods

In order to know which of the two research methods could be more appropriate for this research Table 4.3 was referred which provides a comparative between the quantitative and qualitative research methods.

	Quantitative	Qualitative
General framework	• Seek to confirm hypotheses about phenomena. • Instruments use more rigid style of eliciting and categorizing responses to questions. • Use highly structured methods such as questionnaires, surveys, and structured observation.	• Seek to explore phenomena. • Instruments use more flexible, iterative style of eliciting and categorizing responses to questions. • Use semi-structured methods such as in-depth interviews, focus groups, and participant observation.
Analytical objectives	• To quantify variation • To predict causal relationships • To describe characteristics of a population.	• To describe variation • To describe and explain relationships • To describe individual experiences and to describe group norms
Question format	• Closed-ended	• Open-ended
Data format	• Numerical (obtained by assigning numerical values to responses).	• Textual (obtained from audiotapes, videotapes, and field notes).
Flexibility in study design	• Study design is stable from beginning to end. • Participant responses do not influence or determine how and	• Some aspects of the study are flexible (for example, the addition, exclusion, or wording of particular interview

	which questions researchers ask next. • Study design is subject to statistical assumptions and conditions	questions). • Participant responses affect how and which questions researchers ask next. • Study design is iterative, that is, data collection and research questions are adjusted according to what is learned.

Table 4.3: Comparative Overview of Quantitative and Qualitative Research Methods

(Source: Adapted from Bernard, 1995).

The comparison shows that quantitative method is more suitable to address the research questions because, a large number of participants who are users or service providers need to be accessed for this research, from whom data needs to be collected to test the assumptions made for this research. Such data are expected to be collected efficiently using close-ended questions to help test and verify the hypotheses. Furthermore, statistical methods were required to be used in determining the extent to which the hypotheses or the theory used is valid (Cook and Reichardt, 1979). Other important aspects that pointed towards the use of quantitative research method include that the research will be based on hard and reliable quantitative data, use of sampling process (Orlikowski and Baroudi, 1989) and better numerical precision (Verma and Goodale, 1995) that enable researchers to strengthen the analysis of collected data rendering substance to the findings pertaining to the relationships (Balsley, 1970).

Again, keeping in view the fact that the e-Government security model is similar in nature to those developed by other researchers like Yaghoubi et al., (2010), Kim et al. (2010), Chang and Chen (2009) and McNab (2008) with regard to the data collection method, in this research would be useful to employ quantitative research method to collect data from the population that was identified to participate in the research. The other advantage of the quantitative research method is that the outcome of the research will be objective in nature with limited researcher bias and value affecting the data collection method as well as improved chances of validating the interpretation of the research outcomes (Creswell, 2003). If one uses the qualitative method then there is always a possibility of researcher bias creeping into the research outcomes.

In addition to the above, the strengths and weaknesses of the two methods were studied (see Table 4.3)

Method	Strength	Weakness
Quantitative	• Quantitative analysis allows for the classifying of features, counting them, and constructing more complex statistical models in an attempt to explain what is observed.	• Picture of the data, which emerges from quantitative analysis, lacks richness of detail compared with data from qualitative analysis reduced to

	• Findings can be generalized to a larger population. • Allows researchers to analyze more easily because quantitative data is in numerical form. • Provides high level of accuracy. • Compare measures of dispersion. • Allows to present analysis graphically.	numerical form. • Quantitative implementation slow, and needs time compared with qualitative. Can be expensive. • Low response rates. • Not simple to implement. Quantitative often requires computer analysis.
Qualitative	• The qualitative analysis allows a complete, rich and detailed description. • Can be faster when compared to quantitative methods. • Does not reduce complex human experiences to numerical form and allows a good insight into a person‘s experiences and behavior. Qualitative methods can be cheaper than quantitative research. • Ambiguities, which are inherent in human language, can be recognized in the analysis.	• Qualitative data is difficult to analyze and needs a high level of interpretative skills. • Good chance of bias. Hard to draw brief conclusions from qualitative data. • Qualitative data faces difficulties in terms of comparison. • Low level of accuracy in terms of statistics.

Table 4.3: Summary of Strengths And Weaknesses of The Quantitative and Qualitative Methods

(Source: Adapted from Bernard, 2000)

Despite the many advantages that could be derived while using quantitative research, it was important to acknowledge the weaknesses attributed to quantitative research as stated by Bernard (2000) (refer Table 4.3). Bernard (2000) and Fryer (1991) show that using quantitative research can result in over simplification of the problems by the researchers as well as leaving aside the complexities involved with the phenomenon being studied. Likewise, researchers opine that quantitative study is strong on reliability but weak on validity (Cassell and Symon, 1997). The weaknesses attributed to quantitative research method necessitated the researcher to look at the possibility of using qualitative research method by considering its strengths and weaknesses (see Table 4.3). Review of the strengths and weaknesses attributed to qualitative research method showed that a choice between quantitative and qualitative research method must be based on sound rationale.

Study of the strengths and weaknesses pointed out that quantitative research method is more suitable for this research because the strengths of quantitative research method could provide the basis for the researcher to generalize the findings based on a classification of features or factors and analyzing complex models using statistical analysis and derive findings that are objective and value free. If one were to use the qualitative method, it would be difficult to generate complex models for testing using statistical analysis as the data collected will be from

a very small sample and it is not possible to generalize findings from an analysis of the data that is subjective. In addition, lack of time and higher cost of conducting research also limited wider use of qualitative research method. Thus, as explained earlier quantitative research method is the method that was chosen for this research that is in line with research practices of other researcher (Table 4.2). Thus, it is possible to conclude that quantitative research method is more suitable for this research.

Further to the choice of the research method in this research, data were collected from a large number of participants through quantitative research and the researcher emphasized on objectivity. A was strategy used to collect data from the participants. To know what was the strategy used in in this research a detailed discussion on the type of research method employed in this research is provided in the following sections.

4.6.1 Choice of the Type of Research Method

Literature on research method shows that research methods are categorized as exploratory, descriptive and causal (Aaker et al., 2008; Burns and Bush, 2002; Churchill and Iacobucci, 2004; Hair et al., 2003; Saunders et al., 2007; Babbie, 2004). The type of research method or methods used in a research depends on the problem statements (Hair et al., 2003). The problem statements provided in the first chapter led the researcher to develop factors that affect the e-Government security from users' perspective and define the dependent and independent variables. Again, the research objectives set for this research needed extensive data to be collected from the users of the e-Government services to enable the researcher to understand the characteristics of the e-Government security from users' perspective and test the assumptions or hypotheses formulated for this research.

In order to choose the most appropriate research method, it was essential to examine the research aim and objectives. The research aim and objectives required the researcher to understand the needs of the user in developing an e-Government security and it was essential to gain in-sights into the various aspects of the e-Government security as a phenomenon.

According to Babbie (2004), an exploratory research often relies on research such as reviewing literature data, or qualitative approaches such as informal discussions with consumers, employees, and more formal approaches through in-depth interviews, focus groups, projective methods, case studies or pilot studies. In this research, reviewing literature approach was used as part of the exploratory study. It is also a common practice among researchers (e.g.; Chuairuang, 2010) to use the outcome of the initial exploratory study as the basis for designing a larger descriptive study.

Further to an understanding of the user needs through an exploratory study, the researcher needed to describe the characteristic of a particular subject of a population under study and discover the relationship amongst variables affecting the population (Cooper and Schindler, 2003). In this research, the population characteristic was described taking into account the user perception of e-Government security as well as the user ability to interact with e-Government services portals using the concepts of human computer interaction. Further, there was a need to understand the relationship between the users' trust (attitude) and security built into the e-Government services along with the problems associated in interacting with e-Government services portals. These aspects were described using descriptive studies. In addition, there was a need to describe the security aspects pertaining to the e-Government services websites. Eventually, these aspects were studied with an aim to understand the security perceptions of users in terms of the risk perceived by them. The results of the above discussions pointed towards the need for using a descriptive study. According to Aaker et al. (2008), (see also Burns and Bush 2002; Saunders et al., 2007; Creswell, 2003) the best approach prior to writing descriptive research, is to conduct a survey study. This argument is further substantiated in the following sections where the discussion has focused on the type of data that needs to be collected as well as the method of the data collection.

While exploratory study and descriptive study directed the researcher to identify the variables that have effect on the e-Government security as a phenomenon and perhaps help in developing the conceptual model, it was necessary to relate the identified variables and test the relationship using data. Hence, data collection was an important aspect that let the researcher to explain the phenomenon of e-Government security through the analysis of the data collected which pointed toward the use of causal research. Thus, the casual research enabled the researcher to explain the cause and effect relationship among the variables.

The forgoing discussions clearly indicate that exploratory, descriptive and explanatory research methods needed used in this research. It is necessary to mention here that there are different methods under each one of these research methods, which need to be described to give clearer idea on the way data were collected and analyzed. These aspects are covered in the research design section. Before embarking on the research design, it is essential to know the limits within which this research will be conducted thereby defining the scope.

4.6.1.1 Use of Descriptive Study - Survey Method

Leedy and Ormrod (2005) assumed that quantitative research is specific in its surveying and experimentation, as it builds upon existing theories. The methodology of a quantitative research

maintains the assumption of an empiricist paradigm (Creswell, 2003). Usually, quantitative research begins with a problem statement followed by the formation of a hypothesis, a literature review and a quantitative data analysis. Quantitative research employs strategies of inquiry such as experiments and surveys, and enables collection of data in the social sciences using predetermined instruments that yield statistical data (Creswell, 2003). In the word of Williams (2008), several research methods have identified as part of quantitative research. For instance, descriptive research method, correlational, developmental design, observational studies, and survey research are some of the methods used as part of quantitative research. These research methods may also be used in various degrees with experimental and causal comparative research.

In the survey research method, the researcher tends to capture phenomena "at the moment". Creswell (2003) claims that this method is used for sampling data from respondents that are representative of a population and uses a closed ended instrument or open-ended items. On the other hand, Straub et al. (2004) indicate that surveys can be used with other techniques within the same field for instance interviews for the purpose of data collection. Based on the above arguments and the summary of the strengths and weaknesses of some of the research methods provided in Table 4.4, it was seen that survey method is most suitable for this research.

		Strengths	**Weaknesses**
Experimental Research	Researcher has strong control over environment being observed. This research has roots in scientific practice of biologists and physicians, where variables are manipulated over time, associated numeric data collected, and causal or correlation models tested through statistical analysis.	Solution and control of a small number of variables, which may then be studied intensively. Greater realism; less artificial in case of applying within organization or society.	Limited extent to which identified relationships exist in the real world due to over simplification of experimental situation and isolation of such situations from most variables found in the real world.
Survey Research	This research method has its roots in the work of eco no mists and sociologists. Insure vey research, the researcher typically has considerable samples to be analyzed, which suggests the use of questionnaires with easy questions to be answered	A greater number of variables may be studied than in the case of experimental approaches. Description of real world situations. Easier /appropriate generalizations.	Likely, that little insight is obtained. Possible bias in respondents (self -selecting nature of questionnaire respondents) and this can be affected by the moment in time that the research is undertaken.

	for quantitative evaluation. Survey research is typically applied to validate models and hypotheses.		
Case Research	Roots in business studies. Cases are analyzed either to build up or validate models or theories, typically thro ugh collections of textual data by interviews. Essentially merely a means of describing relationships existing in a particular situation.	Capturing reality in detail and analyzing more variables than possible using experiments and surveys.	Restrictive to single event/organization. Difficulty in generalizing, given problems of acquiring similar data from statistically meaningful number of cases. Lack of control of variables. Different interpretations of events by individual researchers/stakeholders.
Action Research	The origins of this research approach rest in socio-psychological studies and work - life issues. Action research is often uniquely identified by the dual goal of both improving organization and participating in the research project.	Practical as well as theoretical outcomes most often aimed at emancipator outcomes. Biases of researcher can be made known.	Similar to case study research, but additionally places considerable responsibility on researcher when objectives are at odds with other groupings. Ethics of the particular research key issues.

Table 4.4: Categories of Research Methodology Strengths and Weaknesses

(Source: Galliers, 1992)

After determining the type of quantitative research method that was used in this research, the research design for this research was developed that specifies the various aspects related to data collection.

4.7 Research Design

According to Burns and Bush (2002), a research is a master plan that specifies the procedure and method of collection of data and its analysis. While it is observed that the research design adopted by different researchers with regard to e-Government research topics differ, by and large it appears that research designs adopted by the researchers involves the defining the research method, type of data that will be collected, the research strategy, the data collection method, sampling process selected, schedule of the plan of actions and the resources needed for implementing the plan. Further, according to Sekaran (2006), research design involves such aspects as the study setting, type of investigation, the level of interference by the researcher, time horizon, unit of analysis, type of sample that will be used, method used to collect data, measurement process by which variables will be measured and the method of data analysis. These aspects suggested by Sekaran (2006) are discussed in the following sections.

4.7.1 The Type of Investigation

According to Lööf and Heshmati (2008), there are two type of empirical investigation namely correlational and causal. Correlational study delineates important variables that are related to the problem rather than delineating the cause of the problem under investigation. This research uses correlational as well as causal studies because it investigates the relationship between e-Government security and variables like HCI, Privacy and Trust that are linked to users of e-Government. Further, the research uses regression analysis to find out the causal relationship between variables representing user interaction with e-Government security aspects. In other word, this research aimed that establishing correlation between users' perspective variables pertaining to e-Government security as well as established the effect of user's perspective as a cause on security.

4.7.2 The Research Setting

As this research is a correlational study, it was conducted in non-forced settings, while rigorous causal-effect studies are done in forced lab settings. Organizational research like e-Government services research can be done in the natural environment where work proceeds normally (i.e,. in non-forced settings) or in artificial, contrived settings.

4.7.3 Unit of Analysis

For this study**,** the unit of analysis is an e-Government services users' within kingdom of Bahrain. The unit of analysis refers to the level of combination of the data collected during the subsequent data analysis stage. In this research, the researcher treated each response as an individual data source.

4.7.4 Time Horizon of the Research

According to Campbell (2004), a study can be either longitudinal or a cross-sectional study. This research study is classified as a cross-sectional or one-time study because it aims to collect data just once, maybe over a period of months in order to answer the research objectives. A cross-sectional study is different than a longitudinal study, where data on the dependent variable is gathered twice or more times to answer the research question.

4.7.5 Extent of Researcher Interference with the Research

This study was conducted in the natural environment of the e-Government facility provided by the Government of the Kingdom of Bahrain. This process was expected to minimize interference by the researcher with the normal flow of the event, which is the e-Government usage, compared to those caused during causal studies.

4.7.6 Data Collection

Data collection is the process of gathering data related to the variables that are inherent part of the hypotheses that enable the researchers to examine the hypotheses that were generated in this study. However, the detailed discussion on data collection is provided in Chapters 5.

4.7.7 Data Analysis

Data analysis is the phase where data are analyzed through statistical means to see if the research hypotheses can be verified. The data analysis in this research includes analysis of quantitative data. The quantitative data analysis used in this research involved analyzing the data collected from the online survey statistically to test the research hypothesis. This processes was analyzed using the statistical tools SPSS 18.0 and AMOS 18.0. Details about quantitative data analyses are provided in chapter 5. As the next logical step, the discussions focus on the research strategy.

4.8 Research Strategy

As stated in chapter one, the overall aim of this research is to investigate the factors that influence e-Government security from user perspective prior to acceptance of the e-Government services and explain the phenomenon. In order to attain the aim it is necessary to adopt a research strategy or strategy of inquiry that define the direction for procedures identified in the research design (Creswell, 2003). As argued by Creswell (2003), strategies of inquiry are applicable to quantitative research designs.

The researcher developed a strategy to conduct the quantitative research method, which included the survey method and self-administered questionnaire, a practice similar to those adopted by many researchers (e.g. Colesca, 2009; Alsaghier et al., 2009) in e-Government research. Although there are other methods such as collecting data through telephone or e-mail, keeping in mind the effort that will be required to follow-up with a high number of respondents and the lack of time, the researcher adopted the survey method using self-administered questionnaire. Furthermore, the researcher used the strategy of posting the questionnaire online to enable accurate collection of data in a shorter period of time. Although there were pitfalls in collecting data through online mechanism such as lack of availability of online facilities for respondents or lack of clear understanding of the instructions, the researcher overcame these pitfalls by providing easily understandable instructions to answer the questionnaire and contact details so that respondents could clarify any point. Further, the questionnaire was provided in English language.

Further to identifying the research method as part of the strategy, it was important to discuss the development of the data collection tool as part of the strategy. According to Sekaran (2006) interviewing, administering questionnaires and observation of phenomena or people are the widely used data collection methods in survey research. Although there are other researchers (Veal, 2005), who argue that questionnaires and interview are specific methodologies identified under survey research, it can be seen that questionnaire is considered as an important tool in empirical research (Creswell, 2003). As far as this research is concerned, the development of the questionnaire has been dealt with in detail in Sections 5.3 (Chapter 5). In addition, alongside collecting primary data through the questionnaire, it was important to collect secondary data for instance from already published literature, a strategy used by other researchers also (e.g. Ticehurst and Veal, 2000). With regard to the details on the implementation of the research strategy the same has been discussed in Chapters 5. The next step in the research design is the data collection aspect that is discussed next.

4.9 Data Collection

As mentioned in section 4.8, there are two kinds of data namely the primary data and the secondary data. The secondary data was collected from various published literature that helped the researcher to gain knowledge on the various indices as well as methods to compute indices with regard to e-Government security. The researcher developed a questionnaire for collecting primary data by adapting previously developed questionnaires found in the publications of previous researchers involved in the field of e-Government security. In addition, data was collected from a target population for this research, the details of which are addressed in Chapters. After determining the data collection process, as part of the research design the data analysis aspect that was adopted in this research is discussed next.

4.10 Data Analysis

While the foregoing discussions have addressed the issues of the choice of the research method, research design and research strategy that was adopted in this research, an important part of the research design, which is the data analysis process, needs to be discussed.

The data analysis with regard to the quantitative research method adopted in this research follows the procedure given below and these procedures were broadly applied to analyze the conceptual model. With regard to the pilot survey the data analysis procedure dealt with testing the reliability and validity of the research instrument only. The main purpose of the pilot survey was to establish the content validity of the questionnaire, improve such things as the questions,

format and scales and include the comments of the respondents of the pilot study into final research instrument (Creswell, 2003). In addition, the pilot survey examined the contextual factors identified in Section 2.6 namely user education, user experience, user nationality and technological factors for their influence on the relationship between user trust and user centric e-Government security and to know whether they affect the user trust. Out of these technological factors have been used as the core concept (see theoretical framework, Section 3.3) that determines how user centric e-Government security is affected when changes take place in them keeping in view the intervention of trust and risk as factors. However, the remaining three factors namely user education, user experience and user nationality were only used as controlling factors of the relationship between trust and user centric e-Government security. The reason for this is that (see explanation in Chapter 3, Section 3.5) these three factors have been widely used in the literature to explain the population characteristics and those factors have been just used as constants while explaining how user centric e-Government services security is affected if technological factors change. Thus, there is only a need to test the significance of their influence on the relationship between any of the antecedents of user centric e-Government security and user centric e-Government security. In this thesis, trust has been chosen as the antecedent of user centric e-Government security and the control factors were be tested for their influence on the relationship between trust as an antecedent of user centric e-Government security and user centric e-Government security. Such a test was carried out at the pilot survey stage itself as outcomes at the pilot survey stage enabled the researcher to test the hypotheses pertaining to the relationship between the contextual factors and trust. Outcomes of this test could be extended to include other antecedents of user centric e-Government security identified in this research namely technology and risk. Details of the test are provided in Section 5.6 in Chapter 5. Thus while explaining whether the contextual factors have influence on the relationship between trust and user centric e-Government security or not, such an explanation is expected to inform the research on what kind of influence they exert on the relationship between trust and user centric e-Government security. Such knowledge could be useful in dealing with contextual issues separately so that user security could be maximized when such factors come into play.

Further, in order to test the reliability of the instrument used in this research, the researcher used Cronbach's coefficient alpha, which is one of the most popular methods used in research (e.g. Sekaran, 2006). Reliability measures the extent to which the results of a research could be the same if the research was conducted again at a future date or with different samples of the same population (Ticehurst and Veal, 2000). Reliability test is also a test of the consistency of the responses given by the respondents to all the questions in a measure. In addition, Sekaran (2006) argues that reliability provides a measure of the degree to which an item can be

considered to be an independent measure of the same concept when related with another item measuring the same concept. In general researchers (e.g. Sekaran, 2006) opine that reliability measures less than 0.6 are considered to be poor, those around 0.7 as acceptable and values exceeding 0.8 as good. The maximum value of reliability that could be achieved by measuring Cronbach's coefficient alpha is 1.0. As Cronbach's coefficient alpha approaches 1.0, reliability is considered to be better. However, in general many researchers argue that the widely accepted lower limit of Cronbach's alpha is 0.7 (Robinson et al., 1991). However, for exploratory research some researchers argue that the value of Cronbach's alpha at 0.6 as lower limit is acceptable (Robinson et al., 1991).

Although there are other methods of reliability measures that are used by researchers such as Kappa Coefficient (Haley and Osberg, 1989) those measures are not widely used in e-Government research unlike Cronbach's alpha. Thus in this research Cronbach's alpha was used to understand the internal consistency as well as the reliability measures.

Furthermore, other measures of internal consistency were also used in this research as a measure of validity namely the inter-item correlation (correlation between two items) and item-total correlation (correlation of an item with the summated scale of the construct) (Hair et al., 2006). These values were also reported in this research although the significance of these measures to the research is provided in the following discussions addressing the validity of the instrument.

4.10.1 Validity

Validity is the extent to which a research instrument measures what it is expected to measure. For instance, in measuring attitudes and behavior validity indicates the extent to which a certain instrument that is used to measure the attitude or behavior actually measures the attitude or behavior. Researchers (e.g. Ticehurst and Veal, 2000) argue that there are always doubts about the true meanings of responses obtained through surveys. Such doubts can be clarified through validity tests. For the pilot survey, the internal consistency tests namely inter-item correlation and item-total correlation were used to test the validity of the research instrument (Robinson et al., 1991). According to Robinson et al. (1991), inter-item correlation values greater than 0.3 are commonly accepted by in research while item-total correlation values need to be in excess of 0.5. Further, according to Cohen (1988), inter-item correlations for both positive and negative values can be classified as small correlation (0.1 to 0.29), medium correlation (0.3 to 0.49) and large correlation (0.5 to 1.0). Considering the fact that these values are widely used by researchers as acceptable values, in this research also these values have been taken as reference. Furthermore, according to Sekaran (2006) there are a number of types of validity tests that include content validity, criterion validity and construct validity. Each one of these tests is

described in the following sections. Prior to describing the validity tests in the following sections, it must be noted that the researcher used correlational analysis and analysis of variance (ANOVA) to test the relationship between the contextual factors and trust. This method is a commonly used method to test the influence of factors like contextual factors on the relationship between to other variables (Janssens et al., 2008). This test is reported in Section 5.3.2 under Chapter 5.

4.10.2 Content Validity

According to Hair et al., (2006) content validity, also called face validity, tests the relationship between single items and the construct or the concept it purports to measure and such a test is carried out through ratings by experts and pre-tests with different sub-populations. Details on how the content validity was tested in this research are given in Chapter 5.

4.10.3 Convergent Validity

Also called criterion validity or predictive validity, convergent validity assesses the extent to which items that act as indicators of a specific construct converge, in other words share a high proportion of variance in common (Hair et al., 2006). Convergent validity is tested using correlational analysis (Zikmund and Babin, 2007). Detailed discussion on how convergent validity is tested in this research is provided in Chapter 5.

4.10.4 Construct Validity

According to Sapsford and Jupp (2006), construct validity measures the extent to which all the items measure the same thing and enables the researcher to explore the structure of a scale to see if the items measure the same thing. Further, construct validity can be tested through correlational analysis (convergent and discriminant validity) (Straub et al., 2004) and factor analysis (Burton and Mazerolle, 2011). Details on how the construct validity is tested are provided in Chapter 5 for both the pilot survey as well as the main survey.

The foregoing discussions provide an idea on the statistical tests that were conducted till the pilot survey stage. However, there were other statistical tests that were conducted by the researcher during the main survey data analysis stage to not only establish the reliability and validity but also verify the hypotheses. These data analysis tests are discussed next.

4.10.5 Main Survey Data Analysis

The main survey data collected through the questionnaire for the conceptual model was subjected to rigorous statistical tests. According to Zikmund and Babin (2007) data coding is an important step needed for storing data while using SPSS. Furthermore, data was edited by checking the completeness of data using frequency distribution using SPSS. Coding was done

using alphanumeric characters. Each item in the questionnaire as the index list was coded. The coding sheet is discussed in Chapters 5. Chapter 5 addresses the coding related to the conceptual model and the items used to measure each one of the constructs in the model. The data was further screened and cleaned for any omissions by the respondents while answering the questionnaire online using descriptive statistics in SPSS. After correcting errors if any, data sheets and files were created in SPSS setting the basis for analyzing the data. Using SPSS for analyzing data is a standard practice widely used in empirical research.

Data analysis comprised descriptive statistics generated by SPSS including minimum, maximum, frequency, percent, mean, median, standard deviation, skewness, kurtosis and Pearson correlation and testing the internal consistency aspects pertaining to reliability measurement. Further the validity tests were conducted followed by SEM using AMOS 18.0. In order to use AMOS 18.0 to address the SEM, data needed to be managed and certain assumptions needed to be examined for their validity.

Median was computed using the frequency table generated by SPSS 18.0 and provides the central tendency of the collected data (Bakker and Gravemeijer, 2006). Central tendency provides knowledge on the point on the measurement scale around which the responses are distributed (Bakker and Gravemeijer, 2006). Similarly, standard deviation indicates the dispersion of the response around the normal indicating the farthest point of the response recorded from the normal. Standard deviation provides a measure of normality of the collected responses (Bower, 2003). In fact, normality in multivariate analysis using SPSS 18.0/AMOS 18.0 is an important requirement for many tests (Hair et al., 2006). Normality tests include checking for missing data, multivariate outliers, skewness, kurtosis and multicollinearity. Each one of these tests is described next.

4.10.6 Missing Data

Missing data were checked using the frequency table generated by SPSS. Variables or cases with missing data will be deleted and not used as part of the data analysis if the percentage of missing data in the responses is less than 50% (Hair et al., 2006). However, missing data in single cases or observation under 10% can be ignored if the missing data occur in a random fashion. In addition, use of AMOS 18.0 for SEM requires complete data (Arbuckle, 2006). Hence, it is important to check missing data. Details are discussed in next chapter.

4.10.7 Outliers

After cleaning the data for missing data, the next step that was adopted was checking the outliers. Outliers are those observations that create suspicion, as the observations could be either

much smaller or larger in comparison to the majority of the observations (Cousineau and Chartier, 2010). According to Meloun and Militky (2001), Mahalanobis distance can be used to determine outliers using SPSS. Mahalanobis distance is computed using the formula D^2/df where D is the mean of multivariate outlier detection that is used to measure the multidimensional position of each reading or observation compared with the center of all readings or observations on a set of variables. df denotes the degrees of freedom. According to Hair et al., (2006), D^2/df values should be lower than 4 on large samples. This reference value was used in this research based on the recommendations of other researchers like Hair et al., (2006). Any response or case whose Mahalanobis distance is higher than 4.0 were deleted as recommended by Pallant (2010) as extreme cases are potential problem cases and could are counter to the objectives of the analysis as they have the potential to distort statistical tests (Hair et al., 2006). The detailed discussion on Mahalanobis measurement is provided in in Section 5.4.5.

4.10.8 Multivariate Normality

Further to detecting the existence of outliers, the next step taken was to test the multivariate normality of data. According to Hair et al. (2006), normality indicates the normal distribution of data, a reference used in statistical methods. According to Gravetter and Wallnau (2013), data are considered to be normal if the greatest frequency of scores in the middle of a bell shaped symmetrical curve alongside smaller frequencies approaching the extremes. Severity of non-normality could be ascertained based on the shape of the normal curve and has a bearing on the sample size. There are two tests that are conducted to assess the normality. One is skewness and the other is the kurtosis (Hair et al., 2006). Skewness provides an idea about the symmetry of the data distribution while kurtosis shows the extent to which the distribution of data is peaked or flat (Pallant, 2010). Negative kurtosis will manifest as a flat distribution where as positive kurtosis will manifest as a peaked distribution. Similarly, a distribution shifted to the left of the normal indicates positive skewness while a shift to the right indicates a negative skewness (Weisstein, 2004). According to Weisstein (2004), a skewness value of 1 is considered to be moderate. Similarly, Holmes-Smith et al. (2006) argue that kurtosis values less than 1 can be neglected whereas values in the range of one to ten can indicate moderate to severe non-normality. However many researchers argue that generally acceptable value of skewness is within 1.5 while for kurtosis it is within 3.0 (Li, 1999). Furthermore, sample size also has been found to affect normality with larger sizes reducing the negative impact of non-normality (Hair et al., 2006; Pallant, 2010). Although Hair et al. (2006) contend that small sizes contribute to serious non-normality problems, it is also pointed out that as the sample size reaches 200 or more the effect of non-normality diminishes. A complete discussion on skewness and kurtosis is provided in Section 5.4.

4.10.9 Multicollinearity

In addition to the above tests, another important test was conducted to examine whether multicollinearity exists to find out whether correlation amongst variables is very high (Pallant, 2010). According to Pallant (2010), correlations between variables exceeding 0.8 or 0.9 are causes of concern as it indicates multicollinearity. This aspect has been discussed in detail in Section 5.5.6.

4.10.10 Structural Equation Modeling

Further to the discussions on descriptive statistics, the next step undertaken was the structural analysis of the model. This was carried out using Structural Equation Modeling (SEM). According to Hair et al. (2006), SEM provides a facility to compute and assess a series of interrelated dependence relationships at the same time. Since the main idea of this research is to develop an e-Government security conceptual model that comprises multiple variables and a multivariate technique that enabled the researcher to test the meaning and such a technique was provided by SEM (Jöreskog, 1993). SEM puts together aspects concerning multiple regression (causal relationship) and factor analysis (factors with many variables) that led the researcher to assess the various relationships that are interdependent in the model simultaneously (Hair et al., 2006; Schumacker and Lomax, 1996).

In addition, SEM enabled the researcher to conduct path analysis to examine the structural relationship amongst the various constructs (Sharma, 1996). An important factor that contributed in leaning towards SEM is the set of advantages it offers over other methods while analyzing the model like confirmatory approach to data analysis, estimation of error variance parameters, usage of both observed and unobserved variables in analysis and modeling multivariate relationships (Byrne 2001, 2010). SEM was carried out in this research using SPSS 18.0 and AMOS 18.0 computer software packages. A detailed discussion on SEM relevant to the data analysis is provided in Section 5.8. Furthermore, although SEM uses confirmatory factor analysis, which serves the purposes of inferential statistics, in this research even descriptive statistics (e.g. exploratory factor analysis), were also used as part of the multivariate technique. Each one has a distinct purpose and has been discussed in the following sections.

4.10.11 Factor Analysis

In this research factor analysis was carried out using Confirmatory Facto Analysis (CFA). According to Janssens et al. (2008) CFA is an application of SEM. CFA enables the researcher to conduct tests on what are called measurement models with latent variables (latent variables are those that are not immediately observable). CFA also enabled the researcher determine the

number of underlying dimensions leading to the next step (e.g. path analysis) of assessing which relationships may be found between these dimensions. In addition to the above CFA offers a number of advantages, which include assessing the good fit between the model and the data, providing paths between a factor and only a few variables, correlation of measurement errors and correlation of factors (Janssens et al., 2008). However, CFA needs special computer software packages such as the AMOS 18.0 without which it may not be possible to conduct CFA. A more detailed discussion on CFA pertaining to this research is provided in Section 5.7.

After discussing the SEM and factor analyses used in this research, it is important to gain an understanding of the important steps needed to be followed to make decisions regarding the reliable constructs used in the models. Two important tests are commonly recommended (Janssens et al., 2008). One is the unidimensionality Ten Berge and Sočan (2004) and the other is the common method bias (average variance extracted) (Bagozzi and Yi, 1988). Unidimensionality refers to the existence of only one underlying dimension in common (Janssens et al., 2008). Common method bias indicates the systematic effect exerted by common methods shared by measures under two different constructs on the observed correlation between the measures (Podsakoff et al., 2003). For instance if items under Construct A and Construct B share the same 5 point likert scale to measure attitude, such a commonality could exert pressure on the observed correlation between the measures. Such a bias could result in potentially misleading conclusions Podsakoff et al. (2003). Unidimensionality is measured using AMOS 18.0 and is tested by examining the values under the table Regression Weights details about which have been provided in Section 6.11. Similarly, common method bias was measured using the Average Variance Extracted (AVE) test (Bagozzi and Yi, 1988). Details about the examination of common method bias are given in Section 5.11.

4.11 Ethical Consideration

In this research, ethical aspects required consideration during the data collection phase. As part of the ethical requirements, participants in the online survey were assured that full privacy would be maintained with regard to their responses and will be kept confidential and will be destroyed so that they do not fall into the hands of others researchers. In addition participants were informed that the participation was strictly voluntary and they have the right to withdraw from the survey at any stage they considered it as fit. Furthermore participants were fully informed about the purpose and nature of the research and were administered the questionnaire only after they had consented. A covering note was made at the beginning of the survey to inform the participants about all the details given above (See Appendix B, B1). The survey was conducted through online method.

4.12 Methodology Outline

The data collection and analysis processes of this research are outlines in Figure 4.1.

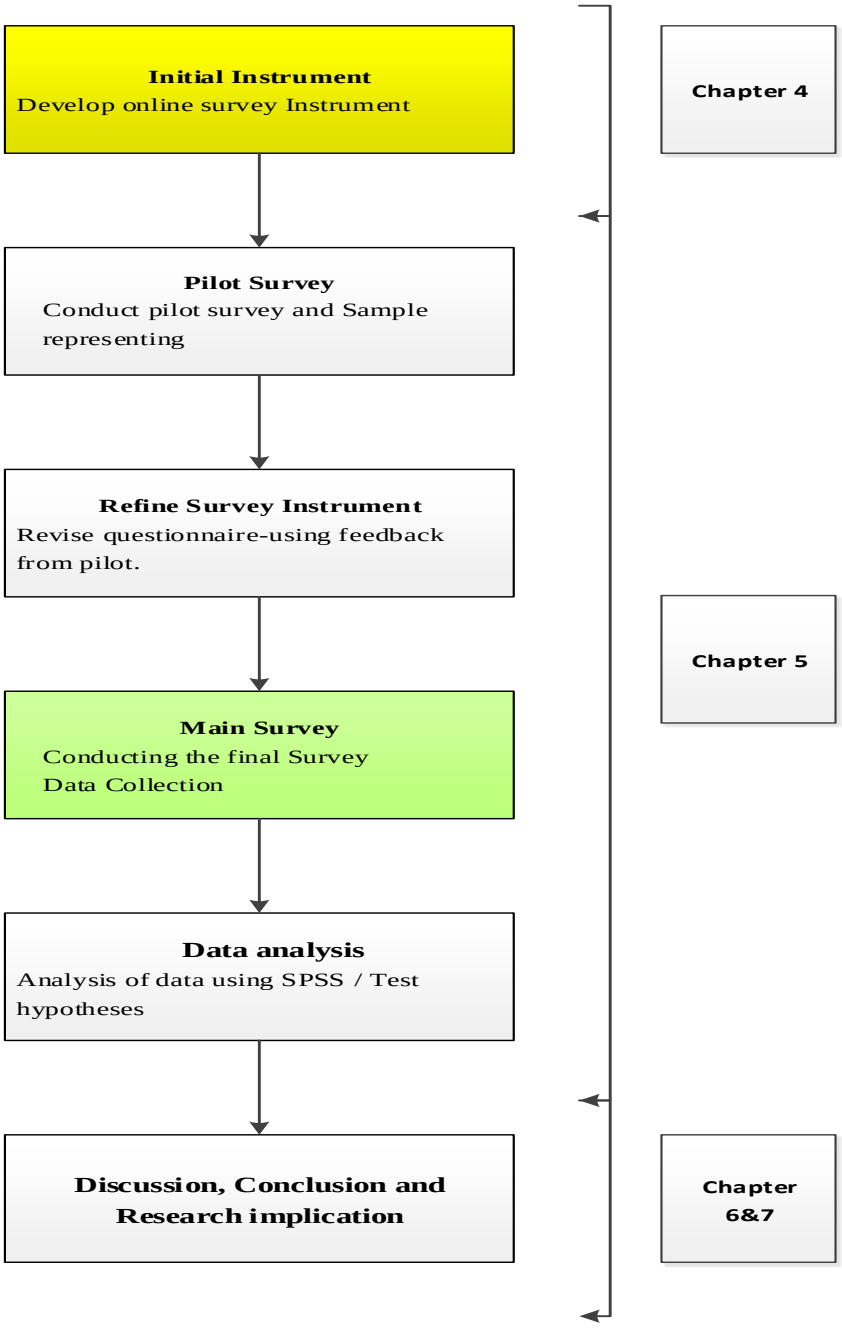

Figure 4.1: Research Methodology Outline

4.13 Summary

This chapter has discussed in detail the epistemological and ontological stance adopted by the researcher. In addition, the chapter has critically looked at the research approaches and methods found in the methodology literature and chose the most suitable approach and method for this research. Positivist epistemology that employs an objective ontology, deductive research approach and quantitative research method was adopted. The research design and research strategy for data collection used was survey research design, sampling process and self-administered questionnaire. As part of the research design, the chapter dealt with the data collection and analysis aspects. Thus, this chapter sets the basis for analyzing the data dealt with in the next chapter.

Chapter 5: Empirical Research: Data Collection and Analysis

5.1 Introduction

The earlier chapter 4 discussed the research methodology of this research. It discusses the various aspects related to data collection and analysis as part of the research design and strategy. This chapter aims to present the finding and analysis methods of the quantitative data of the pilot study conducted in this research, as well the finding and analysis of the data that were obtained from the main survey instrument conducted by online users examining the e-Government security model. Moreover, in order to understand the aim of this chapter, the following objectives are achieved; the researcher conducted a statistical analysis on the pilot study using data collected from online users and examined the data for reliability test, factor loading and correlation among the constructs identified in Chapter 3 and eliminating the items that found statistically unproven before conducting the main survey. The researcher then conducted confirmatory factor analysis (CFA), testing the goodness of fit and path analysis, follows by calculating the average variance extracted, then computing the construct reliability and the structure equation modeling (SEM) for each set of collected data related the main survey, ending with performing unidimensionality test and tackle the issue related to common method bias. Chapter summary is provided in the end. Prior to the discussion about the finding of the pilot study, the discussion about the process of developing the data collection instrument is provide next.

5.2 Questionnaire as the Method for the Main Survey

This section dwells on the development of the questionnaire. According to (Sekaran, 2006) a questionnaire comprises a set of written questions that are pre-formulated to which respondents provide their responses, commonly using closely defined choices. Again, questionnaire was used as the main survey instrument in this research because it offered a mechanism to collect data that was efficient in a situation where the researcher had knowledge on what is required and how to measure variables under study. Other reasons for using the questionnaire include:

a. Studies conducted in the field and experimental designs usually use questionnaire as the method to collect data (Sekaran, 2003).
b. Where quantified data are required pertaining to a particular population like the users of the e-Government, questionnaires are used to collect data and are accepted as source of information (Ticehurst and Veal, 2000).

Furthermore, questionnaire enabled the researcher to administer it to a large number of individuals concurrently and was found to be a less expensive and less time-consuming method in comparison to other methods such as interviews. Although there is a limitation of using questionnaires with regard to confidentiality issues, such problems were overcome through informed consent and anonymity (Hussey and Hussey, 1997).

5.2.1 Development of the Questionnaire

From literature review, information was gathered for developing the questionnaire for testing the hypotheses related to the conceptual model. Themes developed through the data analysis of information in e-Government literature to identify key variables while developing the questionnaire. The main aspects that came up through literature review were human computer interaction, information privacy, e-Government service quality, e-Government security, perceived ease of use of e-Government services, perceived usefulness, trust in e-Government services and risk in using e-Government services. Although some other aspects such as e-Government services satisfaction, transparency, accountability, awareness, usability and the like, it was seen that these aspects could be consolidated under broad factors using e-Government literature to enable avoid any repetition or similarity in the aspects. As such to enable the researcher to optimize on the key variables required for developing the e-Government security model, it was essential to ensure that only the key variables are considered while the others which were either similar in nature or representing the an aspect in a different way were ignored. The reason being the consolidation of the aspects ensured that those aspects that were ignored are represented by the key variables.

5.2.2 Questionnaire Design

The questionnaire that emanated from information from the literature for testing the hypotheses related to the conceptual model is provided in Table C1 in Appendix C. The questionnaire was designed around the key variables identified through the abovementioned process using English language. English was used as the language as it is a widely used language in the Kingdom of Bahrain. Previously developed and validated questionnaires that measured the key variables in similar research were examined to find out whether those questionnaires could be adopted for this research. The outcome of such an examination enabled the researcher to identify the questionnaires developed by other researchers that were already tested and established. The Table C1 in Appendix C provides the complete information about the questions that were extracted and adapted from previous research to measure the key variables identified above.

In addition to the above, 7-point Likert scale was used to measure the variables which is in line with the arguments suggested by other researchers for instance Colesca (2009) and Chang and

Chen (2009), who have conducted similar research and measured key variables namely overall quality of service and privacy. However, where pervious researchers (e.g. Kim et al., 2010; Pu and Chen, 2006 and Alsaghier et al., 2009) have used 5-point Likert scale to measure variables identified in this research namely human computer interaction, trust, risk, perceived ease of use and perceived usefulness, a modification was inserted into the questionnaire by way of changing the scale to a 7-point one to ensure consistency and better accuracy (Finstad, 2010).

5.2.3 Questionnaire Validation

The questionnaire developed above went through a trial run conducted on a group of respondents, which enabled the researcher to detect problems in the questionnaire such as instructions to answer the questionnaire, design of the questionnaire, difficulties faced by respondents in understanding the questionnaire, ambiguity and bias in questions. The respondents were chosen from the population of users of e-Government services who were the final target population for this research. According to Zikmund and Babin (2007), first test group may consist of 25 to 50 subjects. In this study, around 30 users were randomly chosen from the Kingdom of Bahrain who were using the e-Government services. 15 questionnaires were returned. Wordings in some items were changed to ensure better and clearer understanding based on the feedback given by the respondents. The revised questionnaire was sent to two researchers, two practitioners in the e-Government authority of the Government of Bahrain and two academicians who further suggested some changes to the contents of the questions. These changes were incorporated and the questionnaire was then used to conduct the pilot study.

5.3 Pilot Study

The pilot survey was a useful step that enabled the researcher to detect weaknesses in the data collection instrument developed to test the hypotheses related to the conceptual model. For the pilot study, participants were drawn from the target population and the process of data collection was simulated in way similar to that used in the main survey. For instance if the survey is to be conducted online in the main survey, then in the pilot survey also the data collection should be through the online process an argument supported by other researchers (Cooper and Schindler, 1998). Furthermore, a pilot survey is a small-scale version of the larger survey and hence could be related to any type of research procedure. The main purpose of pilot survey has already been outlined under Section 4.10.

The pilot survey was conducted in the Kingdom of Bahrain using the online process. Online process has been accepted as a means to collect quantitative data by researchers (Nesbary, 2000). As outlined under Section 4.10 the researcher took necessary pre-cautions while

conducting the online pilot survey. The questionnaire was posted on a professional website, which provided the web link at which the questionnaire was posted online. The web link was sent to a total of 100 participants by e-mail. These participants were users of the e-Government services provided by the Government of the Kingdom of Bahrain randomly chosen from the population of Bahrain. Follow-up calls were given to request them to participate in the survey. Ethical considerations prescribed Brunel University were followed as per the approval given by the ethical approval committee of Brunel University. Participants were informed through a covering note that the participation in the survey is voluntary and that the information provided by them will be maintained in strict confidence and used only for the purpose intended.

Out of 100 respondents, 63 responses were received out which 52 were valid. The collected data were then analyzed for reliability and validity as described in Section 4.110. The following sections provide details of the outcome of the reliability and validity analysis. Prior to testing the reliability and validity of the pilot data the descriptive pertaining to the demographic and contextual factors are reported in Table (Pilot). This is needed in order to ascertain the acceptability of the data for testing the relationship between the control variables namely education of users, experience of users and nationality of users on the one hand and trust of user on the other.

		Gender	Age	Occupation	Education	Income	Experience	Country
N	Valid	52	52	52	52	52	52	52
	Missing	0	0	0	0	0	0	0
Mean		1.87	3.06	1.35	4.58	3.62	4.50	2.67
Median		2.00	3.00	1.00	5.00	4.00	5.00	2.00
Std. Deviation		.345	1.018	.764	.572	1.374	.804	1.937
Variance		.119	1.036	.584	.327	1.888	.647	3.754
Range		1	3	4	2	4	3	6
Minimum		1	2	1	3	1	2	1
Maximum		2	5	5	5	5	5	7

Table 5.1: Descriptive of Demographic and Contextual Variables

From Sections 4.10 in Chapter 4, it can be seen that the three variables education, experience and country (nationality) have been chosen as the control variable. Table (5.1) shows that the standard deviation for the three variable ranges between 0.572 and 1.937 showing that data fall within two standard deviations and hence normality of distribution of data could be assumed. As explained in Section 4.10 the three variables were correlated (not regressed) with the nine items of trust to examine whether they have statistically significant relationship with trust (an antecedent of trust and hence could be considered as representing security see Section 4.10) or not. This is explained later in Section 5.3 and 5.6 as while conducting such a test, data collected using items measuring trust need to be brought in for analysis only after verifying their

reliability and validity. The reason for not conducting regression to test the relationship between control factors and trust is that the focus of this research is on only one major contextual factor that is technology (not all contextual factors) and its influence on user centric e-Government services security. Hence the analysis related to control factors that are also contextual in nature, is only a minimum and the aim is to report whether any relationship between the control factors and any of the factors that could be related to e-Government security which in this research happens to be trust, exists or not. Existence of any relationship could imply that the control factors could exert some pressure on e-Government services security.

5.3.1 Reliability

As mentioned in Section 4.10 reliability analysis was carried out using Cronbach's alpha. The acceptable value of the reliability parameter alpha was fixed at 0.7 or above, the rationale for which has been provided already in Section 4.10 Cronbach's alpha was computed using SPSS version 18.0. The results of reliability test are given Table 5.2. It can be seen that alpha value for all the constructs exceeds 0.7, thus confirming that the data are reliable. Further to testing the reliability, the internal consistency of the questionnaire was also tested using item-item correlation and item-total correlation, a practice suggested and followed by many researchers (e.g. Olatunji et al., 2007; Nunnally and Bernstein, 1994). The minimum acceptable values of correlation for item-item and item-total measurement were fixed at 0.3 or above and 0.5 or above respectively. The reason for choosing these values has been already provided under Section 4.10. It can be seen from Table 5.2 that five items (PEOU4, EHCI12, ET2, ER3and ER4) contributed to lower values of correlation. The list of items and the constructs they measure has been provided in Appendix C, Table C1.

No.	Construct	No. of Items	Cronbach Alpha	Inter-Item Correlation Matrix	Item-Total Statistics	Low correlation value
1.	PEOU	4	0.741	0.188 - 0.717	0.288 – 0.692	PEOU4
2.	PU	4	0.830	0.356 - 0.709	0.567 – 0.731	
3.	Interface (HCI)	4	0.702	(-0.015) - 0.697	0.083 – 0.671	EHCI12
4.	Privacy	5	0.899	0.453 - 0.825	0.637 – 0.835	-
5.	Service Quality	4	0.831	0.496 - 0.724	0.607 – 0.736	-
6.	Technology	8	0.894	0.312 – 0.798	0.617 – 0.724	-
7.	Trust	9	0.891	0.042 – 0.805	0.178 – 0.844	ET2
8.	Risk	8	0.921	0.246 – 0.825	0.453 – 0.844	ER3and ER4
9.	Security	5	0.895	0.506 – 0.744	0.665 – 0.799	-

Table 5.2: Pilot Survey Finding Summary

The results of the pilot survey clearly indicated that the reliability of the instrument is acceptable with Cronbach's alpha for almost all the items under each construct exceeding 0.7. However, with regard to the internal consistency aspect, results indicate that there were certain

items under some constructs whose inter item-correlation and item-total correlation is weak. For instance, EHCI12 under the construct HCI had poor correlation with the rest of the items and hence could be considered for deletion from the instrument. How these concerns were tackled is given in the next section.

Further to analyzing the reliability aspect, validity tests were conducted on the data. Validity tests included testing the content validity, convergent validity and construct validity. Details on how to test the validity of the data as well as the minimum acceptable values have already been discussed in Section 4.11.2.1. Thus, the following sections provide the validity tests conducted at the pilot survey stage.

5.3.2 Validity

It has been already explained in Section 4.10.1.1 why there is a necessity to test the validity of the questionnaire at the pilot survey stage. Validity measures included content validity, criterion-related validity and construct validity. Validity was assessed through ratings obtained from experts in the field of e-Government security as well as pre-tests conducted on the sub-population (see Section 4.10.1.1) (Hair et al., 2006). Six experts were asked to examine the content validity (face validity) and to give feedback on the contents at the item level under each construct, of the questionnaire using their judgments. The experts were requested to check whether items correspond to the concepts they purport to measure. Based on the feedback minor adjustments were made to the content. Construct validity was checked using correlational analysis (See Section 4.10.1.3 and Section 4.11.2.4). Both convergent and discriminant validity are considered to measure construct validity (Zait and Bertea, 2011). Convergent validity was measured using inter-item correlation and item-total correlation. As mentioned section minimum acceptable values of inter-item correlation and item-total correlation were fixed at >0.3 and >0.5 respectively.

As explained in the previous section it can be seen from Table 5.2 that there were cases of item-item correlation and item-total correlation that caused concern because correlation values were lower than the reference level fixed for this research. However since this is only the pilot review with the sample size being very low, it was decided that the researcher will retain the item and check its validity in the main survey with a larger population size before making any decision on its retention or deletion from the instrument. This argument applies to all the items that had correlation problems in respect of both item-item and item-total correlation values. This phenomenon is a common amongst researchers who have applied quantitative research method and used survey research and self-administered questionnaire (Duncan et al., 2009).

At the pilot survey stage, it can be seen that the reliability, content validity and convergent validity have been found to be acceptable and it was concluded that the instrument is ready for use in the main survey. As far as the discriminant validity was concerned, it was decided that this test would be applied at the main survey data analysis stage as one form of construct validity (that is convergent validity) has already been established. Further to assessing the reliability and validity of the instrument, the researcher conducted the correlation analysis between experience, education, nationality and nine items of the construct trust (see Figure contextual). Correlation analysis provided the initial confirmation on which of the nine items measuring trust is related to the contextual variables found through statistical significance.

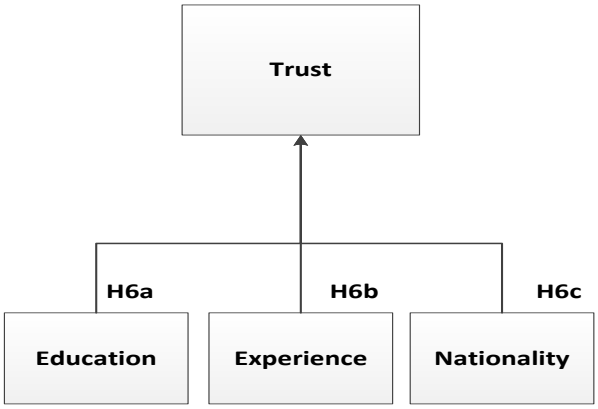

Figure 5.1: Contextual, Relationship between Contextual Factors and Trust as an Antecedent of e-Government Security

From Table C2 in Appendix C, it can be seen that only two correlations are found to be statistically significant (p-value of significance less than 0.05) namely 'Education-ET4' and 'Experiecne-ET9'. Correlation for the relationship Education-ET4 was found to be 0.281 and Experiecne-ET9 0.363. From Table C2 in Appendix C, it can be seen that the correlation between user education and trust is small and between user experience with IT and trust is medium. This implies that the relationship between contextual factors and trust as an antecedent of user centric e-Government security is at best medium in level. One reason for this could be that user education levels are sufficiently high in Bahrain and the maturity level of e – government could be so high that with a certain level of education already prevailing with the users, they are able to understand aspects related to e-Government including transacting through the e-Government portal, trust and security issues. Similar arguments can be extended to the relationship between user experience with IT and trust which perhaps points to the high level of maturity of the e-Government services offered by Bahrain. This is evidenced by the high ranking Bahrain has achieved (rank 14 for e-participation worldwide) in the e-Government survey conducted by UN (UNPAN, 2014) in 2014. Based on this it is possible to conclude that

hypotheses H6a and H6b are accepted while H6c is rejected. Thus, the researcher went ahead with the main survey with the theoretical validity established at the preliminary stage.

5.4 Main Survey

As mentioned in Section 4.10, survey method using self-administered questionnaire was used as the research strategy in this research to test the conceptual model. Already a comprehensive discussion on the instrument developed for the survey, which is the self-administered questionnaire has been provided in Sections 6.1 above. In order to administer the survey, it was necessary to identify the population who will be investigated using sampling procedure if the target population is very large. Thus, the following sections describe the population targeted and the sample size chosen for this research. This section in addition dwells on the data collection aspects as well.

5.4.1 Population

The main population that was targeted to test the conceptual model was the e-Government service users. The users in the Kingdom of Bahrain who used one or more e-Government services offered by the government were targeted. It was necessary that users had some awareness and experience with the e-Government services at the transaction level as security aspects are more prominent at this level of transaction with the e-Government services. While the actual population ran into several tens of thousands, it was important to use the sampling procedure to get responses. Users belonged to either gender, differing nationality, varying educational qualifications, engaged in various professions, having a range of years of experience and above 18 years of age. The minimum conditions to be met were that they should have used one or more e-Government services at the transaction level and must know how to use online facilities. After deciding on the target population, next the sample size was determined as described in the following section.

5.4.2 Sample Size

According to researchers (see Sekaran, 2006), sampling design and sample size are essential to examine the representativeness of the sample so that the outcome could be generalized. Sample size could be computed using two ways. One way is the thumb rule, which provides a broad guideline on the sample size depending on previous experience. For instance, Roscoe (1975) argues that for most research sample sizes exceeding 30 and within 500 are generally accepted as appropriate. Similarly, for multivariate research sample, size should be many times the number of variables (e.g. 10 or more times than the variables). The other way is to compute the sample size using the formula given below;

$$SS = \frac{Z^2 * (p) * (1-p)}{c^2}$$

Where:

Z = Z value (e.g. 1.96 for 95% confidence level)

p = percentage picking a choice, expressed as decimal (0.5 used for sample size needed)

c = confidence interval, expressed as decimal (e.g., .04 = ±4)

Thus for a confidence interval (margin of error) of ±4, Z=1.96 and p=0.5 if the above formula is applied then the sample size (SS) is found to be 600. Furthermore, researchers have used the following formula to provide correction on the formula above for the actual population to compute the new sample size. Thus, the formula for the new sample size is:

$$\text{New SS} = \frac{SS}{1 + \frac{SS - 1}{pop}}$$

Where: pop = population

Thus, for a sample size of 600 calculated without taking into account the actual population number, the corrected new sample size for a population of 10,000 will be approximately equal to 566. It is possible to use both the thumb rule and actual calculation to define the actual sample size required for this research.

For testing the conceptual model in this research, three population levels were considered namely 1,000; 5,000; and 10,000. If one applies, the formula given above it can be seen that the new sample size should be approximately 375; 536 and 566 respectively. Thus, for this research, a total population of 10,000 was considered and 566 responses were aimed to be obtained. A population of 10,000 was considered as reasonable as beyond this figure sample size requirements increase only incrementally. 600 e-mails were sent and 360 responses were

received. This is equivalent to a response rate of 60%, which is considered to be acceptable by researchers (Nulty, 2008). Thus, the sample size satisfies the thumb rule of 30-500 as well as the actual formula used in computing sample size.

The sampling method involved the use of non-probability sampling method was used because the data was to be collected from any citizen of the Kingdom of Bahrain, with one important criterion that the participant should be above the age of 18. There was no specific group that was targeted. Any citizen was eligible to participate as long as the participant had some experience of using e-Government services. Convenient sampling was chosen as an appropriate method because representativeness of the population as a criterion was not required. Although convenient sampling suffers from some limitations such as bias, the results were not expected suffer greatly because even with convenient sampling there was a certain randomness involved in the choice of participants as the characteristics defined for a participant was very simple which was easy to achieve either through probabilistic sampling or non-probabilistic sampling.

5.4.3 Data Collection

Data for testing the hypotheses related to the conceptual model in this research were collected using the instrument (Appendix C, Table C1) developed for this purpose. Users were identified as the participants in the survey. The self-administered questionnaire was posted on the web portal and the Universal Resource Locator (URL) pertaining to the questionnaire was distributed to the participants through e-mail. The use of website to collect data enabled the researcher to access the participants efficiently and also obtain data without error. The participants were followed-up over phone so that the required number of responses could be obtained. As mentioned in Section a wide spectrum of e-Government users were approached to participate in the survey. The collected data were downloadable in various formats including SPSS. The data were collected over a period of about two months. After collection the data were edited and coded using SPSS version 18 software package to conduct the statistical analysis.

5.4.4 Data Analysis

The collected data was edited and coded using SPSS version 18 software. Data were coded using alphabet and numeric symbols and edited prior to entering on SPSS version 18. Each item in the questionnaire has a unique variable name. A coding scheme was used and the coding sheet is provided in Appendix C, Table C1. Data were directly imported from the website using SPSS format thus ensured that there is no data entry error as there is manual intervention. Data were screened to check whether the values are out of range or for continuous variables (which includes examining the minimum, maximum, median and standard deviation). Further, out of

360 responses, only 309 responses were complete and the remaining 51 responses were incomplete and hence were neglected. After verifying that there is no error, SPSS version 18 data sheets were prepared for analysis.

Further to preparing, the data for analysis and as explained in Section 4.10, statistical data analysis comprised descriptive, testing the reliability and validity of the data, factor analysis, SEM and path analysis. Descriptive data analysis is provided in Appendix C (Table C3) and is restricted to analyzing the standard deviation, normality, outliers and multicollinearity. Descriptive data related to demography was not reported as data collected was not complete and many participants did not answer this section. Furthermore, variables pertaining to descriptive were not part of the research model. Since the missing data with respect demographics was very high and they were not part of the research relationship model, the partial analysis of the data did not provide any useful information and was not reported.

The next step taken was to verify whether there are missing data. It was found that there were no missing data. Next, the normality of the data distribution was tested. With respect to normality, the researcher used the widely accepted tests of testing the skewness and kurtosis of the data distribution (Hair et al., 2006). Skewness indicates the symmetry of the normal curve around the center. Kurtosis indicates the extent to which the data distribution is peaked or flat (Pallant, 2010). Positive skewness is indicated by a shift of the distribution to the left while negative skewness indicates the shift to the right. Similarly, Negative kurtosis indicates peaked distribution of data while flat distribution indicates positive data distribution. According to Li (1999), acceptable values of skewness lie in the range of ±1.5 while for kurtosis lie in the range of ±3.0. It was seen from Table C3 in Appendix C that values computed indicated that for no item skewness exceeded ±1.5 and kurtosis exceeded ±3.0. Thus, it was concluded that the data distribution was normal.

5.4.5 Outliers

After testing the normality of distribution of data, the presence of outliers was checked. As explained in section 4.10.1.7, Mahalanobis distance was used to determine outliers using SPSS/AMOS version 18. Mahalanobis distance was computed using the formula D^2/df. The commonly accepted value of D^2/df is 4 or less. Any response or case whose Mahalanobis distance is higher than 4.0 could be deleted as recommended by Pallant (2010). On the other hand, according to Burke (2001) as a rule of thumb, if more than 20% of the responses are identified as outlier, the assumption about data distribution or the quality of the data collected must be questioned. In this research, the maximum percentage of outliers was found with regard to perceived usefulness which stood at 5.8% (18 responses were found to exceed the value of

4.0 for the measure D^2/df). (See Appendix C, Table C4). This is much less, than the tolerable limit of 20% suggested by Burke (2001). Hence, no response was deleted from the data collected.

5.4.6 Multicollinearity

As explained in section 4.10.1.9, multicollinearity test was used to test the correlation among the variables. If the correlation amongst variables is exceeding 0.8 or 0.9, then it would indicate the presence of multicollinearity. SPSS/AMOS version 18 was used to compute the correlation amongst the observed variables under a construct. In this research it was found that the correlation among the observed variables measuring a latent variable did not exceed 0.8 (see Appendix C, Table C5). Thus, the data were found to be free of multicollinearity.

The foregoing discussions indicate that the data are now ready for further statistical analysis as they have been checked for cleanliness and tidiness. As a next step, it was necessary to conduct the factor analysis to ensure that optimum set of variables are used in the measurement of the model. As explained in Section 4.10.1.11, there are two types of factor analysis. One is the Exploratory Factor Analysis (EFA) and the other is the Confirmatory Factor Analysis (CFA). While detailed explanation about the concepts of EFA and CFA have been already provided under Section 4.10.1.11, in the following sections the actual factorization has been provided.

5.5 Confirmatory Factor Analysis (CFA)

In this research, the specified model (Figure 3.1) and the hypotheses was tested using CFA, which is the first step in SEM, followed by path analysis and hypotheses testing. CFA is part of part of structural equation modeling (SEM) which is used to test the structural model and the measurement model (Janssens et al., 2008; Hair et al., 2010). According to Anderson and Gerbing (1998), two approaches are recommended in measuring model using confirmatory factor analysis (CFA) which requires testing causal relationship between items and constructs, and the second approach is testing causal relationship between exogenous and endogenous constructs. Thus, in this research, confirmatory factor analysis (CFA) was conducted using AMOS 18.0 to specify the casual relationship between the items (observed factors) and underlying theoretical constructs. Then, in the second stage, specifying the casual relationship between underlying exogenous and endogenous constructs in the structural model.

The CFA model in Figure 5.2, is a representation of the conceptual model developed in Figure 3.1. In this model circles or ovals indicate latent variables while squares or rectangles indicate manifest or observed variables. Thus, in Figure 5.2 the rectangles indicate the observed

variables that are directly measured and represent the items in the questionnaire. The circles with 'e' indicate error components. The remaining circles are the latent variables representing the constructs (Byrne, 2001; Ullman, 2001).

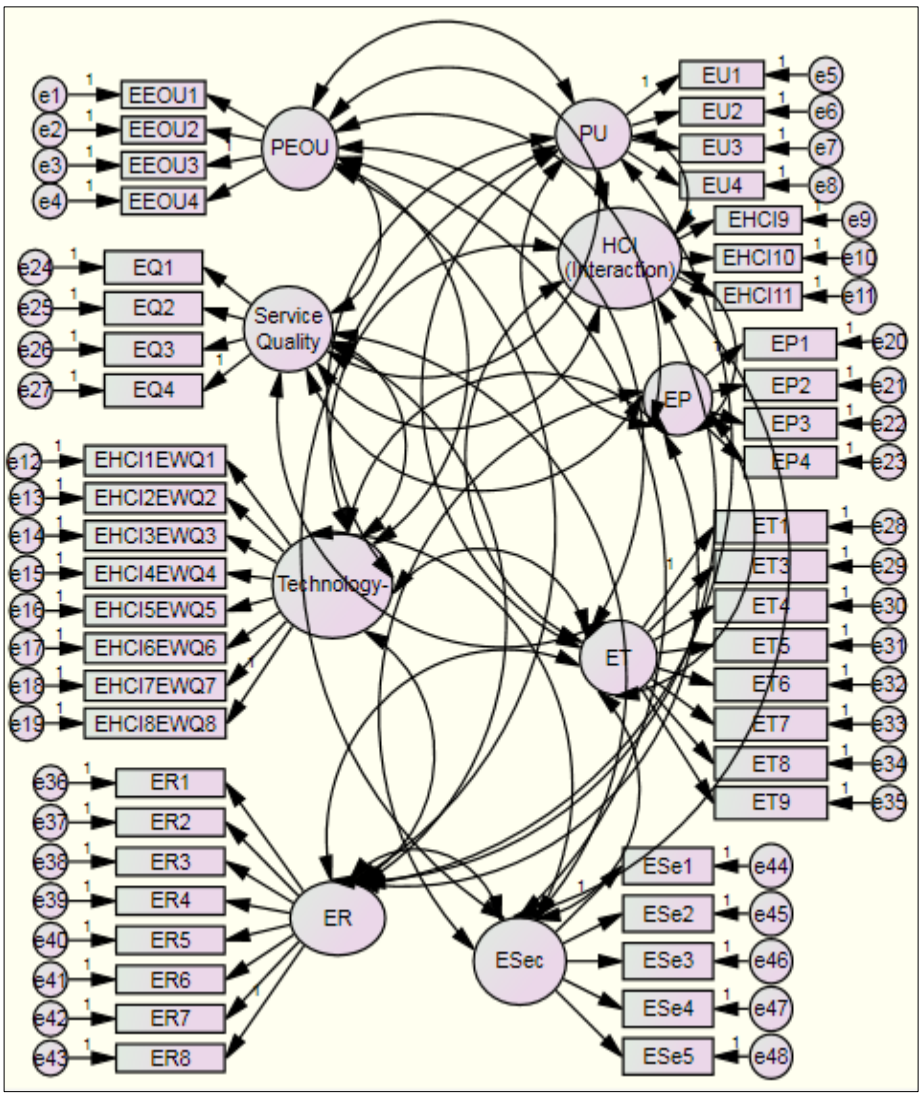

Figure 5.2, Specified CFA model

There are nine constructs namely PEOU, PU, HCI, Privacy, Quality, Technology, Trust, Risk and Security that form the latent variables. Amongst these PEOU, PU, and Technology were called the exogenous constructs (independent variables, from which arrows lead away) while Trust, Risk and Security were called the endogenous variables (dependent variables, towards which arrows lead in) (Arbuckle and Wothke, 1999). HCI, Privacy and Quality have been treated as moderating variables as they have been assumed to influence the relationship between technology and security (see Section 5.6.1). Each measurable variable has an error term. The two-headed arrow connection indicates covariance between the constructs. One headed arrow

connection indicates the casual relationship path from construct to measurable variable (items), also called Standardized Regression Weights (SRW), or Factor Loading (FL).

Prior to proceeding with SEM researchers, suggest that reliability and validity tests need to be conducted on the constructs (Bollen, 1989). The two tests suggested by researchers with regard to reliability (consistency) and validity (accuracy) are the construct reliability and discriminant validity (Holmes-Smith et al., 2006). These two aspects are discussed next.

5.5.1 Construct Reliability

According to researchers, one of the methods that is used to test construct reliability is the Squared Multiple Correlation (SMC) (Holmes-Smith et al., 2006). This parameter measures the reliability coefficient and is the correlation between an item that is used to measure a construct and the construct that is measured using the item. SMC is calculated for an observed variable as the square of the items standardized loading on the construct. According to researchers, the minimum accepted value of SMC is 0.3 (Holmes-Smith et al., 2006). In this research SMC for all observed variables have been seen to exceed 0.3 except for EHCI11 (SMC 0.217) which was deleted (see Appendix C, Table C5). Thus, it can be concluded that the construct reliability for the research model has been established.

5.5.2 Discriminant Validity

Validity measures the accuracy of the measures that have been used in this research. Discriminant validity is supposed to be there if the measure used in the model is found to be a perfect representation of the variable that is purported to be measured. Discriminant validity provides an idea on the extent to which constructs in a model are different (Holmes-Smith et al., 2006). AMOS was used to test the discriminant validity. Three types of tests were carried out by the researchers to assess the discriminant validity as part of the SEM technique. These were sample correlations (between constructs) (Holmes-Smith et al., 2006), residual covariance (between items) and standardized residual covariance (between items) (Jöreskog and Sörbom, 1984). In addition to the three tests, another important test of validity that has been suggested by researchers is the test of goodness of measures (Sekaran, 2003). The following sections discuss the abovementioned tests conducted on the research model using the collected data.

According to Holmes-Smith et al. (2006), large correlations (exceeding 0.8 or 0.9) can be said to contribute to lack of discriminant validity. In this research the model was tested using AMOS and the sample correlation report generated by AMOS (see Appendix C, Table C5) shows that none of the correlation values exceeded 0.8 except the correlation between the items EP2 and EP3 (0.81) and EU1 and EU3 (0.809). However, these values were considered to be

approximately equal to 0.8 when rounded off to the first decimal place and hence none of the items were deleted from the analysis. Thus, discriminant validity was concluded to exist after the first test. Subsequent to the first test, the residual covariance and standardized residual covariance tests were conducted to corroborate the results obtained through sample correlation test. According to researchers, acceptable residual covariance values should not exceed ±0.2 (Jöreskog and Sörbom, 1984) while for standardized residual, covariance the value should not exceed ±2.0 (Jöreskog and Sörbom, 1984). If there are values that are found to exist that exceed these values then those elements that contribute for this problem were deleted from the model. It was found that some items contributed to values of residual covariance exceeding 0.2. They were EHCI11, EU2, ER2, ER7, ET5 and ESec4. These items were deleted and the AMOS was run again and it was found that all residual covariance values were within the specified limit of ±0.2 (see Appendix C, Table C6).

The redrawn model after deleting the item is provided in Figure 5.3

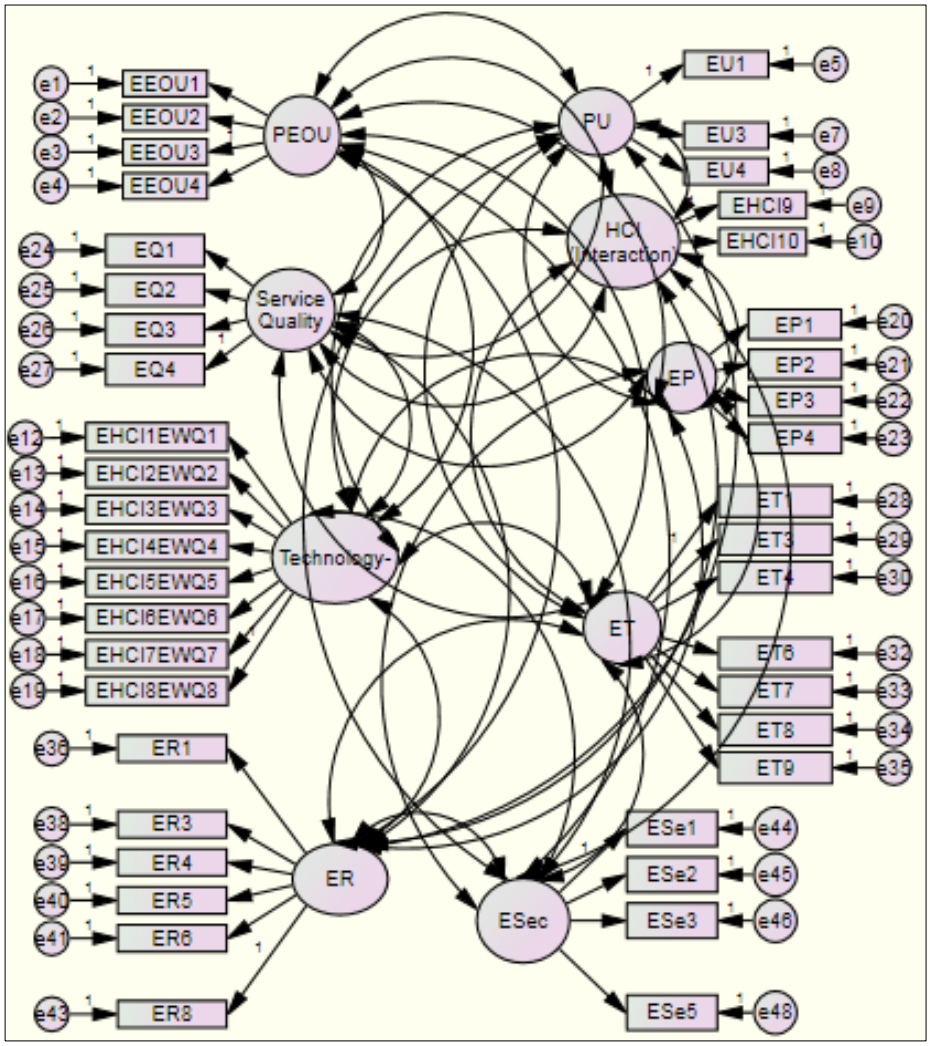

Figure 5.3: CFA Model after Deleting Items (HCI11, EU2, ER2, ER7, ET5 and ESec4)

Next, the standardized residual covariance test was conducted to find whether any value exceeds the prescribed limit of ± 2.0. AMOS was run to confirm that all standardized residual covariance values were within the prescribed limit of ±2.0 (see Appendix C, Table C7). In addition variance extracted (VE) reading was compared with construct reliability reading using AMOS reports provided in Table C9, Appendix C to test discriminant validity. From Appendix C provides how construct reliability and VE are calculated. Computations show that construct reliability reading (0.9988) is greater than VE reading (0.953).

Further to the testing of the sample correlation, residual covariance and standardized residual covariance, the next test conducted was the goodness fit measure. According to researchers there are many different tests that are conducted by researchers to test the goodness fit of the model to the data which include Chi-square, Goodness Fit Index (GFI), Comparative Fit Index (CFI), Norm Fit Index (NFI), Incremental Fit Index (IFI), Relative Fit Index (RFI), Tucker-Lewis Index (TLI), Root Mean Square Residual (RMR) and Root Mean Square Error Approximation (RMSEA) (Schreiber et al., 2006). However according to Park (2008) although there are many different indices developed by researchers, it is conventional to report at least one amongst them. One reason for this is that each one of the indices have some draw back or the other leading to lack of consensus on the part of researchers on the acceptability of any one index as unique and universal (e.g. Schreiber et al., 2006). Thus in this research as many fitness indices that could be measured by AMOS as possible will be reported.

Thus, in this research CFI, NFI, IFI, TLI, RMR and RMSEA were reported. Acceptable values of CFI, IFI and TLI that have been reported in the extant literature should exceed 0.9 (Hu and Bentler, 1998, 1999) while RMR should be as close zero as possible (less than 0.05 is considered good) and RMSEA should be less than 0.08 (Schermelleh-Engel, Moosbrugger and Müller 2003). It was seen that NFI (0.890) and RFI (0.879) where very close to 0.9 while GFI at 0.81 was less than 0.9. Thus from Table C9 and Table C10 Appendix E, it can be seen that all values of CFI (0.945), IFI (0.946), TLI (0.940), RMR (0.043) and RMSEA (0.053) are able to meet the limits prescribed indicating that five of the seven tests were found to be acceptable. The above tests confirm that the data have been found to withstand the reliability and validity tests.

Further to confirming the reliability and validity of the data, the model that emerged after CFA is what is provided in Figure 5.2 At this juncture it is important to recall the basic model derived in Section 3.6 of Chapter 3. Since the model is having nine latent constructs, and according to literature it is important that in one round of analysis discriminant analysis should not contain

more than five latent variables the covariance model arrived at in Section 5.5.2 above the model was reorganized as follows and tested again. Figures 5.4 and Figure 5.5 have been redrawn in order to ensure that the number of latent variables being examined for discriminant validity does not exceed 5.

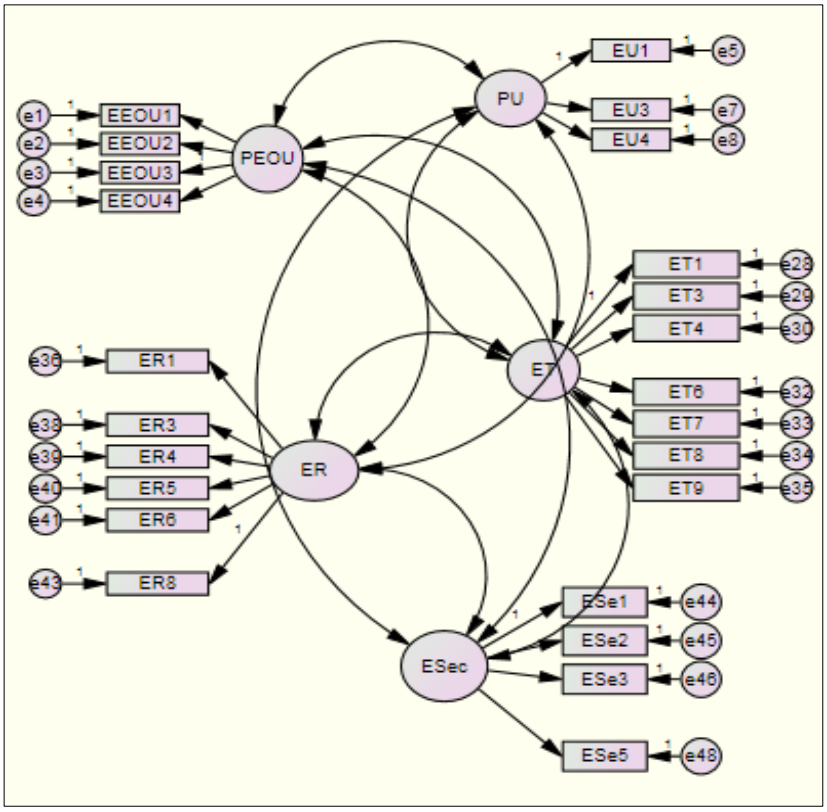

Figure 5.4: Discriminant Analysis of Five Latent Variables

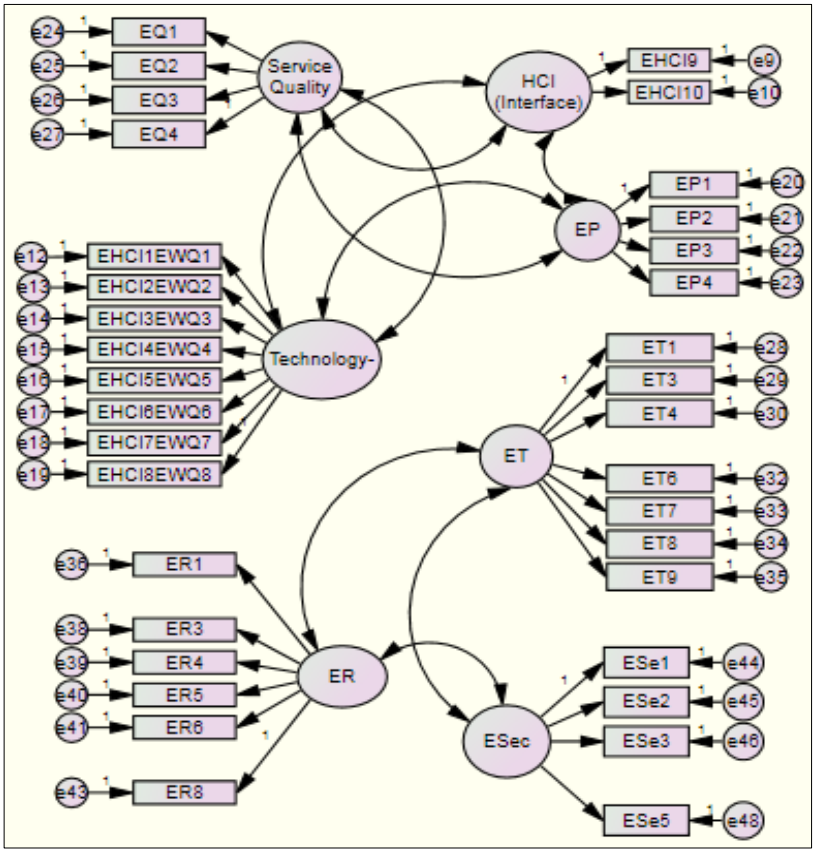

Figure 5.5 Discriminant Analysis of Six Latent Variables

All the parameters that have been outlined for testing the model in Section 5.5.2 above were tested and readings reported to be found to be within accepted limits (see Appendix C). As the next step, the structural aspects of the model in Figure 5.2 were tested using SEM.

5.6 Structure Equation Modelling (SEM)

According to Abramson et al. (2005), SEM consists of the following steps:

- Model specification
- Model identification
- Measure selection to data preparation
- Model Evaluation
- Model analysis
- Model re-specification

Each one of the above mentioned steps have been discussed in the following sections.

5.6.1 Model Specification

According to Kline (1998), model specification comprises a mathematically or pictorially expressed hypothesized relationship amongst the variables that contribute to the model. Two aspects were achieved. The first one is to include all the endogenous and exogenous variables that contribute to the core endogenous variable. In this research, the core endogenous variable is the user centric e-Government services security. According to Kline (1998) the remaining variables found in the model should be contributing to the prediction of the core endogenous variable that could be identified as the main variables supported by extant literature and theory (refer to Chapters 2 and 3).

Using the Figure 3.1of the conceptual model, a two-part test was conducted. The first part tested the influence of technology as an antecedent of user centric e-Government security on user centric e-Government security with the moderators. The analysis of this part led to findings on how technology (in this research the e-Government environment was investigated where cloud computing technology has been introduced) as a contextual factor affected user centric e-Government security in the presence of two other mediating antecedents of user centric e-Government security namely trust and risk and moderators HCI, user privacy and web design quality. The second part of the analysis led to findings regarding how users have perceived the e-Government security in an environment characterized by cloud computing technology in terms of their feeling of trust and risk and their perceived ease of use and usefulness of the technology when they operate through the e-Government portal. The first part of the conceptual model tested was given in Figure 5.6. It was called SEM1.

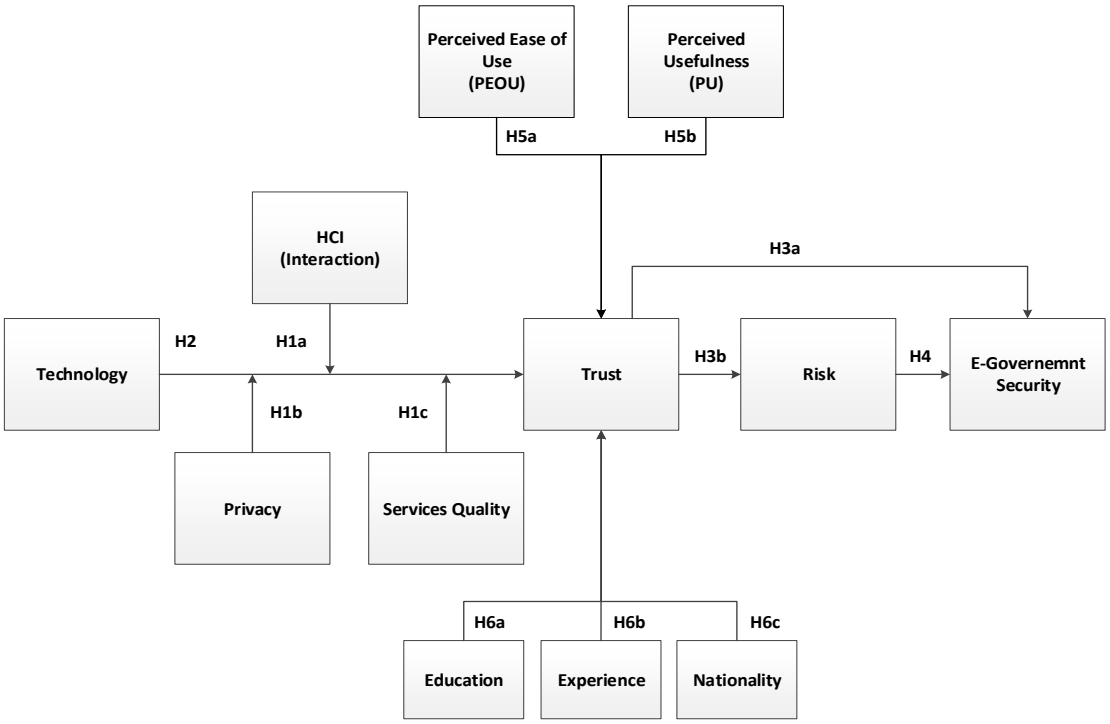

Figure 5.6: SEM1 for Analyzing Influence of Technology on E-Government Security.

The second part of the conceptual model tested is given in Figure 5.7. This was called SEM2.

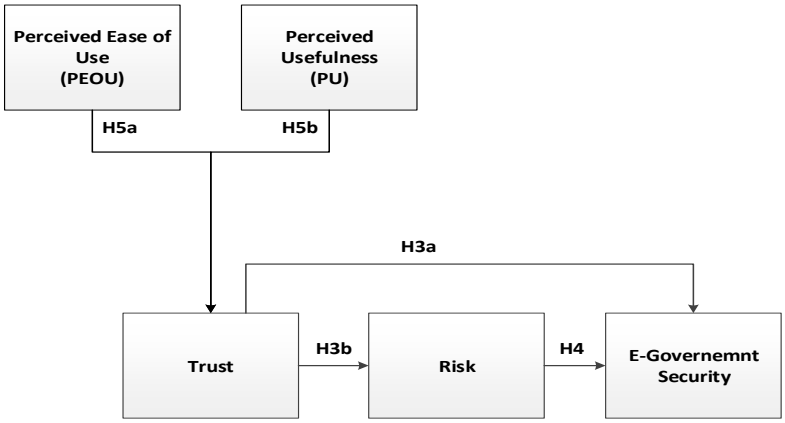

Figure 5.7: SEM2 for Analyzing Perception of Users of E-Government Security Characterized by Cloud Computing

According to the SEM, the models must determine the direction of relationship between any two variables in the SEM model. While the direction specified could be a subject of argument, the important aspect that provides support to the direction indicated in the models in Figures (5.6 and 5.7) is the theory and discussion on past research provided in Chapters 2 and 3. Thus, the models given in Figures (5.6 and 5.7) act as the 'specified models' (measurement models) for this research. Prior to proceeding with the remaining steps in the SEM, the researcher ran AMOS to check the regression weights on the relationship between the independent and dependent variables and the p-value of significance. This was necessary to identify the model, which involves determining the number of parameters used in the model and the data points involved in the model (Ullman, 2006). Thus, both SEM1 and SEM2 have been tested initially for checking the regression weights on the relationship between the independent and dependent variables as well as control and dependent variables and the p-value of significance.

5.6.1.1 SEM1

The initial Figure 5.8 derived from conceptual model in Chapter 3 and the CFA model above is provided below (Figure 5.8).

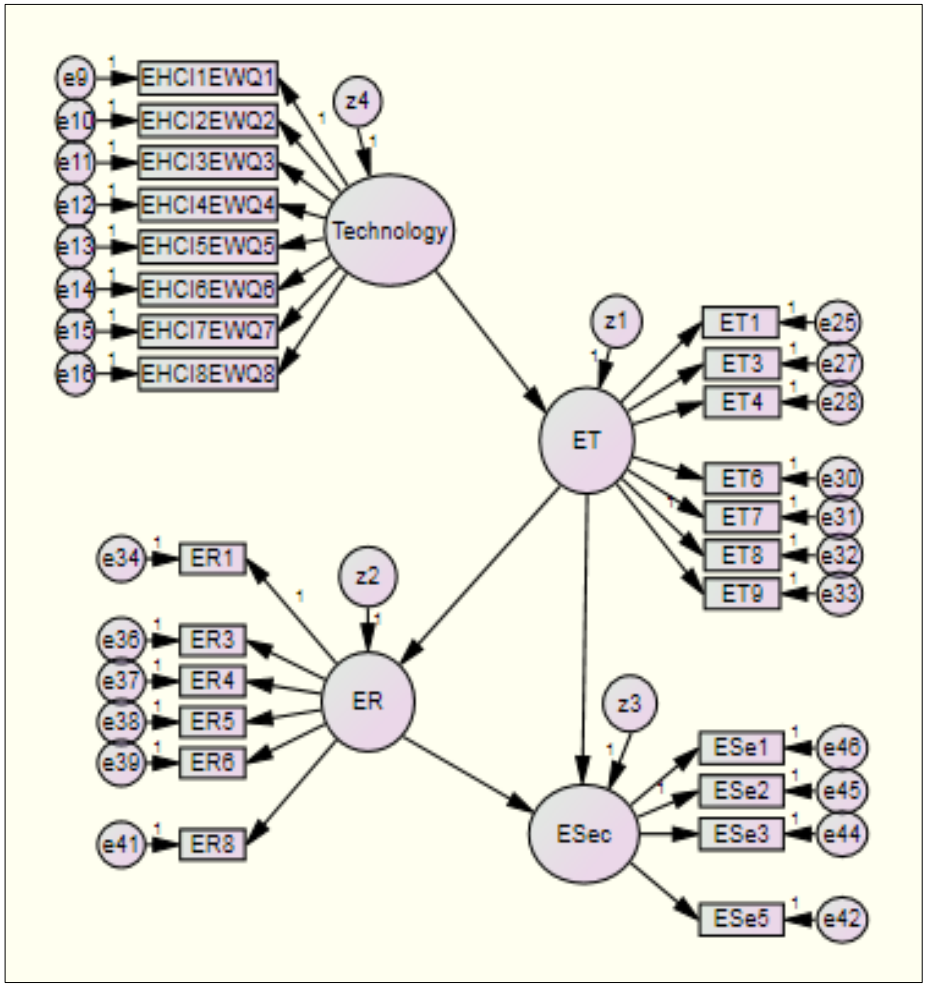

Figure 5.8: SEM1 without Moderators

As a first step the significance of the relationships amongst the constructs were tested using the report generated by AMOS (see Table 5.3). The outcome of the tested model (standardized) in Figure (5.8) is provided in Figure (5.9), RMR=0.045; GFI=0.888; NFI=0.926; RFI=0.918; IFI=0.965; TLI=0.961; CFI=0.965; RMSEA=0.052.

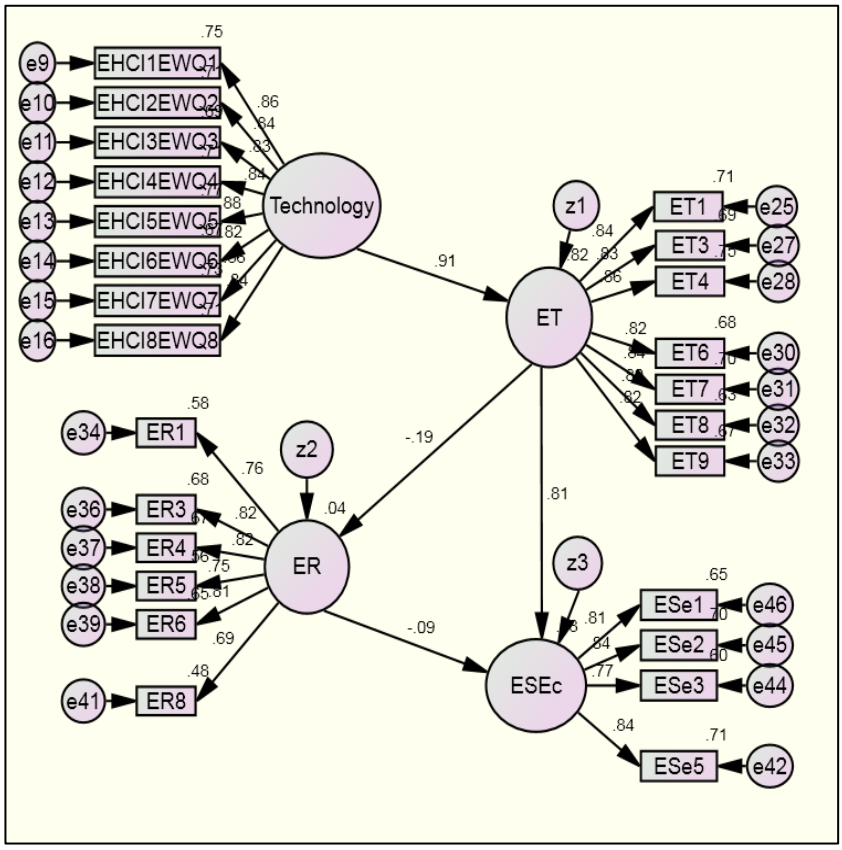

Figure 5.9: SEM1.1 without Moderators (Standardized)

Sample correlation between all items was well within limits (less than 0.9) (see Appendix C, Table C10). Construct reliability was tested using SMC (see Table 5.3). It can be seen that all values are above 0.3.

	Estimate
ET9	.669
ESe5	.711
ESe3	.596
ESe1	.654
ESe2	.704
ER8	.479
ER6	.649
ER5	.564
ER4	.672
ER3	.677
ER1	.581

	Estimate
ET1	.714
ET3	.687
ET4	.745
ET6	.678
ET7	.699
ET8	.635
EHCI8EWQ8	.712
EHCI7EWQ7	.732
EHCI6EWQ6	.665
EHCI5EWQ5	.773
EHCI4EWQ4	.707
EHCI3EWQ3	.694
EHCI2EWQ2	.711
EHCI1EWQ1	.746

Table 5.3: SMC for Model SEM1.1

Residual and standardized residual covariance readings were within ±0.2 and ±2.0 respectively (see Appendix C, Table C12). Construct reliability reading is greater than variance extracted reading (see Appendix C, Table C13, Table C9 AVE extracted for SEM1.1) indicating the presence of discriminant validity. Model fit indices show that RM R (0.045), NFI (0.926), RFI (0.918), IFI (0.965), TLI (0.961), CFI (0.965) and RMSEA (0.052) are satisfactory. One more test was conducted to confirm that the model was fit to the data. It is the use of Bollen-Stine bootstrap that provides a method to simulate sample sizes that could see whether the Chi-square minimum (CMIN) value that is largely dependent on sample size could be found to be significant. Thus from Table 5.4, it can be seen that the null hypothesis that the model fits the data is rejected because the p-value of significance is lower than 0.05.

Model	NPAR	CMIN	DF	P	CMIN/DF
Default model	54	495.978	271	.000	1.830
Saturated model	325	.000	0		
Independence model	25	6726.580	300	.000	22.422

Table 5.4: CMIN for Model SEM1.1

In order to test whether model fit could improve, Bollen-Stine bootstrap method provided by AMOS was used and the report from AMOS is provided in Table Bollen-Stine Bootstrap (Default model), SEM1.1. From Table Bollen-Stine Bootstrap (Default model) it can be seen that the null hypothesis is accepted at a bootstrapped p-value of 0.139 indicating that model fit with respect to CMIN.

The model fit better in 173 bootstrap samples.
It fit about equally well in 0 bootstrap samples.
It fit worse or failed to fit in 27 bootstrap samples.
Testing the null hypothesis that the model is correct, Bollen-Stine bootstrap p = .139

Table 5.5: Bollen-Stine Bootstrap

Further, the regression weights report produced by AMOS was examined and is provided in Table 5.6. This test provides information on the statistical significance of the relationship between the endogenous and exogenous variables without verifying which it is difficult to conduct SEM.

			Estimate	S.E.	C.R.	P	Label
ET	<---	Technology-	.914	.057	16.016	***	par_24
ER	<---	ET	-.201	.066	-3.051	.002	par_23
ESec	<---	ER	-.088	.040	-2.177	.029	par_22
ESec	<---	ET	.819	.062	13.275	***	par_25

Table 5.6: Regression Weights for Model SEM1.1 (Without Moderators)

From the column headed as 'P' it can be seen that all readings are less than 0.05 indicating that relationships are statistically significant. The foregoing analysis provides the basis to identify the model because all the relationships amongst the endogenous and exogenous variables have been found to be significant. Thus, the next step was to identify the model SEM1.

5.6.1.2 Model identification of SEM1

Model identification was done in accordance with the guidelines provided by Ullman (2006). According to Ullman (2006), a model is identified if the number of parameters in the model is less than the data points in the model. The data in the model are equal to the number of variances and covariance in the model (Ullman, 2006). The number of data points in the model is given by the following formula (Ullman, 2006):

Number of data points (N) = [p (p+1)] ÷2 → ①
Where p equals the number of measured variables.

The number of parameters is calculated as the sum of the number of regression coefficients, variances, and covariance that are to be estimated. Thus, in Figure C1 in Appendix C, it can be seen that the number of measured variables are 29 [the number of variances from each construct to the items (25) + the number of variances between the constructs (4)]. Therefore if N = [29 (29+1)]/2 = 435 (29 variances and 406 covariance). The number of parameters to be estimated is the sum of 25 regression coefficients, 25 variances, 4 regression coefficients between the constructs and 3 variances related to exogenous constructs (z1, z2 and z3) which is equal to 57. Thus, the model has 435-57 = 378 fewer parameters than what is available in the model. When the number of parameters is fewer than the number of data points then the model is said to be identified (Ullman, 2006). Following the identification of the model, the next step taken was measure selection to data preparation, which is described below.

5.6.1.3 Measure Selection to Data Preparation

This step involves four steps namely measure selection, data collection, data cleaning and data preparation (Abramson et al., 2005). Measure selection has been described in section 5.3. Data collection aspects have been addressed under section 4.7.6. Data cleaning and preparation are addressed under section 4.10.2. Following this section model fit was examined.

5.6.1.4 Model Evaluation (Model fit)

According to researchers (e.g. Arbuckle, 2006, 2010; Bollen and Long, 1993; Browne and Cudeck, 1993; Byrne, 2001, 2010; Holmes-Smith et al., 2006; MacCallum, 1996; Mulaik et al., 1989; Steiger, 2000) model analysis also referred to as model fit (Abramson et al., 2005) comprises tests that include the following:

a) Test of parsimony
b) Testing the minimum sample discrepancy function for acceptability of the model fit
c) Assessing population discrepancy measures
d) Comparing baseline model
e) Checking the goodness of fit index

Each one of these tests was conducted and discussions are provided next.

5.6.1.5 Test of Parsimony

Parsimony indicates that the model fits better to the data. According to researchers (e.g. Mulaik, 2001; Mulaik et al., 1989) a model is considered to be parsimonious if it has relatively few free parameters or relatively many degrees of freedom. The data analysis output from AMOS given in Table Parsimony below indicates that the model has 54 parameters against 271 degrees of freedom indicating that the model is parsimonious.

Model	NPAR	CMIN	DF	P	CMIN/DF
Default model	54	495.978	271	.000	1.830
Saturated model	325	.000	0		
Independence model	25	6726.580	300	.000	22.422

Table 5.7: Parsimony

5.6.1.6 Testing the Minimum Sample Discrepancy Function for Acceptability of the Model Fit

Researchers argue that sample size plays an important role in determining the model fitness (Gao et al., 2008). Gao et al. (2008) sample discrepancy function indicates the degree of discrepancy between the model-implied and sample-derived covariance matrices. While there are different methods (e.g. using the Chi-square minimum and CFI) to measure the discrepancy and ensure that it is a minimum, this research uses the CFI as the measure of the sample discrepancy function, an argument supported by Hu and Bentler (1999). According to Hu and Bentler (1999), minimum sample discrepancy exists if CFI exceeds 0.9. The AMOS output in this research shows that CFI is measured as 0.965 (see Table 5.8) indicating that the discrepancy is minimum.

Model	NFI Delta1	RFI rho1	IFI Delta2	TLI rho2	CFI

Model	NFI Delta1	RFI rho1	IFI Delta2	TLI rho2	CFI
Default model	.926	.918	.965	.961	.965
Saturated model	1.000		1.000		1.000
Independence model	.000	.000	.000	.000	.000

Table 5.8: Baseline Comparisons

5.6.1.7 Assessing Population Discrepancy Measures

According to Steiger (2000), population discrepancy function is defined as the function that would be obtained as a measure of population fit, if an estimation technique is applied to the population covariance matrix. Commonly RMSEA is used as the population discrepancy measure (Steiger, 2000). According to researchers, acceptable values of RMSEA should be in the range of 0.06 to 0.08 (Schreiber et al., 2006). AMOS output in this research shows that RMSEA value stood at 0.052 (see Table 5.9), thus implying a lower population discrepancy.

Model	RMSEA	LO 90	HI 90	PCLOSE
Default model	.052	.045	.059	.323
Independence model	.264	.258	.269	.000

Table 5.9: RMSEA

5.6.1.8 Comparing Baseline Model

An important measure that indicates good fit is the comparison to baseline models generated by AMOS. Report from AMOS clearly indicates that three of the goodness fit indices namely IFI, TLI and CFI (see Table 5.9) are close to the saturation model and above the zero value indicated against the independence model. This test indicates that the model fits to the data appropriately (Arbuckle, 2010).

5.6.1.9 Checking the Goodness of Fit Index

Several measures have been used by researchers to test the goodness fit of the model to the data, for instance use of GFI, IFI, TLI, NFI and CFI (Schreiber et al., 2006). However, researchers argue that at the least one of the indices should be reported in order to confirm that the data fits to the model (Park, 2008). Thus, in this research three indices were reported. They were IFI, TLI and CFI. As mentioned earlier (Section 5.7.2 and Section 5.8.4.2) in this thesis, acceptable values of IFI, TLI and CFI should be greater than or equal to 0.9. Accordingly, the AMOS report produced for this research shows that IFI (0.941), TLI (0.937) and CFI (0.941) exceed the reference value of 0.9 (see Table 5.9) indicating the goodness fit of the model.

5.6.1.10 Model Analysis (Model Estimation)

In order to estimate a model (estimation of the procedure to fit the model with data) Maximum Likelihood is the method that is widely used by researchers (e.g. Kline, 1998). According to

Abramson et al. (2005), AMOS is used to analyze and estimate a model, which uses ML method and produces unstandardized and standardized outputs. Unstandardized output provides information on individual exogenous variable variances directly on the model itself while standardized output provides information on endogenous variable variances (through the use of the squared multiple correlation coefficient) on the model (Arbuckle and Wothke, 1999). Since unstandardized and standardized outputs from AMOS have a specified purposes researchers generally report both the outputs. Furthermore, Kline (1998) argues that regression beta weights can be classified in absolute values of 0.1, 0.3 and 0.5, which in turn are regarded to have small, moderate and large effects respectively. Figure 5.10 (Unstandardized) and Figure 5.11 (Standardized) give the unstandardized and standardized AMOS output.

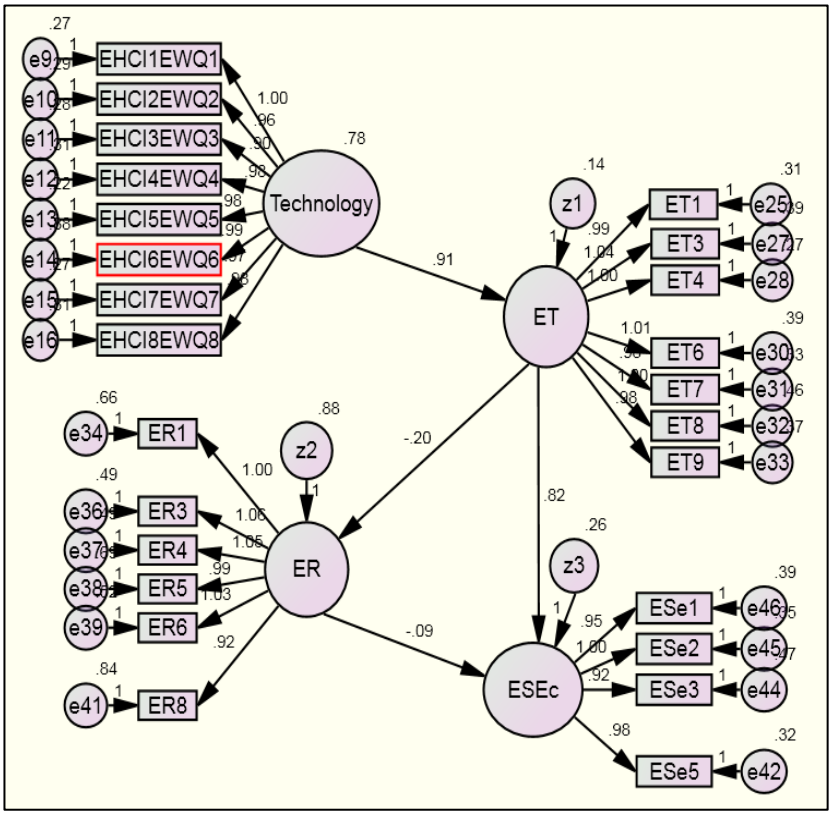

Figure 5.10: SEM1.1 Unstandardized Model

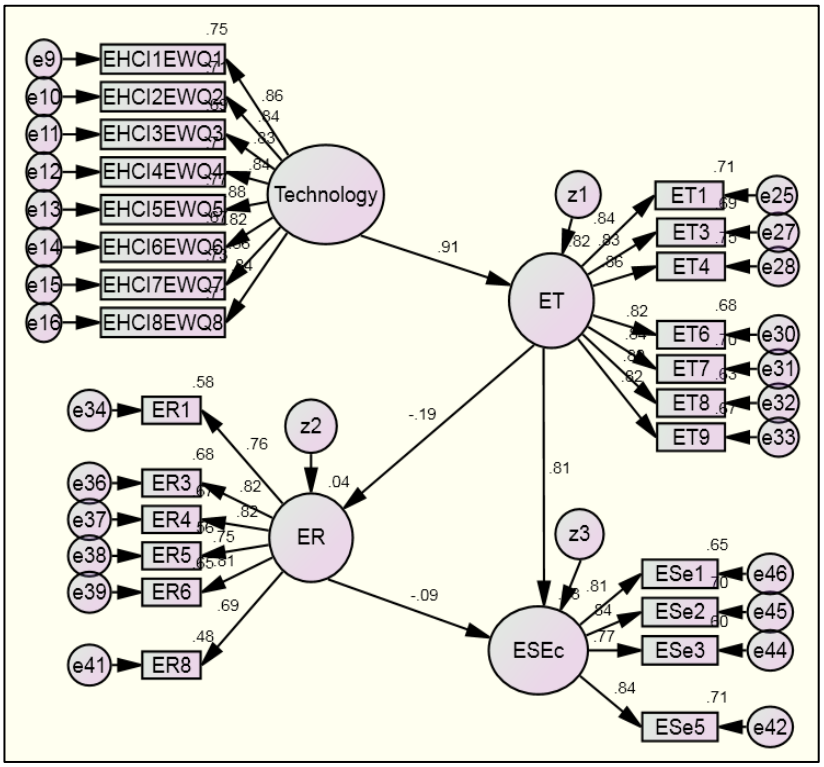

Figure 5.11: SEM1.1 Standardized Model

Using the model the SMC, parameter summary, sample correlation, standardized residual covariance and goodness fit of the model were tested as part of the model analysis. In addition, path analysis was carried out. The following sections provide a discussion on the outcome of these tests.

From Table 5.3, it can be seen that SMC values of all items is above the reference value of 0.3. Similarly, parameter summary in Table 5.7 indicates that the model is over identified, as the number of parameters is fewer than the degrees of freedom. Sample correlation provided in Table C in Appendix C11 indicates that none of the values exceeds 0.8. Residual covariance (see Appendix C, Table C12) and standardized residual covariance (see Appendix C, Table C13) values produced by AMOS for the model in Figure 5.11(standardized) reported none of the values exceed the reference value of ± 0.2 and ± 2.0 respectively fixed for this research. Furthermore, the goodness fit indices (see Appendix C, Table C14, Table C15 and Table C16) NFI (0.926), RFI (0.918), IFI (0.965), TLI (0.961), CFI (0.965), RMR (0.045) and RMSEA (0.052) have been found to be better than the reference values fixed for this research (see Section 5.7). Thus, the tests indicate that the estimation procedure to fit the model in Figure 5.11, with the data provided enabled the researcher to conclude that the initial solution is fine.

5.7 Path Analysis

The initially identified model in Figure 5.11 was assessed further with respect to the various paths. Table 5.10 provides information on the significance of the paths found in the initial e-Government security model. It can be seen that all the four paths depicted in the initial e-Government security model are significant with p-values for the four paths indicating significant at the 0.01 level (see Table 5.10).

			Estimate	S.E.	C.R.	P	Label
ET	<---	Technology	.914	.057	16.016	***	par_24
ER	<---	ET	-.201	.066	-3.051	.002	par_23
ESec	<---	ER	-.088	.040	-2.177	.029	par_22
ESec	<---	ET	.819	.062	13.275	***	par_25

Table 5.10: Regression Weights for SEM1.1

The identified model also provides the basis to explain the relationship between:

- Change in technology and user trust in e-Government service.
- User trust in e-Government service and user felt risk in e-Government service.
- User felt risk in e-Government service and user centric e-Government services security.
- Trust in e-Government services and user centric e-Government services security.

Further to determining the significance of the relationship between the endogenous and exogenous variables, explanations on the relationship between the exogenous and endogenous variables through path analysis can be provided in statistical terms (using SMC) as follows:

Table 5.11 provides squared multiple correlations of the initial e-Government security model.

	Estimate
ET	.824
ER	.035
ESec	.685

Table 5.11: SMC, SEM1.1 (Constructs)

Table 5.11shows that the determinant technology accounts for:

- 82.4% of variance of ET
- 3.5 % of variance of ER
- 68.5% of variance of ESec

It must be noted here that although a 3.5% variance could be considered very low what could be interpreted is that there is a variance in ER due to a change in ET, which is very small. However if one considers the R-value then it can be seen that the estimate is 0.187 indicating a good association between the two variables although negative in nature. Even otherwise if one examines the mean of the responses provided by the participants against the 8 questions used to measure the exogenous variable risk, it can be seen that the responses revolve around the points 3 (somewhat disagree) and 4 (neither) on the 7-point Likert scale with the mean score of the responses ranging between 3.38 (for ER6) and 3.57 (for ER1). This could perhaps explain why the variance in the construct due to trust is low. This could be interpreted in a way that respondents associated lower risk with the e-Government technology and appear to have greater trust on the e-Government technology and felt that the user centric e-Government security is high even in a situation where a new technology (cloud computing) has been introduced. When this argument is read in conjunction with the overall variance (68.5%) seen in user centric e-Government security introduced by the construct technology, then it is reasonable to conclude that participants in the research have clearly felt lower risk associated with the change in technology and hence higher user centric e-Government security. Besides, the negative sign indicates that higher the trust then lower will be risk and vice-versa. Thus from the direction point of view the results are consistent with the logical aspect whereas from the magnitude point of view such a change appear to be minimal bordering insignificant. In this situation, statistically an argument could be put forward which says that the model identified is not the just identified model and there is a need to review the model identified through a review of the manifest variables that have been used to measure risk an aspect that could be examined in future research.

After accounting for the variance caused in the endogenous variables by the exogenous variables, the next step used was to assess the relative effect of each independent variable on the dependent variable using standardized regression weights (Hair et al., 2006). This also provided the basis to verify the hypotheses developed for the thesis. From Table 5.10, it can be seen that the following four hypotheses have been accepted as the paths between the predictors and e-Government services security are found to be statistically significant. That is to say that the following hypotheses are accepted.

- H2: e-Government technology positively influences user trust in e-Government services
- H3a: User trust on e-Government negatively influences user centric e-Government security
- H3b: User trust on e-Government negatively influences the risk felt by users of e-Government

- H4: User felt risk negatively influences user centric e-Government security

It can be interpreted that technology as a contextual factor influences user centric e-Government security through the paths 'Technology→Trust→e-Government security' and 'Technology→Trust→Risk→e-Government security'. Further, from Table 5.10, it can be seen that the relative affect (standardized regression weights) between contextual factor (cloud computing technology) and user centric e-Government security shows stronger paths (with p-value of significance below 0.05) through the relationship Technology→Trust (0.914) and Trust→e-Government security (0.819) but weaker paths through the relationship Technology→Trust (0.914), Trust→Risk (-0.201), Risk→e-Government security (-0.088).

The above results point out that cloud computing technology affects e-Government security through the path 'Technology→Trust→e-Government security'. Another important point is that the path Trust→Risk (-0.201) shows a negative relationship indicating that when trust increases risk decreases and vice-versa. A similar argument can be made with regard to the path Risk→e-Government security (-0.088) which shows a negative relationship indicating that when risk increases e-Government security decreases and vice-versa. Overall the relationship between trust and e-Government security operates in a way that when trust changes in the positive direction, risk changes in the negative direction and hence e-Government security changes in the positive direction leading to the interpretation that when trust increases, e-Government security increases due to a reduction in risk. In summary, the above findings can be tabulated as follows (Table 5.12):

Hypothesis No.	Hypothesis	Exogenous Latent Constructs	Endogenous Latent Construct	Results of Hypotheses verification	Explanation
H2	E-Government technology positively influences user trust in e-Government services	Technology	ET	**Accepted**	Technology positively and significantly influences ET
H3a	User trust on e-Government negatively influences user centric e-Government security	ET	ESec	**Accepted**	ET positively and significantly influences ESec
H3b	User trust on e-Government negatively influences the risk felt by users of e-Government	ET	ER	**Accepted**	ET negatively and significantly influences ER
H4	User felt risk negatively influences user centric e-Government security	ER	ESec	**Accepted**	ER negatively and significantly influences ESec

Table 5.12: Summary of results of SEM1.1 (Summary of the Significant Influence of Determinant on e-Government security)

The resulting SEM1 model is provided in Figure (5.12)

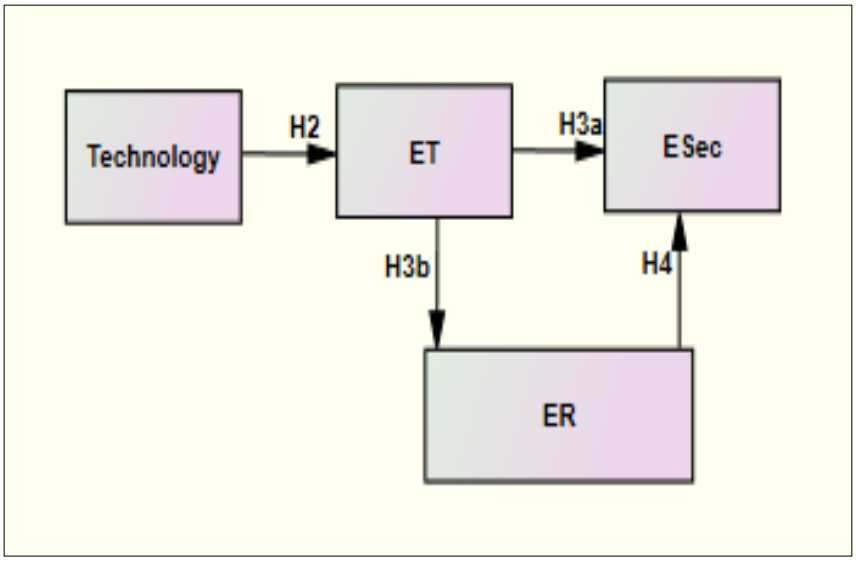

Figure 5.12: (Final SEM1.1)

5.7.1 Effect of moderators on SEM1

From Sections 5.3, it can be seen that three moderators namely HCI, ER and Service Quality have been analyzed for the reliability, validity and goodness fit at the CFA level. The resulting factors confirmed by CFA are provided in Figure 5.3. Further, the main SEM1 has already enabled the researcher to confirm the relationship between the determinant (Technology) and the determined (user centric e-Government services security) (see Sections 5.6 and 5.7). The next step was to know the influence of moderators on the relationship between the determinant (Technology) and the determined (user centric e-Government services security) (see Sections 3.3 in Chapter 3). To achieve this, SEM1 was extended to include the three moderators in the SEM (see Figure SEM1.0-Initial model) as the initial model.

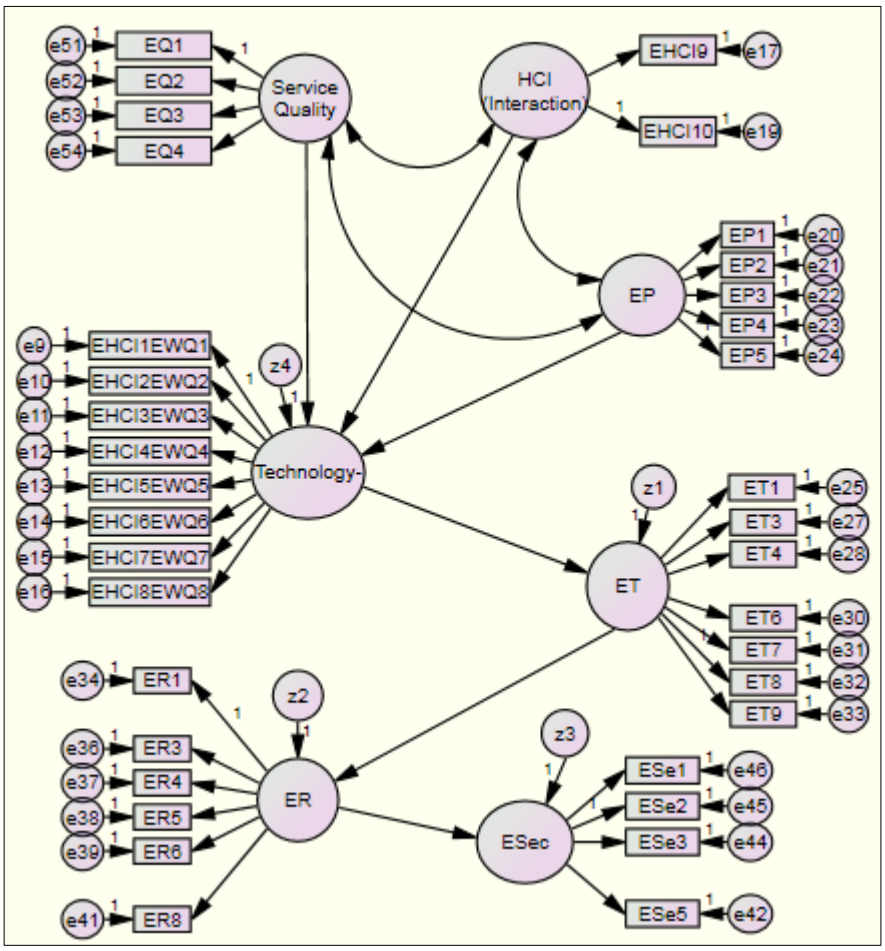

Figure 5.13: SEM1.0-Initial Model, Moderators of Technology-e-Government Security

All the tests detailed out under the Section SEM1 were conducted on this model. To begin with sample correlation amongst the items was examined. All values were found to be less than 0.8. (See Appendix C, Table C10). Additionally SMC values were examined (Table 5.13) and all values were seen to be above the minimum of 0.3.

	Estimate
EQ4	.668
EQ3	.745
EQ2	.736
EQ1	.665
ET9	.665
ESe5	.712
ESe3	.596
ESe1	.653
ESe2	.703
ER8	.479
ER6	.649
ER5	.564
ER4	.672
ER3	.677
ER1	.581
ET1	.718
ET3	.690
ET4	.744

	Estimate
ET6	.681
ET7	.694
ET8	.628
EHCI9	.783
EHCI10	.643
EP1	.749
EP2	.757
EP3	.816
EP4	.747
EP5	.726
EHCI8EWQ8	.691
EHCI7EWQ7	.723
EHCI6EWQ6	.651
EHCI5EWQ5	.757
EHCI4EWQ4	.705
EHCI3EWQ3	.688
EHCI2EWQ2	.704
EHCI1EWQ1	.741

Table 5.13: SMC for Model SEM1.0

Residual covariance readings in some cases were exceeding ±0.2 (see Appendix C, Table C6). Five items namely EP1, EP2, EP3, EP4 and EP5 appear to contribute to this problem and were deleted. The resulting residual covariance readings were within ±0.2 (see Appendix C, Table C17). The standardized residual covariance readings were correspondingly found to be within ±2.0 (see Appendix C, Table C18). This result of this test was that the construct ER deleted from the model as it was found to cause problems in the residual measurements. The resulting model is provided in Figure 5.14.

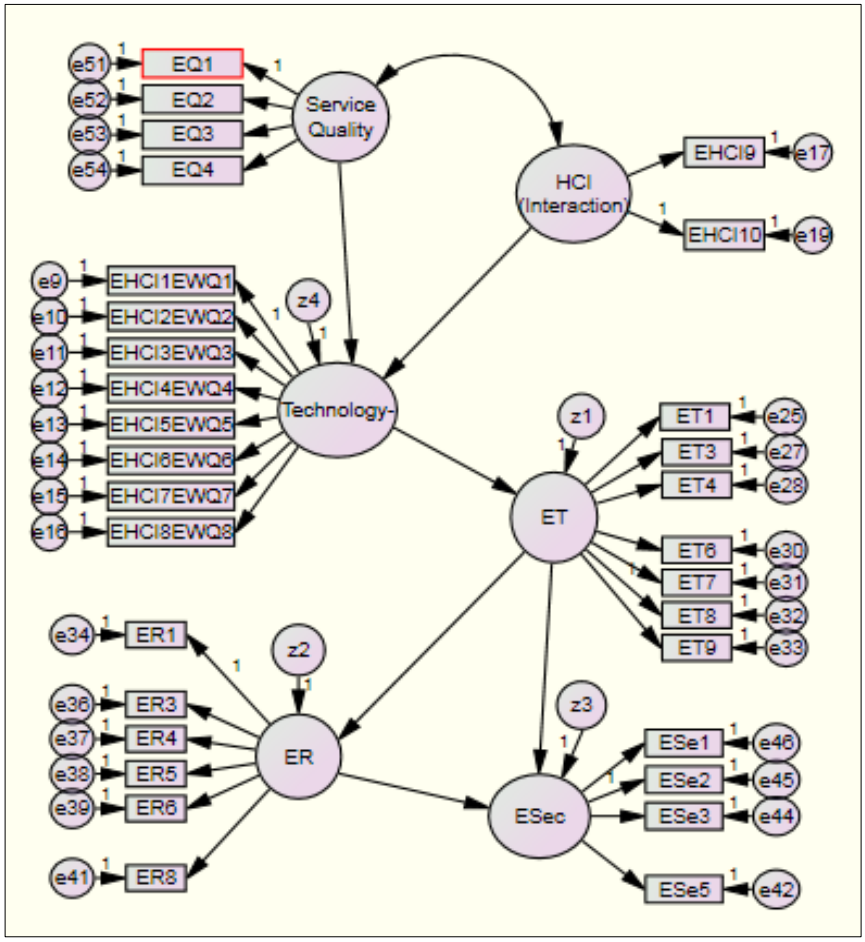

Figure 5.14: AMOS-SEM1.0-Initial Model-after Deleting EP

Construct reliability reading is greater than variance extracted reading (see Appendix C, Table C23) indicating the presence of discriminant validity. Model fit indices show that RMR (0.046), NFI (0.899), IFI (0.944), TLI (0.938), CFI (0.943) and RMSEA (0.061) were satisfactory (see Appendix C, Table C19, Table C20, and Table C21). Chi-square test (see Table 5.14) was found to be unsatisfactory indicating probable non-normality of data.

Model	NPAR	CMIN	DF	P	CMIN/DF
Default model	69	913.594	427	.000	2.140
Saturated model	496	.000	0		
Independence model	31	9071.310	465	.000	19.508

Table 5.14: CMIN, AMOS-SEM1.0-Initial Model-after deleting EP

Bollen-Stine test was conducted and the null hypothesis was accepted at a Bollen-Stine p-value of 0.054. Further, the regression weights report produced by AMOS was examined and is

provided in Table 5.15. The readings show that the relationship between the endogenous and exogenous variables is statistically significant as the p-values are below 0.05.

			Estimate	S.E.	C.R.	P	Label
Technology-	<---	Service_Quality	.735	.086	8.579	***	par_28
Technology-	<---	HCI_(Interaction)	.394	.085	4.657	***	par_30
ET	<---	Technology-	.942	.057	16.467	***	par_29
ER	<---	ET	-.203	.066	-3.064	.002	par_27
ESec	<---	ER	-.087	.040	-2.174	.030	par_23
ESec	<---	ET	.827	.062	13.309	***	par_31

Table 5.15: Standardized Regression Weights SEM1.0

5.7.2 Model Identification

From equation ① the number of data points (Figure 5.14) were calculated as [37(37+1)] ÷ 2 = 703. That is to say, there are 37 variances and 666 covariances. The number of parameters to be estimated is the sum of 29 regression coefficients, 29 variances, 6 regression coefficients between the constructs, 4 variances related to exogenous constructs (z1, z2, z3 and z4) and 1 covariance, which is equal to 69. Thus, the model has 703-69 = 634 fewer parameters than what is available in the model. It can be seen that the number of parameters (634) are fewer than the number of data points (703) indicating that the model is identified (see Section 5.6.1.2).

Furthermore, measure selection to data preparation step remains the same as Section 5.6.1.4. Next model fit was examined which included test of parsimony, testing the minimum sample discrepancy function for acceptability of the model fit, assessing population discrepancy measures, comparing baseline model and checking the goodness of fit index. As described under Section 5.6.1.5, parsimony was tested using the condition that the model has few free parameters or relatively many degrees of freedom. Table 5.16 provides the report from AMOS.

Model	NPAR	CMIN	DF	P	CMIN/DF
Default model	69	913.594	427	.000	2.140
Saturated model	496	.000	0		
Independence model	31	9071.310	465	.000	19.508

Table 5.16: Parsimony of SEM1.0

It can be seen that the number of parameters 69 is relatively lower than the degrees of freedom (427) which indicates that the model is parsimonious. From Section 5.6.1.6, it can be seen that CFI can be used as the measure of the sample discrepancy function and should be greater than 0.9. From Table 5.17, it can be seen that CFI exceeds 0.9 and hence it can be concluded that the sample discrepancy is minimum.

Model	NFI Delta1	RFI rho1	IFI Delta2	TLI rho2	CFI
Default model	.899	.890	.944	.938	.943
Saturated model	1.000		1.000		1.000
Independence model	.000	.000	.000	.000	.000

Table 5.17: Baseline Comparisons SEM1.0

As far as assessment of population discrepancy measure was concerned RMSEA report produced by AMOS was used (see Section 5.6.1.8). From Table RMSEA SEM1 it can be seen that RMSEA reading is within the range 0.06 to 0.08. Thus it is possible to conclude that population discrepancy is minimum.

Model	RMSEA	LO 90	HI 90	PCLOSE
Default model	.061	.055	.066	.001
Independence model	.245	.241	.250	.000

Table 5.18: RMSEA SEM1.0

A comparison of the baseline model was done using the Table 5.8 (see Section 5.6.1.6). Report from AMOS clearly indicates that three of the goodness fit indices namely IFI, TLI and CFI are close to the saturation model and above the zero value indicated against the independence model. This test indicates that the model fits to the data appropriately.

Model	NFI Delta1	RFI rho1	IFI Delta2	TLI rho2	CFI
Default model	.899	.890	.944	.938	.943
Saturated model	1.000		1.000		1.000
Independence model	.000	.000	.000	.000	.000

Table 5.19: Baseline Comparisons SEM1.0

Goodness fit of the model was assessed using three fitness indices namely IFI, TLI and CFI (see Section 5.6.1.9). From Table 5.19, it can be seen that IFI, TLI and CFI are above 0.9 confirming goodness fit of the model. Next step involved model analysis (estimation of the model) and the steps provided under Section 5.6.1.10 were followed, and for this the unstandardized and standardized outputs from AMOS have been provided (see Figures 5.15 and Figures 5.16).

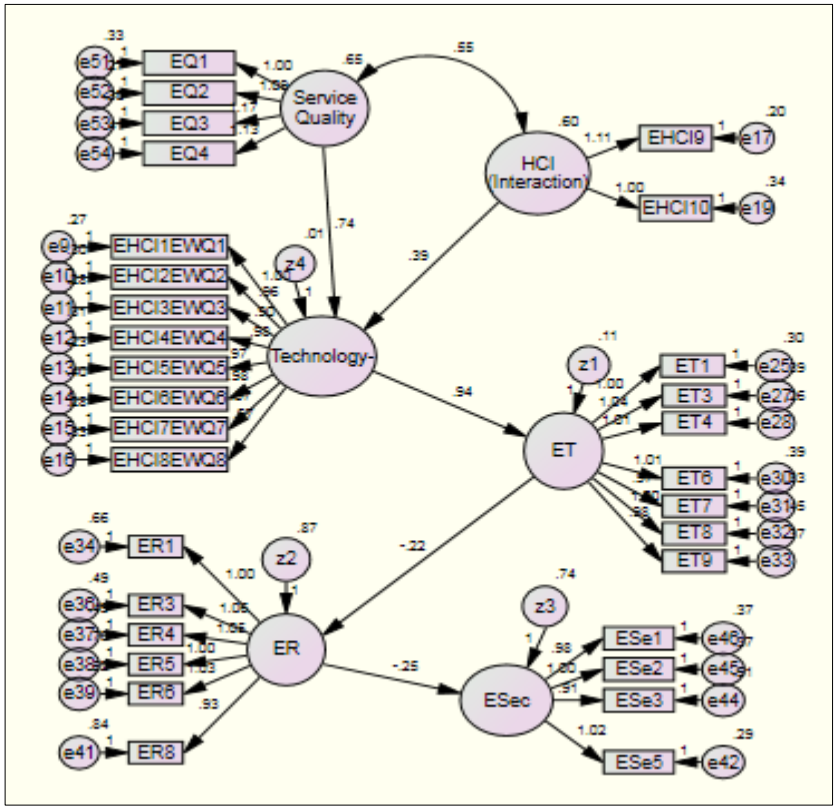

Figure 5.15: SEM 1.0 (Unstandardised)

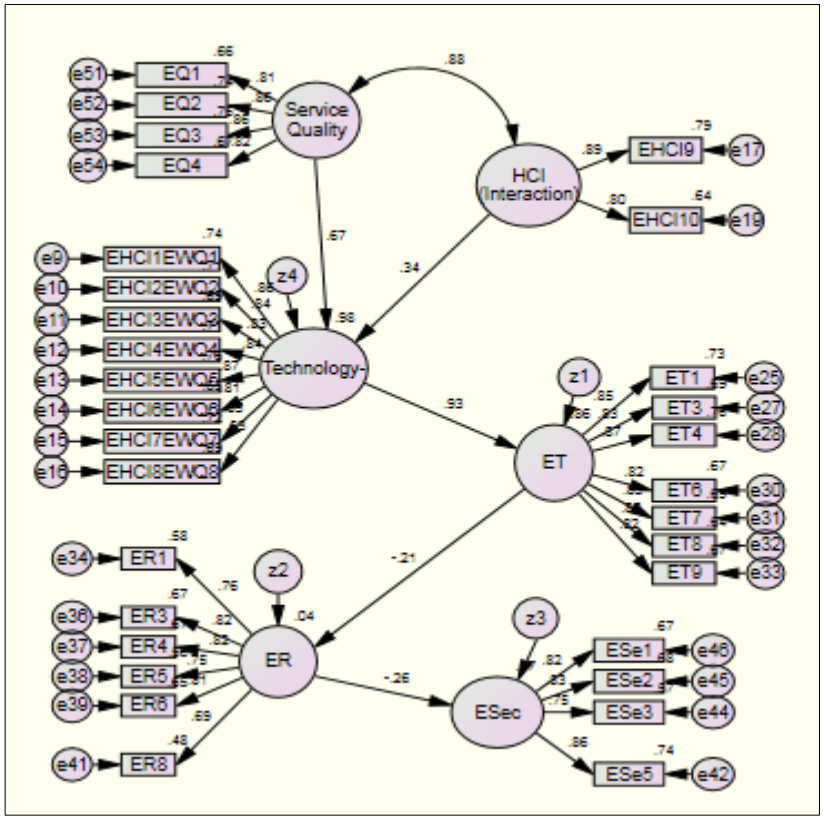

Figure 5.16: SEM 1.0 (Standardised)

SMC, parameter summary, sample correlation, standardized residual covariance and goodness fit of the model were tested and found to be within acceptable limits (see Sections 5.6.1.10). Thus, the initial model provided in Figure 5.14 is accepted. Once the initial model is accepted, then the path analysis was conducted details of which are given next.

5.7.3 Path Analysis of SEM1.0

From Table 5.15, it can be seen that all the paths connecting the latent constructs are significant established by the p-value of significance which is less than 0.05. Thus, the identified model provides the basis to explain the influence of the moderators namely service quality and HCI on the relationship between the constructs technology and user centric e-Government services. In order to do this, SMC readings were used to explain how the moderators account for the variance in the dependent variables. Table 5.20 (constructs) provides the SMC report of AMOS.

	Estimate
Technology	.984
ET	.878
ER	.036
ESec	.691

Table 5.20: SMC, SEM1.0 (Constructs)

It can be seen from Table SMC, SEM1.0 (constructs) that moderators account for:

- 98.4% of variance of technology
- 87.8% of variance of ET
- 3.6% of variance of ER
- 69.1% of variance of ESec

An important aspect that needs to be understood here is that if one compares the variance accounted for by the exogenous variables in the endogenous variables in the presence of moderators with that of the situation when moderators are not present (see Section 5.6.1 and Table 5.11), then it is evident that moderators have affected the variance accounted for in the endogenous variables. This can be explained by arguing that when quality of website design and human computer interaction are taken into consideration they certainly influence the technological aspects that in turn influences user centric e-Government services security. Another important finding is that user privacy is not found statistically significant to be a moderator of the relationship between technology and user centric e-Government services security (see Section 5.6 above). This may be because users have felt that privacy concerns are not necessarily related to technological factors but others. A reasonable assumption that could

be made here is that changes in technology do not seem to bother the users with regard to privacy to that extent as much as it affects other factors such as user trust or user risk or e-Government services security. Since the invention of internet over two decades ago there is a metamorphic change witnessed in the technological front like from personal computers to laptop computers to tablets to mobile gadgets as also from simple e-mail transactions to e-Government transactions. Such changes must have made the participants feel that technological changes could be less of a concern with regard to privacy issues as they might have experienced less number of difficulties that have arisen due to change in technology. This is only an inference that needs to be further examined in future research.

Another important aspect that needs to be examined is the influence of technology on user trust, user felt risk and user centric e-Government services security in the absence and presence of moderators. This can be done by comparing Tables Table 5.10 and Table 5.15. One can see that the variance accounted for by technology on trust is higher (.942) in the presence of moderators than in their absence (0.914). Same effect can be seen with respect to the relationships ET→ESec, ET→ER and ER→ESec. Thus it is reasonable to infer that the presence of moderators enable a better understanding of how technology influences user centric e-Government services security. Thus, using the above arguments and the Table 5.15, it is possible to verify and accept or reject the following hypotheses.

Accepted hypotheses

- H1a: Human computer interaction positively influences the relationship between e-Government technology and user centric e-Government security.
- H1c: Web design quality positively influences the relationship between e-Government technology and user centric e-Government security.
- H2: e-Government technology positively influences user trust in e-Government services.
- H3a: User trust on e-Government negatively influences user centric e-Government security.
- H3b: User trust on e-Government negatively influences the risk felt by users of e-Government.
- H4: User felt risk negatively influences user centric e-Government security.

Rejected hypothesis

- H1b: User privacy positively influences the relationship between e-Government technology and user centric e-Government security.

A summary of the table of the verified hypothesis is given in Table 5.21.

Hypothesis No.	Hypothesis	Exogenous Latent Constructs	Endogenous Latent Construct	Results of Hypotheses verification	Explanation
H1a	Human computer interaction positively influences the relationship between e-Government technology and user centric e-Government security	HCI	Technology	**Accepted**	Human computer interaction **moderates** technology positively
H1b	User privacy positively influences the relationship between e-Government technology and user centric e-Government security	EP	Technology	**Rejected**	User privacy does not **moderate** technology
H1c	Web design quality positively influences the relationship between e-Government technology and user centric e-Government security	Service Quality	Technology	**Accepted**	Web design quality **moderates** technology positively
H2	E-Government technology positively influences user trust in e-Government services	Technology	ET	**Accepted**	Technology positively and significantly influences ET
H3a	User trust on e-Government negatively influences user centric e-Government security	ET	ESec	**Accepted**	ET positively and significantly influences ESec
H3b	User trust on e-Government negatively influences the risk felt by users of e-Government	ET	ER	**Accepted**	ET negatively and significantly influences ER
H4	User felt risk negatively influences user centric e-Government security	ER	ESec	**Accepted**	ER negatively and significantly influences ESec

Table 5.21: Summary of the Significant Influence of Determinant on e-Government Security

The resulting model that is accepted is given in Figure 5.17.

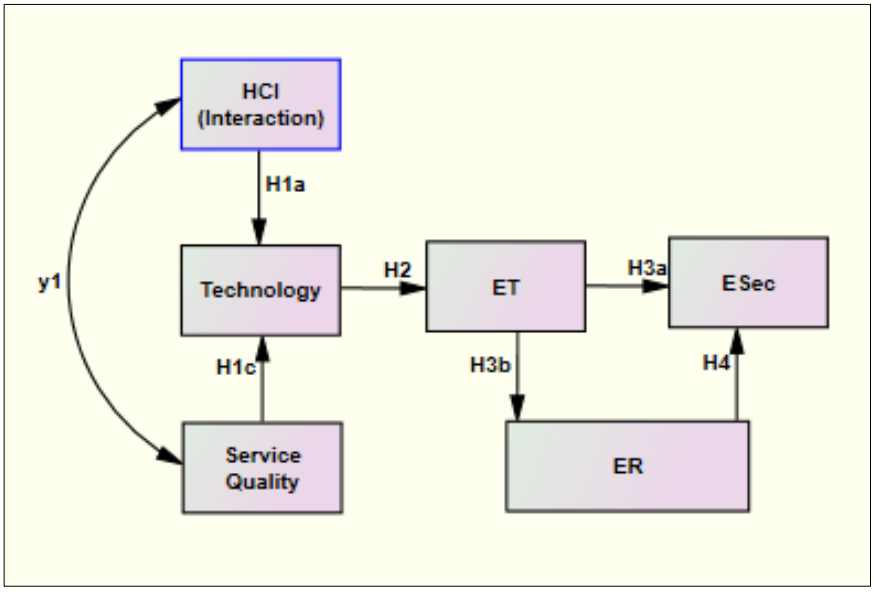

Figure 5.17: SEM 1.0 (Final Model)

Further the covariance (γ1) amongst the endogenous variables namely HCI and Service Quality has been measured and provided in Table Covariance HCI and Service Quality which shows that the covariance HCI (Interaction) <--> Service Quality is high and the endogenous variables are interrelated.

			Estimate	S.E.	C.R.	P	Label
HCI_(Interaction)	<-->	Service_Quality	.552	.059	9.285	***	par_32

Table 5.22: Correlations HCI and Service Quality

The measure of 0.552 indicates that the human computer interaction is highly associated with web design quality suggesting that when the web design quality is high then the user interaction with e-Government portal is high. Next, the impact of the technology on user centric e-Government services security was verified by analyzing whether perceived ease of use and usefulness affect user trust and hence its relationship to user centric e-Government services security.

5.7.4 SEM2

For convenience the figure related to the second part of the analysis is reproduced below.

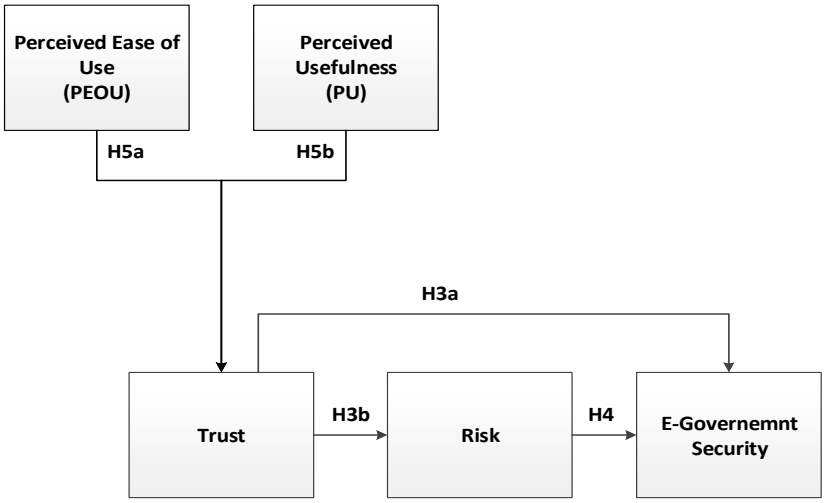

Figure 5.18: SEM2 For Analyzing Perception of Users of E-Government Security Characterized by Cloud Computing (Part 2)

From Figure 5.2 and Section 5.5, it can be seen that perceived ease of use (PEOU) and perceive usefulness (PU) have been analyzed for reliability, validity and goodness fit at the CFA level. Moving further to the next step of structural equation modelling, the impact of change in technology on user centric e-Government security was conducted to using two important constructs that have direct relationship to user perception namely PEOU and PU based on Chapter 3. Figure 5.19 was used for conducting structural equation modelling as the initial model.

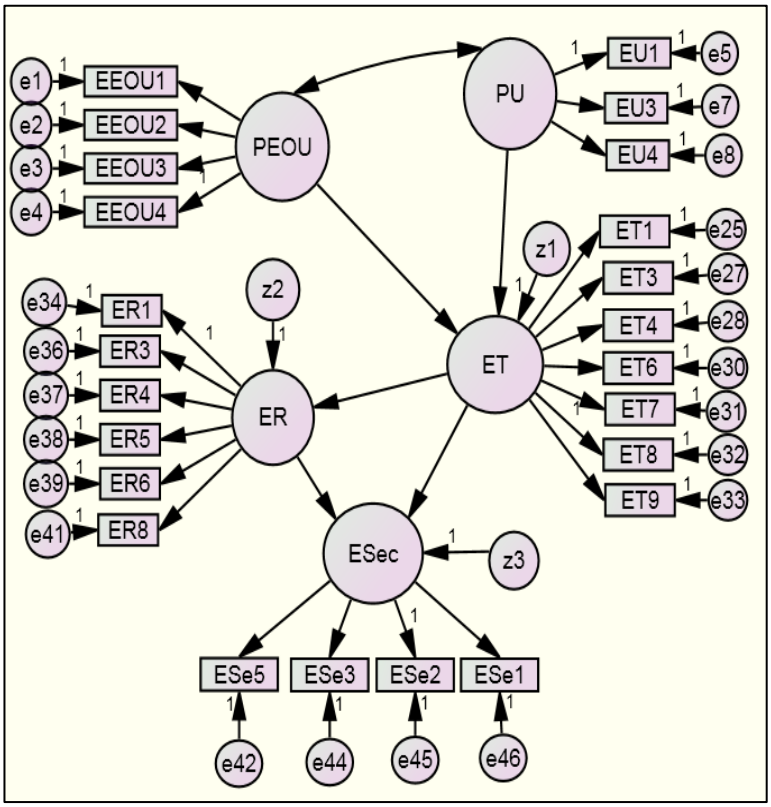

Figure 5.19: SEM2

All the tests detailed out under the Section SEM1 were conducted on this model. Sample correlation amongst the items was examined and were found to be less than 0.8. (See Appendix C, Table C22). Additionally SMC values were examined (Table 5.23) and all values were seen to be above the minimum of 0.3.

	Estimate
ET9	.670
ESe5	.710
ESe3	.594
ESe1	.658
ESe2	.703
ER8	.479
ER6	.649
ER5	.564
ER4	.672
ER3	.677
ER1	.581
ET1	.719
ET3	.670
ET4	.753
ET6	.684
ET7	.703
ET8	.626
EU4	.740
EU3	.818

	Estimate
EU1	.761
EEOU1	.729
EEOU2	.765
EEOU3	.745
EEOU4	.615

Table 5.23: SEM2, SMC

Construct reliability reading is greater than variance extracted reading (see Appendix C, Table C24). Residual and standardized residual covariance readings were within ±0.2 and ±2.0 respectively (see Appendix SEM 2- SEM2-Residual Covariances and SEM2-Standardized Residual Covariances). Model fit indices show that RM R (0.055), NFI (0.924), RFI (.915), IFI (0.962), TLI (0.957), CFI (0.961) and RMSEA (0.055) were satisfactory. Chi-square test (see Table 5.24) was found to be unsatisfactory indicating probable non-normality of data.

Model	NPAR	CMIN	DF	P	CMIN/DF
Default model	54	476.126	246	.000	1.935
Saturated model	300	.000	0		
Independence model	24	6253.003	276	.000	22.656

Table 5.24: Chi-square test

Bollen-Stine test was conducted and the null hypothesis was accepted at a Bollen-Stine p-value of 0.08. Regression weights report produced by AMOS was examined (see Table 5.25). The readings show that the relationship between the endogenous and exogenous variables is statistically significant as the p-values are below 0.05.

			Estimate	S.E.	C.R.	P	Label
ET	<---	PEOU	.513	.134	3.820	***	par_20
ET	<---	PU	.386	.128	3.002	.003	par_21
ER	<---	ET	-.201	.067	-3.017	.003	par_19
ESec	<---	ER	-.089	.040	-2.220	.026	par_17
ESec	<---	ET	.824	.062	13.306	***	par_22

Table 5.25: Standardized Regression Weights SEM2

5.7.5 Model Identification

From equation ① the number of data points (Figure 5.19) were calculated as [27(27+1)] ÷ 2 = 378. That is to say, there are 27 variances and 351 covariances. The number of parameters to be estimated is the sum of 25 regression coefficients, 25 variances, 5 regression coefficients between the constructs, 3 variances related to exogenous constructs (z1, z2 and z3) and 1 covariance, which is equal to 59. Thus, the model has 378-59 = 319 fewer parameters than what is available in the model. It can be seen that the number of parameters (319) are fewer than the

number of data points (378) indicating that the model is identified (see Section- 5.6.1.2). Measure selection to data preparation step remains the same as Section 5.6.1.4.

5.7.6 Model Fit

This included test of parsimony, testing the minimum sample discrepancy function for acceptability of the model fit, assessing population discrepancy measures, comparing baseline model and checking the goodness of fit index. As described under Section 5.6.1.5, parsimony was tested using the condition that the model has few free parameters or relatively many degrees of freedom. Table bb shows that the number of parameters 59 is relatively lower than the degrees of freedom (246) indicating that the model is parsimonious. CFI is greater than 0.9 indicating that the sample discrepancy is minimum (see Table 5.26).

Model	NFI Delta1	RFI rho1	IFI Delta2	TLI rho2	CFI
Default model	.924	.915	.962	.957	.961
Saturated model	1.000		1.000		1.000
Independence model	.000	.000	.000	.000	.000

Table 5.26: Baseline comparison SEM2

RMSEA provided the measure to test the population discrepancy. From Table 5.27, it can be seen that RMSEA is within 0.06 indicating that the population discrepancy is minimum.

Model	RMSEA	LO 90	HI 90	PCLOSE
Default model	.055	.048	.062	.126
Independence model	.265	.259	.271	.000

Table 5.27: RMSEA SEM2

The independence of the model was determined by the goodness fit indices. Table 5.26 shows that NFI, RFI, IFI, TLI and CFI are close to the saturation model and above the zero value confirming the independence of the model. This test indicates that the model fits the data. The same table enabled the assessment of the goodness fit of the model using NFI, RFI, IFI, TLI and CFI all of which are above 0.9. Thus from the foregoing discussions it can be concluded that the model fitness has been tested satisfactorily.

5.7.7 Model Analysis (Model Estimation)

Both unstandardized and standardized AMOS diagrams will be reported as has been explained in earlier sections (see Sections 5.6.1.10). Thus Figures 5.20 (Unstandardized) and Figures 5. 21 (Standardised) have been provided below.

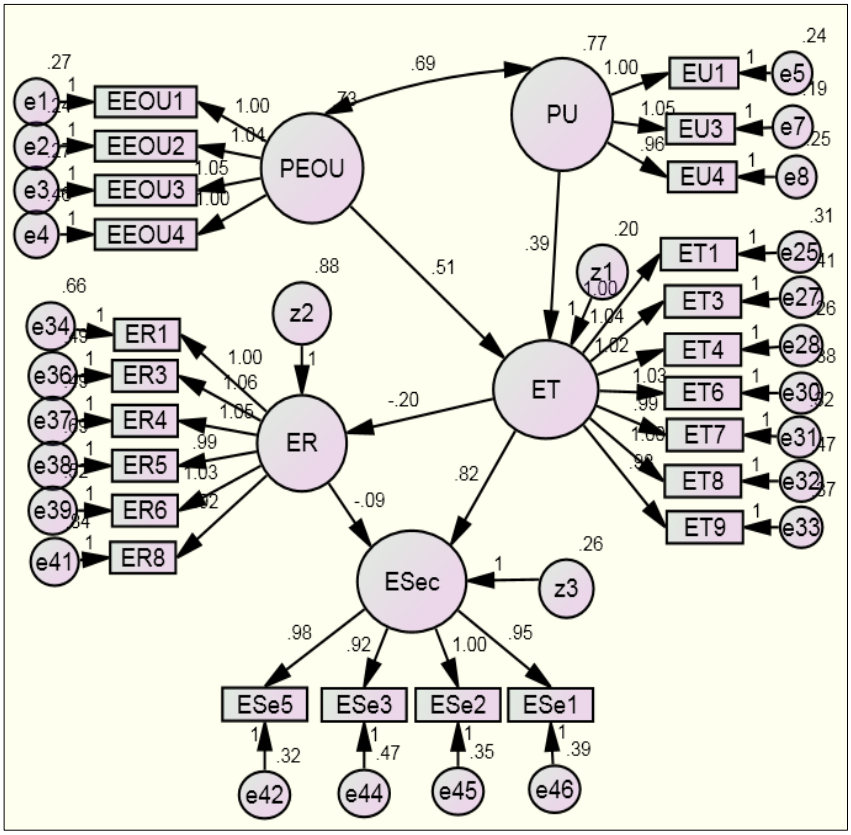

Figure 5.20: SEM2 (Unstandardized)

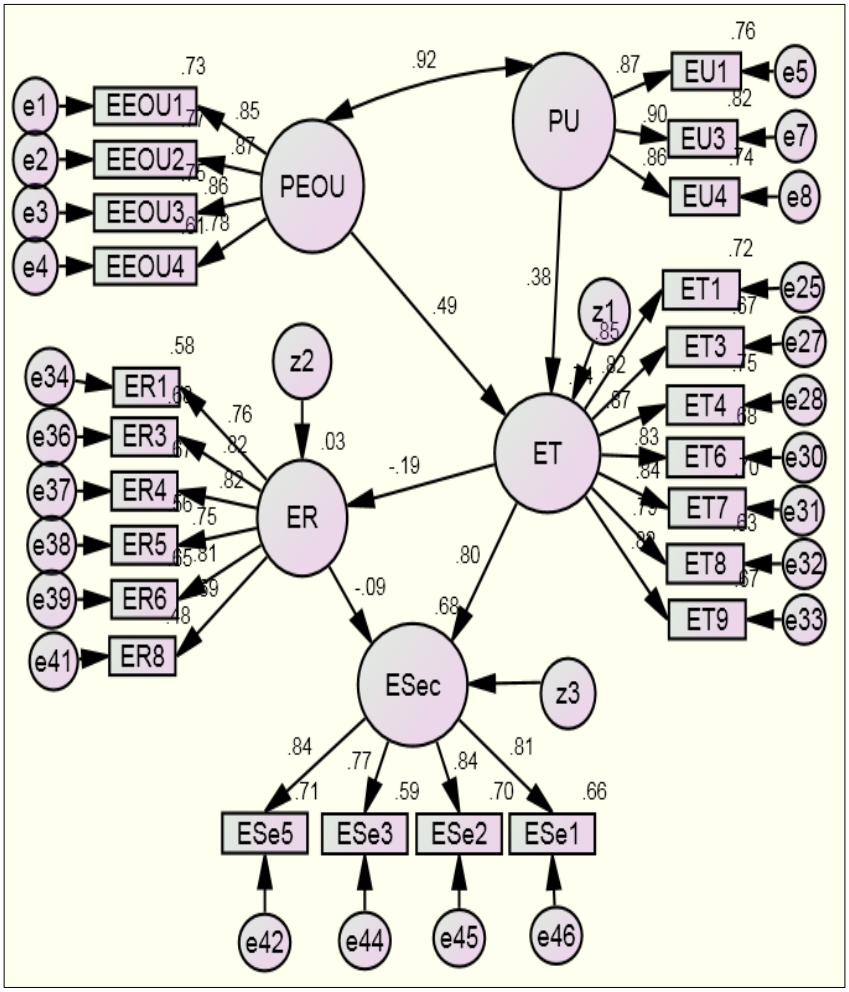

Figure 5.21: SEM2 (Standardized)

SMC, parameter summary, sample correlation, standardized residual covariance and goodness fit of the model were tested and found to be within acceptable limits (see Sections 5.5.2 and 5.6.1.9). Thus, the initial model provided in Figure SEM2 is accepted. Following this the path analysis was conducted.

5.7.8 Path Analysis of SEM2

First Table 5.25 was used for analyzing the paths connecting the latent variables to see whether paths are statistically significant (p-value of significance less than 0.05) and the table shows that the paths are statistically significant. Next the identified model (see Figure 5.21) was used to explain the relationship between PEOU and PU on the one hand and user centric e-Government security on the other mediated by user trust and user felt risk. SMC values provided the basis to explain the extent to which PEOU and PU accounted for the variance in the dependent variables. Table 5.28 (constructs) provides SMC report from AMOS which shows that PEOU and PU account for 73.8% of variance in ET, 3.5% variance in ER and 68.5% variance in ESec.

	Estimate
ET	.738
ER	.035
ESec	.685

Table 5.28: SMC, SEM2 (constructs)

The above findings can be explained in a way that when users perceive the ease of use and usefulness of transacting through an e-Government portal characterized by change in technology (cloud computing in this instance), then the trust level in the users varies. So also is the case with regard to user centric e-Government security. However the variance in the user felt risk accounted for by PEOU and PU is not very high which could be explained in way that users are not particularly concerned with risk due to the high level trust they have developed in the changed technology. One reason for this could be is that in an environment wherein users are facing frequent change in technology (for instance one could see in the modern era that electronic applications are frequently affecting e-Government such as the introduction of Facebook, Instagram, Skype and the like) it is possible that users have developed certain level of trust in the new technologies which might automatically reduce their feeling of risk in the technology due to lower number of incidences the users might have encountered while using those new technologies. Thus, a lower variance in ER could be expected.

Further from Table 5.28, it can be seen that the paths PEOU→ET, PU→ET, ET→ESec, ET→ER and ER→ESec are all statistically significant with the regression coefficients showing that PEOU and PU influence ET positively; ET influence ESec positively while ET influences ER negatively and ER influences ESec negatively. That is to say that when PEOU and PU are high, ET is high; ET is high, ESec is high; ET is high ER is low; and ER is low, ESec is high. The above arguments can then be used to verify whether the hypotheses related to model (Figure 5.21), SEM2 for analyzing perception of users of e-Government security characterized by cloud computing) are accepted or not. Thus, the following hypotheses are accepted.

- H3a: User trust on e-Government negatively influences user centric e-Government security.
- H3b: User trust on e-Government negatively influences the risk felt by users of e-Government.
- H4: User felt risk negatively influences user centric e-Government security.

- H5a: Perceived ease of use of e-Government services positively influences user trust in e-Government.
- H5b: Perceived usefulness of e-Government services positively influences user trust in e-Government.

The above findings are summarized in Table Summary of results of SEM2.

Hypothesis No.	Hypothesis	Exogenous Latent Constructs	Endogenous Latent Construct	Results of Hypotheses verification	Explanation
H3a	User trust on e-Government negatively influences user centric e-Government security	ET	ESec	**Accepted**	ET positively and significantly influences ESec
H3b	User trust on e-Government negatively influences the risk felt by users of e-Government	ET	ER	**Accepted**	ET negatively and significantly influences ER
H4	User felt risk negatively influences user centric e-Government security	ER	ESec	**Accepted**	ER negatively and significantly influences ESec
H5a	Perceived ease of use of e-Government services positively influences user trust in e-Government	PEOU	ET	**Accepted**	PEOU positively and significantly influences ET
H5b	Perceived usefulness of e-Government services positively influences user trust in e-Government	PU	ET	**Accepted**	PU positively and significantly influences ET

Table 5.29: Summary of Results of SEM2

The resulting final model that is statistically tested and accepted is provided in Figure 5.22.

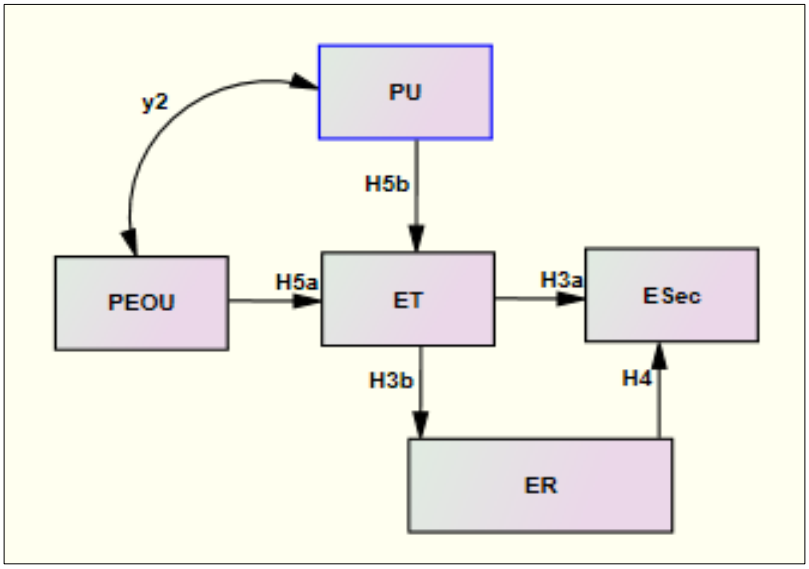

Figure 5.22: SEM2 (Final Model)

Further correlation (γ2) amongst the endogenous variables namely PEOU and PU has been provided in Table Covariance PEOU and PU which shows that the covariance PEOU<-->PU is high and the endogenous variables are interrelated.

			Estimate	S.E.	C.R.	P	Label
PEOU	<-->	PU	.685	.070	9.735	***	par_18

Table 5:30: Covariance PEOU and PU

The measure of 0.685 indicates that the perceived ease of use of e-Government technology is highly associated with perceived usefulness of the e-Government technology suggesting that when the perceived ease of use is high then the users perceive that the e-Government technology is useful. That is to say, that cloud computing technology is perceived to be easy to use and useful by the users, which is reflected, in the high trust users have on the technology and the consequent feeling of high security by the users.

After analyzing the models, the next step taken was to test the unidimensionality of the models. The following section deals with unidimensionality.

5.8 Unidimensionality

Uunidimensionality was tested by examining the values reported by AMOS under the table Regression Weights for the three models in Figures 5.9 (Unstandardized), Figures 5.9 (Standardised) and Figures 5.21 (Standardized). For these three models Regression Weights tables proceed by AMOS were analyzed (see Appendix C, Table 9). Two important parameters were examined. They were the values under the column ‘estimates’ and the other the values

under the column 'C.R'. According to Janssens et al., (2008), none of the values pertaining to the items under the estimate column should be less than 0.5 and the C.R. column should be less than ± 1.96. An inspection of the tables under Appendix C, models clearly demonstrates that this condition has been satisfied indicating that the models are unidimensional. Further to testing the unidimensionality, the final test that was conducted was the assessment of the common method bias. The next section discusses this measurement.

5.9 Common Method Bias

As explained in Section 4.10.11, common method bias was tested by measuring the average variance extracted (AVE). Table 5.31 was used to assess AVE for the CFA model in Figure 5.3. The table was constructed from two reports generated by AMOS. They are the SMC of the constructs used in the model and the correlations table both generated by AMOS (see Appendix C). If there exists common method bias in the responses, then the squared multiple correlation (SMC) value of the constructs (the variance) extracted indicated by bold numbers in the Table 5.31, would be less than 0.5 and any or all of the other correlation values measured between the variable indicated on the top of the column and any other variable will be higher than the AVE of the variable. For instance under the column PU the SMC of PU is given in bold letters as 0.969. No other correlation between PU and the remaining variables exceed 0.969. Thus since all the SMC values are above 0.5 and the correlation between the main variable in a column and other variables in the table do not exceed the SMC of the main variable, it can be said that common method bias is absent. However, one notable exception is there.

	PEOU	**PU**	**HCI**	**EP**	**EQ**	**Technology**	**ET**	**ER**	**ESec**
PEOU	**0.961**								
PU	0.846	**0.969**							
HCI	0.882	0.841	**0.960**						
EP	0.082	0.041	0.048	**0.952**					
EQ	0.769	0.819	0.790	0.052	**0.960**				
Technology	0.878	0.880	0.897	0.074	0.906	**0.966**			
ET	0.682	0.682	0.694	0.061	*0.982*	0.806	**0.956**		
ER	0.051	0.017	0.033	0.448	0.032	0.038	0.033	**0.912**	
ESec	0.709	0.709	0.692	0.105	0.643	0.663	0.645	0.060	**0.946**

Table 5.31: AVE (Average Variance Extracted)

That is the correlation between ET and EQ, which is reported as 0.982 and is exceeding the AVE of EQ, which is 0.960. This exception was allowed as further analysis showed that the composite reliability of the three structural models was found to be within acceptable limits (see

Sections related construct reliability). Thus, it can be concluded that common method bias was not found in the responses.

From the foregoing discussions, it can be concluded that the initial e-Government security model has not changed and was treated as finally specified research model.

5.9 Summary

This chapter has provided a comprehensive discussion on the statistical analysis conducted on the research models developed for this research. The chapter enabled the researcher to optimize on the number of factors that must be used in the models, number of latent variables to be used in the models and the number of observed variables to be used in the models using CFA. The resulting models were evaluated and analyzed using SEM. Hypotheses were tested. Findings have been derived. Thus, the findings in this chapter set the basis for discussions in Chapter 6.

Chapter 6: Discussion

6.1 Introduction

In the previous chapter the outcomes of the data analysis have been provided that pertain to the models depicted in Chapter 3 alongside the findings derived from the rigorous data analysis. These findings have been used by the researcher to answer the research questions in this chapter. The chapter is organized by providing discussion about the answer to research question one, follows by discussion about the answer to research question two, then analytical discussion about the relationship between the constructs and then ending chapter summary.

6.2 Research Question RQ1: What are the Factors that can be Considered as User-Centric and Affect E-Government Services Security?

E-Government is a service that affects users. User centric e-Government services are usually understood as a service that complies with the needs and wishes of citizens within a context (van Velsen et al., 2009). Literature review (see Chapter 2) shows that a number of factors related to e-Government affect user needs and wishes including those that are contextual, behavioral, managerial, organizational, technical and environmental in nature. Specific user centric factors that have been identified in Chapter 2 as affecting users include e-Government security (organizational factor), user felt risk (behavioral factor), user trust (behavioral factor), e-Government technology (contextual/environmental factor), web design quality (managerial factor), user privacy (behavioral factor), HCI (contextual factor), perceived ease of use of e-Government technology (behavior), perceived usefulness of e-Government technology (behavior), demography and culture (contextual factors). The above factors either enable users to fulfill their needs and wishes or can act as barriers if they are not addressed taking into account the user needs and wishes by the service providers. It must be recognized here that there are a number of other factors that have been identified in the literature as affecting users of e-Government including awareness, user access, user adoption, user attitude and others (Chapter 2) which have not been considered in this research. The reasons for considering the factors mentioned above only are highlighted in Section 2.6. In addition, the importance of the factors to e-Government has been widely acknowledged in the literature and arguments have been posted in the literature to include them in any research involving e-Government and its users and their usefulness in expanding current research outcomes. For instance Shah et al. (2014)

who have developed a model to study the influence of antecedents of online security, suggested that trust and risk must be included as antecedents of online security. These arguments and similar others determined the choice of the factors in this research that are considered as user-centric. In addition, in this research user centric e-Government security was chosen as the main factor for study, reason for which have been outlined in Sections 2.5, 2.6, 2.7 and 2.11. Which includes lack of knowledge on how user concern on e-Government security can act as a barrier to the success of e-Government and how user needs and wishes regarding their security if not taken into consideration could impact e-Government services.

The reason for identifying the factors and focusing on them was their reported (see Chapter 3) influence on online security and user centricity as those factors have been argued to be affecting user centric e-Government security an area of research that was promising to reveal knowledge that could be useful in managing e-Government services. Especially if one considers the needs and wishes of the users, these factors have been found to affect them. For instance studying how those factors affect user centric e-Government security was expected to produce knowledge that could be useful to users when contexts change, especially when technology as a contextual factor changes.

However, there was a need to know more about how those factors could be related to user centric e-Government service security for they did not belong to a single category and research related to those factors has treated them variedly in the literature. For instance while website design has been suggested to be an antecedent of online security (Shah et al., 2014), demographic variables have been used as control variables and independent variables in the extant literature (Hasan, 2015). Thus, there was a need to classify those factors before finding out how they could be related to user centric e-Government service security.

Amongst the different factors that were to be linked to user centric e-Government service security, technology has been identified as the most important factor that could determine user centric e-Government service security (see Chapter 3). This has been supported by both theory and literature (see Sections 2.4, 2.6 and 2.7.2). Thus, the findings of this research point out that e-Government technology is the main determinant of user centric e-Government service security. This was tested in the context of cloud computing technology used by Government of Bahrain in the e-Government services. Statistical tests confirmed that technology could act as the determinant of user centric e-Government service security (see Section 2.7 in Chapter 5). This could be explained by the everyday happening one witnesses where users could be seen to be worried about online security when they get new gadgets such as touch screen devises. There is a corroboration of the findings of the research through real life happenings. In addition, it can

be seen from the findings that technology has a high potential to satisfy user needs and wishes when user centricity is considered and hence becomes a prime factor that needs to be examined for its role on user centric e-Government service security.

Similarly, literature showed that technology does not operate in isolation (see Sections 2.4, 2.6.2 and 2.7). Factors that could affect technology and its relationship with user centric e-Government service security were identified as moderators. The factors identified were HCI, user privacy and web design quality. The reasons for identifying these factors as moderators have been outlined in Section 3.4 (Chapter 3). HCI is vital to the interaction between a user and the e-Government or for that matter any online application. Modern day computing requires users to be familiar with how to navigate, operate and achieve their objectives that have serious implications to security issues. For instance in cloud computing users have the facility to use online computing facilities such as using spreadsheets about which users need to be apprised of. Any wrong operation or improper commands can jeopardise the users leading to data loss or even loss of money if the user is operating a payment gateway. Although these happen every day, the best way by which users could interact with computers without security breaches especially in online applications is an area of deep concern. The study on this subject until now has been largely restricted to the technology specialists although a deeper look into this aspect revealed that management concepts need to be addressed as well. For instance, how to depict icons on the computer screen in a way by which user interaction is ensured to be safe and what is the most suitable way by which user interaction could be made efficient are concerns pertaining to management. However, studies concerning HCI with regard to online applications, viewed from managerial perspective are rare in the literature. Particularly how HCI moderates the relationship between technology and user centric e-Government service security has hardly been studied and outcomes of any such study could be very useful to designing and developing technological applications that enable safe and better management of user applications by users. Similar arguments could be extended to the choice of user privacy and web design quality although these aspects have been studied to some extent (see Chapter 2). While the rationale and purpose behind the choice of these moderators have been explained above, theoretical support on how such moderation takes place has been provided in Sections 3.4. Further, statistical analysis provided in Chapter 5 point out that except for the factor EP, HCI and web design quality have been found to be moderating the relationship between technology and user centric e-Government service security.

At this stage, the determinant and moderating factors have been identified taking into account user centric e-Government service security. However, an important aspect that has been widely discussed in the e-Government security literature is the influence of contextual factors on user

centric e-Government service security. Although Chapter 2 shows that a number of contextual factors can be considered, in this research three factors were considered namely user education, user experience and nationality. Reasons for the choice have been outlined (see Section 2.6.1 and 2.6.3). Since these factors have been widely discussed in the literature, the purpose of studying these factors was only to know whether they affect user centric e-Government service security or not and if so how when a new technology is introduced in the e-Government services. Interest on these factors is limited to just the examination whether they affect users and user centric e-Government service security in an environment (that is Bahrain) where a new technology has been introduced in the e-Government services. This was achieved by using the three factors as control variables and assessing their influence on the relationship between user trust (a user behavioral factor) and user centric e-Government service security. More factors could be analyzed in a similar fashion. While theoretical support for employing these factors in this study has been provided under Sections 2.5, actual observations in real life clearly show that the influence of user education, experience and nationality have varying influence on user centric e-Government service security. No clear conclusions are drawn in the extant literature on this issue. Hence, there is some consistency that can be seen between empirical outcomes and real life situations. This is once more confirmed in this research. Findings in Chapter 5 show that nationality as a factor did not influence user centric e-Government service security whereas user education and experience did thus corroborating similar propositions found in the extant literature. This also suggests that user centricity in terms of user needs and wishes have to be considered when one considers the contextual factors as the results of this research show that they affect the relationship between the users and user centric e-Government service security.

Furthermore, this research while attempting to explain the relationship between the determinant and user centric e-Government service security, did not limit the examination to just testing the relationship statistically or reviewing the literature. Instead, the researcher went one-step further to check the real situation on the ground. Another test was carried out to know how a change in technology introduced in the e-Government services affects user needs and wishes with regard to user centric e-Government service security. Two factors namely perceived ease of use and usefulness were chosen to understand whether at all the introduction of a new technology namely cloud computing improved user centric e-Government service security when viewed from the angle of user centricity. The choice of these two factors served the purpose of knowing how easy it was to transact through the cloud computing technology based e-Government services and how useful it was. Theoretical support to examine these aspects has been discussed in Chapter 2. While there is hardly any evidence of any such examination conducted by researchers in the extant literature, the results of this research showed that these two factors affected user centric e-Government service security (see Chapter 5). This is

corroborated by the limited evidence available in the literature as well as real life perceptions of users of e-Government services. When the technology is easy to use and useful, users feel that the technology could satisfy their needs and wishes. Thus, PEOU and PU become important user centric predictors of e-Government service security.

Finally two factors namely trust and risk have been used as antecedents of user centric e-Government service security in this research, the rationale for the choice of which has been provided in Chapter 2. There is wide acknowledgement in the literature (see Sections 2.7 and 2.8) which says that trust and risk factors are user centric as they directly affect security issues concerning users when there is change in context. There is evidence in the live interactions of users that suggests that user needs and wishes with regard to e-Government service security are related to user trust and user felt risk when changes are incorporated in the e-Government technology. Statistical analysis in Chapter 5 provides findings to this effect. Theoretical support to suggest the inclusion of these factors as user centric is provided in Chapter 2. Although there is no unique method of including trust and risk while analyzing the relationship between technology and user centric e-Government service security, what is clear is that their influence on the relationship could be brought out in many ways including as mediators. When user centricity is involved, trust and risk direct affect user needs on security and their wish to transact in a secure manner. The findings in Chapter 5 show that both trust and risk do affect user centric e-Government service security thus justifying their inclusion in this research.

In summary, the foregoing discussions have provided knowledge on user centricity, factors that can be considered as user centric and whether they affect user centric e-Government service security. The discussions show that the factors can be classified under many categories. The purpose and reasons behind their choice in this research have been explained. User centric e-Government service security has been identified as the dependent factor. Changing technology has been identified as the determining factor. Need to use of moderators of the relationship between technology and user centric e-Government service security have been identified. Influence of contextual factors that are important to define user centricity of e-Government security have been discussed. Factors that could be used to verify how technology affects user centric e-Government service security in reality have been discussed. Mediating factors that are necessary when examining the relationship between user centric technology and user centric e-Government service security have been examined. Evidence in terms of literature and findings from statistical analysis has been provided. Thus, it can be concluded RQ1 has been answered.

6.3 Research Question RQ2: How Those Factors Affect E-Government Services Security when there is a Change in Technology?

This question has been answered using the findings of the statistical analysis provided in Chapter 5. The analysis uses the findings of the three models SEM1, SEM1.0 and SEM2.

6.4 Analysis of the Relationship Technology–ET-ER-User-Centric e-Government Services Security

This relationship has been analyzed using the paths 'Technology→Trust→e-Government security' and 'Technology→Trust→Risk→e-Government security' shown in Figure 5.12. As explained in Section 5.7, it can be seen that technology as a determinant affects e-Government security through both the paths. However, when one considers the path Technology→Trust→e-Government security the total effect of technology on trust, risk and e-Government services security is given by the AMOS report provided in Table 6.1.

	Technology	ET	ER	ESec
ET	.908	.000	.000	.000
ER	-.171	-.188	.000	.000
ESec	.747	.823	-.093	.000

Table 6.1, Standardized Total Effects (SEM1)

When Table 6.1 is viewed in conjunction with Figure 5.11 it can be seen that Technology as the determinant is affecting ESec, the dependent variable. This finding shows that when technological changes are incorporated, it is essential to consider user-centric e-Government services security an argument supported by both theory and practice (see Chapter 2). Further, from Figure 5.9 and Table 5.10, it can be seen that the relationship Technology→Trust→e-Government security can be decomposed as Technology→Trust and Trust→e-Government security. This decomposition shows that technology affects user trust directly and user trust affects e-Government security directly. In Section 2.7, it has already been shown that Technology→Trust and Trust→e-Government security relationships are significant (β=0.914 and 0.819 respectively). That is to say, that 91.4% of variation in user trust is predicted by technology whereas 81.9% of the variation in e-Government security is predicted by user trust. Thus, when one takes the complete relationship Technology→Trust→e-Government security then it can be seen that technology has an indirect effect on e-Government security, which is explained by Table 6.2 in conjunction with Figure 5.11.

	Technology	ET	ER	ESec
ET	.000	.000	.000	.000
ER	-.171	.000	.000	.000
ESec	.747	.017	.000	.000

Table 6.2 Standardized Indirect Effects

From Table 6.2 it can be seen that technology is exerting an indirect influence on ESec. In terms of regression coefficients the indirect effect of technology on e-Government security is computed as [0.914 (Technology→Trust) x 0.819 (Trust→e-Government security)] = 0.75. This can be interpreted in a way that a one standard deviation change in technology effects a 0.75 standard deviation change on e-Government security.

A similar analysis can be made with regard to the path Technology→Trust→Risk→e-Government security, which can be decomposed as Technology→Trust, Trust→Risk and Risk→e-Government security. This decomposition shows that technology directly affects user trust, user trust directly affects risk felt by users and risk felt by users directly affects e-Government security. In Section 2.7, it has already been shown that Technology→Trust Trust→Risk and Risk→e-Government security relationships are significant (β=0.914, -0.201 and -0.088 respectively). This implies that 91.4% of variation in user trust is predicted by technology, 20.1% of variation in risk is predicted by user trust although in the negative direction and 8.8% variation in e-Government is predicted by risk. Thus, when one takes the complete relationship Technology→Trust→Risk→e-Government security then it can be seen that technology has an indirect effect on e-Government security through not only trust but also risk which is explained by Table 6.2 in conjunction with Figure 5.11. In terms of regression coefficients the indirect effect of technology on e-Government security through trust and risk is computed as [0.914 (Technology→Trust) x -0.201 (Trust→Risk) x -0.088 (Risk→e-Government security)] = 0.016. This can be interpreted in a way that a one standard deviation change in technology effects a 0.016 standard deviation change on e-Government security. It can be seen that a comparison of the indirect effect of technology through two paths namely 'Technology→Trust→e-Government security' (indirect effect of technology on e-Government security is 0.75 standard deviation) and 'Technology→Trust→Risk→e-Government security' (indirect effect of technology on e-Government security is 0.016 standard deviation) on e-Government security shows that the path 'Technology→Trust→e-Government security' has higher predicting power than the path 'Technology→Trust→Risk→e-Government security'.

This can be interpreted in a way that when a new technology is introduced in the e-Government services then, it is important trust is generated leading to better user-centric e-Government

services security. Users in Bahrain have felt that the new technology has generated greater trust in them and hence have felt greater e-Government services security and consequent reduction in the feeling of risk. This is an important finding that user centric factors when taken into consideration in providing e-Government services, user trust improves and risk felt by users reduces leading to better security felt by users while using e-Government services. This can further enhance the success of e-Government services. This result has contradictory support in the literature. For instance, literature says that technology, trust and risk could be antecedents of e-Government security which is what was found in this research (see Section 2.7). However literature is suggesting that there is a strong relationship between trust and risk on the one hand, and risk and e-Government security on the other (see Sections 2.7 and 2.8), which is not supported by this research. Thus as argued in Chapter 5 hypotheses H2, H3a, H3b, H4 were accepted.

6.5 Analysis of the Relationship (HCI, EP, Service Quality)-Technology–ET-ER-User Centric e-Government Services Security

Section 5.7.3, in Chapter 5 has clearly shown that the EP is not contributing to the 'Technology–ET-ER-user-centric e-Government services security' relationship. Explanations have been provided under the same section what could be the reason. In similar vein, it can be seen from the same section that HCI and web design quality enhance the relationship between technology and e-Government security through the relationship 'Technology→Trust→e-Government security'. The finding that can be derived is that moderating factors HCI and web design quality have the potential to enhance the user centric e-Government security. Hence, managers involved in the service provision of e-Government must ensure that HCI aspects and web design quality aspects must be addressed as they become important user centric factors. This aspect is not well discussed in the management section of the literature and hence could contribute as a finding although there is evidence in the literature to suggest that HCI needs to be considered from the management perspective when there is an interaction between humans and computers (see Section 2.10.1) and that web design quality is an important aspect in e-Government services adoption (see Section 2.10.3). Thus, as mentioned in Chapter 5, hypotheses H1a and H1c have been accepted and H1b was rejected. At this stage it is important to highlight here that while accepting H1a and H1c, it is important to mention whether in the presence of the moderators H2, H3a, H3b and H4 are accepted or not. Since SEM was conducted on the complete model in the presence of moderators (see Figure 5.13), it is necessary to state whether H2, H3a, H3b and H4 are accepted or not as the effect of moderators has already been shown to affect the relationship between 'Technology' and 'e-government security' and hence it is necessary to provide information on the acceptance or rejection of H2,

H3a, H3b and H4. Thus from the foregoing analysis and Table 6.3 it can be seen that H2, H3a, H3b and H4 are accepted in the presence of moderators.

6.6 Relationship between User Experience, Education and Nationality and E-Government Security

From Section 5.3.2 in Chapter 5 it can be seen that experience and education have exert influence on the relationship between users and user centric e-government security in the context of Bahrain through the correlation Eduction↔Trust, Experience↔Trust. Nationality was not found to be a factor influencing this relationship. Possible reasons have been explained under the same section. Literature has both supporting and contradicting arguments. However, considering the fact that e-government services invariably depend on contextual factors, an argument supported by literature, the findings of this research can considered to be in line with the arguments in the literature. From these findings, it is possible to conclude that hypotheses H6a and H6b were accepted while H6c was rejected.

6.7 Relationship between Perceived Ease of Use, Perceived Usefulness and E-Government Security

This relationship was studied in order to know whether users really have felt the benefit of the introduction of a new technology in Bahrain. From Section 5.7 in Chapter 5 it can be seen that e-government services security is affected by both perceived ease of use and usefulness. The findings of the data analyzed in Section 5.7.7 and 5.7.8 shows that when users perceive that the technology is easy to use and useful, then their trust in the technology increases, risk felt reduces and e-government security increase. While linking PEOU and PU to e-government services security is not found in the literature, current evidence available in the literature that shows that PEOU and PU can enhance user adoption of e-government (see Chapter 2) although this statement is not free of controversy. Thus, while in this research a clear finding has emerged that shows that better PEOU and PU of e-government technology can enhance user centric e-government security through trust and risk, such a finding provides a different way of understanding e-government services security not addressed in the literature. As far as the implications of the findings it can be seen that managers of e-government services need to ensure that any new technology introduced should be easy to use and useful thereby enhancing the trust of users and reducing user felt risk. Hence as explained in Chapter 5 hypotheses H5a and H5b were accepted. In addition, it is important to highlight that while H5a and H5b were accepted, what has happened to the relationships 'Trust→e-government security' and 'Trust→Risk→e-government security'. Sections 5.7.8 in Chapter 5 show that SEM conducted on the relationships in the presence of PEOU and PU are valid. Thus it is important to note here

that while H5a and H5b are valid, at the same time H3a, H3b and H4 are valid and accepted. From the above arguments, it can be concluded that RQ2 has been answered.

The foregoing discussions it is possible to provide a final inference on the verification of the different hypotheses formulated for this research. Table 6.3 provides the list of hypotheses accepted and rejected.

Hypothesis No.	Hypothesis	Exogenous Latent Constructs	Endogenous Latent Construct	Results of Hypotheses verification	Explanation
H1a	Human computer interaction positively influences the relationship between e-government technology and user centric e-government security	HCI	Technology	**Accepted**	Human computer interaction moderates technology positively.
H1b	User privacy positively influences the relationship between e-government technology and user centric e-government security	ER	Technology	**Rejected**	User privacy does not moderate technology.
H1c	Web design quality positively influences the relationship between e-government technology and user centric e-government security	Service Quality	Technology	**Accepted**	Web design quality moderates technology positively.
H2	E-government technology positively influences user trust in e-government services	Technology	ET	**Accepted**	Technology positively and significantly influences ET in the presence of moderators.
H3a	User trust on e-government negatively influences user centric e-government security	ET	ESec	**Accepted**	ET positively and significantly influences ESec in the presence of moderators, PEOU and PU.
H3b	User trust on e-government negatively influences the risk felt by users of e-government	ET	ER	**Accepted**	ET negatively and significantly influences ER in the presence of moderators, PEOU and PU.
H4	User felt risk negatively influences user centric e-government security	ER	ESec	**Accepted**	ER negatively and significantly influences ESec in the presence of moderators, PEOU and PU.
H5a	Perceived ease of use of e-government services	PEOU	ET	**Accepted**	PEOU positively and significantly

	positively influences user trust in e-government				influences ET.
H5b	Perceived usefulness of e-government services positively influences user trust in e-government	PU	ET	**Accepted**	PU positively and significantly influences ET.
H6a	Education level of users positively influences user trust in e-government	Education	ET	**Accepted**	Education is positively correlated to ET.
H6b	Experience of users in e-government positively influences user trust in e-government	Experience	ET	**Accepted**	Experience is positively correlated to ET.
H6c	Nationality of users influences user trust in e-government	Nationality	ET	**Rejected**	Experience is not correlated to ET.

Table 6.3, Final List of Hypotheses Accepted and Rejected

6.8 Summary

The foregoing discussions have brought out how the user centric factors are related to e-Government security. Technology, trust and risk act as antecedents of user centric e-Government security. The major finding is that user centric factors have a strong influence on e-Government security. Technology is a strong predictor of user centric e-Government security mediated by trust. HCI and web quality design moderate the relationship between technology and user centric e-Government security positively. Perceived ease of use and usefulness moderate the relationship between user trust and e-Government security. Contextual factors user education and experience influence the relationship between user trust and e-Government security. The foregoing discussions thus provide the basis to conclude the outcomes of this research in the next chapter.

Chapter 7: Conclusion

7.1 Introduction

Based on the data analysis in Chapter 5 and discussions on the findings of the analysis provided in Chapter 6, this chapter provides the conclusions derived. The chapter includes examination of whether the aim and objectives set for this research have been achieved, contributions to knowledge, theoretical implications and contribution to practice. The chapter is organized as follows:

7.2 Study Context

Prior to writing the conclusions, it is important to review the context in which the study was conducted. Here the context refers to users of e-Government services in the Kingdom of Bahrain. Bahrain is one of the leading nations in the world that has successfully implemented e-Government. Currently it enjoys a high rank amongst the nations in the world with regard to e-participation (14th rank as per UN, 2014). In addition a wide ranging set of services are included of as part of the e-Government services in Bahrain. Bahrain is one of those nations that has consistently introduced the latest in technology in computing including cloud computing technology early into the e-Government services. While other nations are still deliberating on introducing cloud computing, Bahrain is already appearing to reap the benefits although it is not clear how it has affected the users. Particularly, how user centric factors including e-Government services security have been affected due to a change in technology in the e-Government services is yet to be investigated in many contexts (see Sections 2.4, 2.5 and 2.6) including the context of Bahrain. Thus, Bahrain offered a fertile ground for investigating into the user centric aspects of e-Government services including e-Government security, in an environment where a new technology has been introduced. Such an investigation had the potential to reveal how user centric factors including e-Government security are affected by a change in technology (e.g. introduction of cloud computing). In fact, Bahrain provided an opportunity to investigate into a context of e-Government where the influence of a changing contextual factor like technology has been witnessed on user centric e-Government security, a phenomenon not yet clearly understood (see Section 2.3 and 2.7). Amidst growing calls from researchers to investigate user centric e-Government factors, particularly e-Government security, (e.g. Shah et al.; 2014; European Commission, 2013; Shareef et al., 2011; Colesca, 2009), the e-Government environment at Bahrain offered those conditions essential to investigate a phenomenon such as user centric e-Government services security. Keeping this brief about the research context, following sections examine how the aim and objectives this study have been achieved alongside the contributions made by this research.

7.3 The Aim

In order to assess whether the aim has been achieved the aim is reproduced here for convenience "The aim of the research is to examine how changing technology as a contextual factor is related to user centric e-Government security".

Change in technology is a reality. Technology is the backbone of e-Government. Hence, technological changes have serious implications to the users of e-Government services and the service providers. More importantly, the security aspects concerning users of e-Government attract attention when there is a change in technology as literature (see Section 2.7) shows that security, including user centric security, is a prime factor that needs to be addressed when there is a change in technology.

In Sections 2.5 and 2.6, it has been highlighted that technology is a contextual factor that changes constantly. A number of examples of technological changes that affect e-Government and users of e-Government have been provided. Security problems caused by changing technology to users of e-Government have been highlighted. Lack of solutions to handle security issues of users viewed from user and managerial perspective has been highlighted, which is a gap in the literature (see Section 2.11).

A theoretical framework has been drawn to tackle this gap (see Chapter 3). User centric factors pertaining to e-Government have been examined and identified. Theoretical support has been provided. Relationship between technology as a contextual factor and user centric e-Government security has been established through a conceptual model. Technological factors have been identified as antecedents of e-Government security, based on the concepts developed by Shah et al. (2014). Associated antecedents that are essential to understand the relationship which include user trust and risk felt by users have been brought into the examination. Moderating factors that have the potential to affect the relationship have been examined as without these factors the real influence of technology as an antecedent would be less clear. User perception in terms of perceived ease of use and usefulness has been examined to know whether the conceived relationship is valid in reality. In addition, a general examination of the user centric contextual factors that have bearing on the relationship has been conducted to establish that contextual factors affect the relationship in the context of Bahrain. Analysis of the collected data and findings (Chapters 4 and 5) that have been derived provided support for the examination which culminated into the discussions which in turn showed whether the examination can lead to results that can contribute to knowledge, theory and practice (this chapter). Thus, it can be concluded that the aim set for this research has been

achieved. Next, the discussions progress to see whether the objectives have been achieved. For convenience, the objectives have been reproduced below.

Objectives

- To study the various factors concerning users in the field of e-Government in an environment characterized by changing technology.
- To elicit specific user-centric factors that could be related to e-Government security with the support of theories or models.
- To conceive a model using the factors elicited above that could relate those factors based on theories, concepts and models found in the extant literature.
- To derive findings by testing the model and achieve the aim set.

Discussion on each one of the objectives follows.

To study the various factors concerning users in the field of e-Government in an environment characterized by changing technology.

A review of the literature (Chapter 2) showed that there are a number of factors that concern users in the field of e-Government in an environment characterized by changing technology. However the focus of majority of the studies in the literature is technology as e-Government is essentially based on technology and hence user centric factors of e-Government that have bearing on the managerial aspects have found limited attention (see Chapter 2). There was a need to know how user needs and wishes could be addressed when e-Government is affected due to changing technology. There was no clear identification of user centric factors in the literature that could be effectively tackled by managers of e-Government services when changes occur. Lack of such knowledge has invariably limited the success of e-Government in terms of user uptake of e-Government services and their trust and belief in e-Government. There was a need to study the literature to identify such factors that could be considered as user centric and could be exploited to ensure better user engagement with e-Government services. The literature review in Chapter 2 shows that the factors can be classified under different disciplines including behavioral, social, technological, contextual, managerial, organizational and cultural ones. Under each classification many different factors were identified in the extant literature for instance e-Government security (organizational factor), user felt risk (behavioral factor), user trust (behavioral factor), e-Government technology (contextual/environmental factor), web design quality (managerial factor), user privacy (behavioral factor), HCI (contextual factor), perceived ease of use of e-Government technology (behavior), perceived usefulness of e-Government technology (behavior), demography and culture (contextual factors). Thus, these factors formed the basic components to understand how user centric e-Government security is affected by changing technology. Such factors have been investigated in this research to gain knowledge on how they affect users of e-Government and

e-Government security viewed from user perspective. Thus, it can be concluded that this objective is achieved.

To elicit specific user-centric factors that could be related to e-Government security with the support of theories or models.

The main factor that has been identified in the literature as user centric is the contextual factor. Within this category, a number of factors have been identified by researchers as user centric which includes demographic factors, technological factors and cultural factors (see Section 2.5 and 2.6). However demographic factors have also been shown to be factors that affect e-Government users when technology changes. Further, when one considers the meaning of the term user centric, many other factors were found to be linked to e-Government services security which included user trust in e-Government technology, user felt risk in e-Government, factors that influence the technology including HCI, user privacy and web design technology and user perceptions such as perceived ease of use and usefulness (see Chapter 2). Linkage between the user centric factors and e-Government services security as well as their application is supported by many theories (see Chapter 3). For instance, the relationship between the user centric factor trust and e-Government security could be explained by technology acceptance and adoption behavior theories whereas the relationship between risk and e-Government security could be explained with the help of technology acceptance theories. Similar arguments could be provided with regard to the other relationships identified in this research (see Chapter 3). The main user centric dependent factor that has been investigated as being determined by the prime contextual factor technology is the e-Government services security. The technology factor has been considered as the antecedent of e-Government security. Other important factors that have been identified as user centric and antecedent of e-Government security are user trust and user felt risk. In addition, three factors have been identified as supporting the relationship between technology and e-Government security which are HCI, user privacy and web design quality. However, user privacy as a factor had to be dropped from the list due to lack of statistical significance. Besides technology as the main contextual factors user education, experience and nationality were also identified as factors that need to be considered to explain the influence of contextual factors on the relationship between antecedents of e-Government security and e-Government security. Finally, perceived ease of use and usefulness were elicited as factors to verify whether cloud computing technology really has any influence on the user perception of e-Government security. Thus, it can be concluded that this objective has been achieved.

To conceive a model using the factors elicited above that could relate those factors based on theories, concepts and models found in the extant literature.

As far as this objective is concerned, Chapter 3 provides the complete details on how the various user centric factors elicited in this research are related to each other and in particular user centric e-Government security, depicted by the conceptual model in Figure (3.1). The main conceptual model was analyzed in parts due to the involvement of a number of variables. The conceptual model has been broken down into three parts (see Figures 5.12, 5.18, and 5.1). The first part (Figure 5.12) provides the basis for analyzing the relationship between three antecedents of user centric e-Government security (technology, user trust and user felt risk) and user centric e-Government security as a dependent factor. The next figure (Figure 5.12) provides the relationship between contextual factors and trust as an antecedent of e-Government security, depicts how other contextual factors namely user education, experience and nationality (representing culture) are related to user centric e-Government security through the antecedents trust and risk (see Figure 5.1). Finally, the model was broken down to test the influence of user perception of the e-Government technology by relating perceived ease of use and usefulness of the technology to the antecedents of e-Government security with e-Government security (see Figure 5.22). Reasons for dealing with the main conceptual model have been provided in Chapter 5.

The conceptual model has been developed based on established theories and models details of which have been provided in detail in Chapter 3. Expanding the application of those theories and models detailed out in Chapter 3 to cover the antecedents of e-Government security, user centric factors affecting users and user centric e-Government security has provided knowledge on how those antecedents and factors operate and can be related. This aspect has been added to the body of theoretical knowledge by this research. Through this conceptualization, this research has derived knowledge on how user centric factors affect e-Government security viewed from the user perspective when a major contextual factor "technology" changes. Thus, it can be seen that this objective has been achieved.

To derive findings by testing the model and achieve the aim set.

The findings in the form testing the hypotheses that described the relationships between the various factors and answering research questions have been provided in Chapters 5 and 6 respectively. The results showed that except for two hypotheses (H1b and H6c) the rest of the hypotheses are accepted (see Table 6.3). The results derived in Chapter 5 and 6 show that a new technology (cloud computing) when introduced in e-Government services in Bahrain, has significantly influenced the direct relationship between user trust and e-Government security. However, the findings show that technology's influence on the relationship ET→ER→ESec is insignificant when compared to its influence on the direct relationship ET→ESec although the ET→ER→ESec is statistically significant. Similarly, the relationships ET→ESec and ET→ER→ESec were found to be valid in the presence of PEOU of PU although the relationship ET→ESec provided a stronger explanation

of how PEOU and PU exert their influence on this relationship when compared to ET→ER→ESec. Finally, the contextual factors user education and experience where found to be correlated positively to ET thus implying that these two contextual factors can influence the relationship between antecedents of e-Government security and e-Government security in association with ET. The other contextual factor nationality was not significantly correlated to ET and hence its association with ET was rejected. These explanations clearly point out that the objective has been achieved. Further to explaining how the aim and objectives have been achieved for this research, the next step was to discuss the contributions to knowledge, theory, practice and methodology.

7.4 Contribution to Knowledge

The literature review revealed the gap existing with regard to an understanding of how contextual factors influence the phenomenon of e-Government and associated aspects including user centric e-Government security. What is known is that every time there occurs a change in the contextual factors, particularly technology, such a change is seen to effect a change in the e-Government services, particularly e-Government security. However, what is not known is that how those changes in the contextual do factors affect e-Government or more particularly e-Government security. Literature shows that each change has the potential to bring out new situations not addressed in the literature and that need to be understood (see Section 2.6) as they could affect user confidence in the e-Government services.

In addition, literature is silent on user centric factors affecting e-Government security that are examined from the managerial angle and useful to managers of e-Government services although literature is replete with investigations on technological factors that are needed to make the technology more secure. For instance quoting many authors Shah et al. (2014) assert that antecedents of online security have been studied by researchers applying the concepts of computer science and engineering and the approach has been one of technical and engineering and not social science or management. Shah et al. (2014) further affirm that technical and engineering approaches provide objective perspectives while social science or management approaches offer subjective insights. Needless to say subjective and objective perspectives involve different factors that can be called antecedents of online security (Chellappa and Pavlou, 2002; Kim et al., 2010; Linck et al. 2006; Peikari, 2010b,c) and it is argued that knowledge gained through one perspective is not applicable to another perspective Shah et al. (2014). These strong statements can be easily witnessed in everyday life. For instance, when a person is paying electricity and water charges through the online portal of the Government of Bahrain, there is always a concern in the minds of users on what will happen if the technology fails when the payment process is on. There are a number of examples of double payment that has been effected due to the failure of some objective steps in the e-Government process. It is easy to trace back how the error happened due to

technology but it is not easy to track and rectify the feelings of the users. The feeling is a subjective aspect. Therefore, subjective factors gain importance. In addition, such subjective factors have been analyzed keeping in view the user centricity, an aspect that is not well addressed in the literature.

Shah et al. (2014) further lament that despite the importance of the issue of antecedents that need to be viewed from subjective perspective, studies that have investigated those antecedents are limited and the outcomes have provided only limited understanding of the determinants of perceived online security. In fact, there is gap in the literature with regard to complete understanding of the interrelations between different antecedents and determinants of security and investigations. While Shah et al. (2014) have addressed these issues partially by investigating the online security aspects using limited set of antecedents, they have also recommended further research to investigate other factors like user trust and user felt risk. This research has contributed to this body of knowledge of online security in the context of e-Government security in Bahrain, by focusing on the most important contextual factor 'technology' on which e-Government and e-Government security depends and about which much less is known as an antecedent of e-Government security examined through the lens of management. The outcome of this research has produced knowledge with regard to those antecedents and factors that affect online security that have not been so far investigated fully from the management perspective with a focus on the relationship between technology and e-Government security.

Foremost, the research has been conducted in an environment in Bahrain where one of the latest technologies cloud computing has been introduced in e-Government and literature shows that user security is a major concern of cloud computing technology. The investigation focused on how change in technology introduced in e-Government services affects user centric e-Government security and related factors. User centricity as a focus is in itself still a phenomenon not widely addressed in the literature. No similar research appears to have been conducted on e-Government security in the context of cloud computing, particularly keeping in focus user centric nature of the factors associated with the 'technology-e-Government security' relationship viewed from different aspects of management like user behavior, organizational aspects, technology adoption aspects, contextual aspects, environmental aspects and managerial aspects.

For instance this research has demonstrated that technology is an antecedent of e-Government security using theoretical, practical and statistical means (see Chapter 3 and 6) in the context of changing technology, in this case introduction of cloud computing, introduced in e-Government. Although literature argues that technology affects e-Government security (see Section 2.7 in Chapter 2), there is no corroborating evidence to prove it in the context of cloud computing and the outcomes produced in this research provide evidence to corroborate it. In addition, this research has

verified the recommendations of Shah et al. (2014) to examine the effect of more antecedents of online security on online security in the context e-Government security by introducing trust and user felt risk as antecedents alongside technology. The results of this research clearly point out that the relationship between technology and e-Government security when mediated by user trust provides a strong evidence of technology indirectly influencing user centric e-Government security (see Section 5.16 in Chapter 5). The results imply that when new technology is introduced, trust levels increase and hence user centric e-Government security increases. The relationship between technology and e-Government security mediated by trust is a new way of looking at user centric aspects pertaining to subjective analysis of e-Government security. Thus this research while confirming previous research outcomes that posit that new technology (in this case cloud computing) could affect e-Government security, it can also enhance user trust and hence user centric e-Government security if the technology is perceived to be accepted by the user, a finding that contributes to knowledge.

However, the same could not be said of the antecedent risk. There is a general belief in the literature (see Section 2.8 in Chapter 2) that when trust levels are high, risk felt by users are low and vice-versa. Similarly, when risk is low, e-Government services security is expected to be high (see Section 2.9 Chapter 2). The results of this research point out that although the relationship between trust and risk on the one hand and risk and e-Government security on the other is inverse in nature, the relationships are not appearing to be statistically strong. From the results of statistical analysis, (see Section 5.7 in Chapter 5) it can be seen that the relationship 'Technology→Trust→Risk→e-Government security' was weaker when compared to the relationship 'Technology→Trust→e-Government security'. While these results contradict other research findings with respect to the relationship between trust and risk (for instance Belanger and Carter, 2008), the weak relationship that is seen in the relationship 'Technology→Trust→Risk→e-Government security' could be due to the overwhelming trust users may have with regard to the e-Government security that would have offset their feeling of risk. It must be noted that although the path 'Technology→Trust→Risk→e-Government security' is weak, it is not possible to discount the presence of risk and hence managers of e-Government services must pay attention to any risk factor that could exist and eliminate such risk. For instance cloud computing includes such applications on the e-Government site as twitter, Facebook or Skype. Users of e-Government services might have been already familiar with these applications and hence they might have developed a high level of trust in e-Government services that hosts such applications through cloud computing. Hence, risk levels felt by users could be low. This is a major finding that could be very useful to service providers. This knowledge also proves that it is not necessary that when a new technology is introduced the feeling of risk or security concerns will be high in the users. Thus as an antecedent of e-Government security, alongside trust this research has shown that technology

positively but indirectly influences user centric e-Government security and the influence is strong when mediated by trust but is weak when mediated by trust and risk. The outcomes of this research are thus contributing to the body of knowledge that is relevant to e-Government security, management, behavioral aspects of users and organizations. Additionally the above discussions clearly point out that e-Government technology acts as an independent user centric variable, user centric e-Government security acts as the dependent variable and trust and risk act as user centric mediators. In effect, e-Government technology, user trust and user felt risk have been brought in in this research as antecedents based on the concepts and recommendations of Shah et al. (2014) and confirming their assumption that trust and risk could be used as antecedents of online security, which in this research is the e-Government security, viewed from management perspective. Thus from the findings of Chapter 5, it is possible to conclude that when technology is high, then the influence of technology on user trust is high and when user trust is high then user centric e-Government security is high but the influence of user trust on user felt risk is low. Similarly, when user felt risk is low, then user centric e-Government security is high.

In addition to testing the 'Technology, Trust, and Risk' as antecedents of 'e-Government security' technology as a factor could not be involved in isolation in the relationships 'Technology→Trust→Risk→e-Government security' and 'Technology→Trust→e-Government security' as literature strongly posits that e-Government technology is affected by a number of factors whose influence on technology and hence on the two relationships cannot be ignored while technology is involved. Thus, three important factors namely HCI, user privacy (EP) and web design quality (Service Quality) were examined as moderators of the two paths. Reasons for choosing the three moderators have been provided in Section 5.3.1. Amongst the three HCI and its influence as a user centric factor on the two paths has not been studied in the literature although there are calls in the literature positing that it is necessary to view the impact of HCI on e-Government from the managerial perspective as much of the research on HCI has been conducted under the lens of technology. Hardly any research has been conducted to know how HCI affects users and their behavior towards e-Government. Section 5.7 shows how users could be affected irretrievably if HCI is not tailored to the needs of the different types of users. Thus, the outcome of this research significantly contributes to knowledge by producing results about the effect of HCI on the relationships 'Technology→Trust→e-Government security' and 'Technology→Trust→Risk→e-Government security' as a moderator. Results clearly show that when moderators are present the strength of the paths go up in comparison to the situation when they are absent. Thus from the findings of Chapter 5 it can be concluded that when HCI is high, then the influence of HCI on technology is high, when technology is high, then the influence of technology on user trust is high and when user trust is high then user centric e-Government security

is high but user felt risk is low. Again, when the user felt risk is low, then user centric e-Government security is high.

Similar arguments could be posited with regard to the two other moderators namely user privacy and web design quality. While the research outcomes show that user privacy was not found statistically significant and had to be dropped from the model (possible reasons are provided in Section 5.7), web site design quality was found to be statistically significant in acting like a moderator of the two paths 'Technology→Trust→e-Government security' and 'Technology→Trust→Risk→e-Government security'. That website design quality is related to e-Government technology is an argument that is supported by literature (e.g. DeLone and McLean, 2003) and website design quality is related to online security is also supported by literature (Shah et al., 2014). Nevertheless, website design quality moderates the two paths is not discussed in the literature. The importance of this finding is that when the degree of website design quality is high, then the results prove that the influence of technology on trust in users is high, the influence of user trust on e-Government is high, the influence of user felt risk is low and the influence of user felt risk on user centric e-Government security is negative that is to say when risk is low, e-Government security is high. It is clear that users attach importance to web design quality as a user centric factor affecting e-Government security, a phenomenon that must be taken into consideration when new technology is introduced or technology is changed by managers of e-Government. A good web design quality has the potential to improve technological functioning and hence raise the trust level in users, reduce their feeling of risk and enhance user centric e-Government security.

Besides, both HCI and web design quality have been found to have positive interrelationship (see Section 5.7.1 and 5.7.3) which indicates that when HCI changes then web design quality changes and vice-versa. This interrelationship is rarely captured in the literature. That is to say that when web site design is being attended to, then it is important to address HCI concerns also and vice-versa. A typical example could be that when technical experts are designing the web site, then they have to invariably take care of quality aspects regarding such factors as navigability through the website, readability and the like. While doing so designers are well advised to focus on how a user would interact with those web design features using a computer leading to betterment of user interaction with the e-Government portal. For instance, the screenshot of the front page of the e-Government portal of the Government of Bahrain in Figure 7.1 shows that the contents are less crowded, social media network icons are very clear and links to various ministries are well positioned to attract the users and includes a chatting facility.

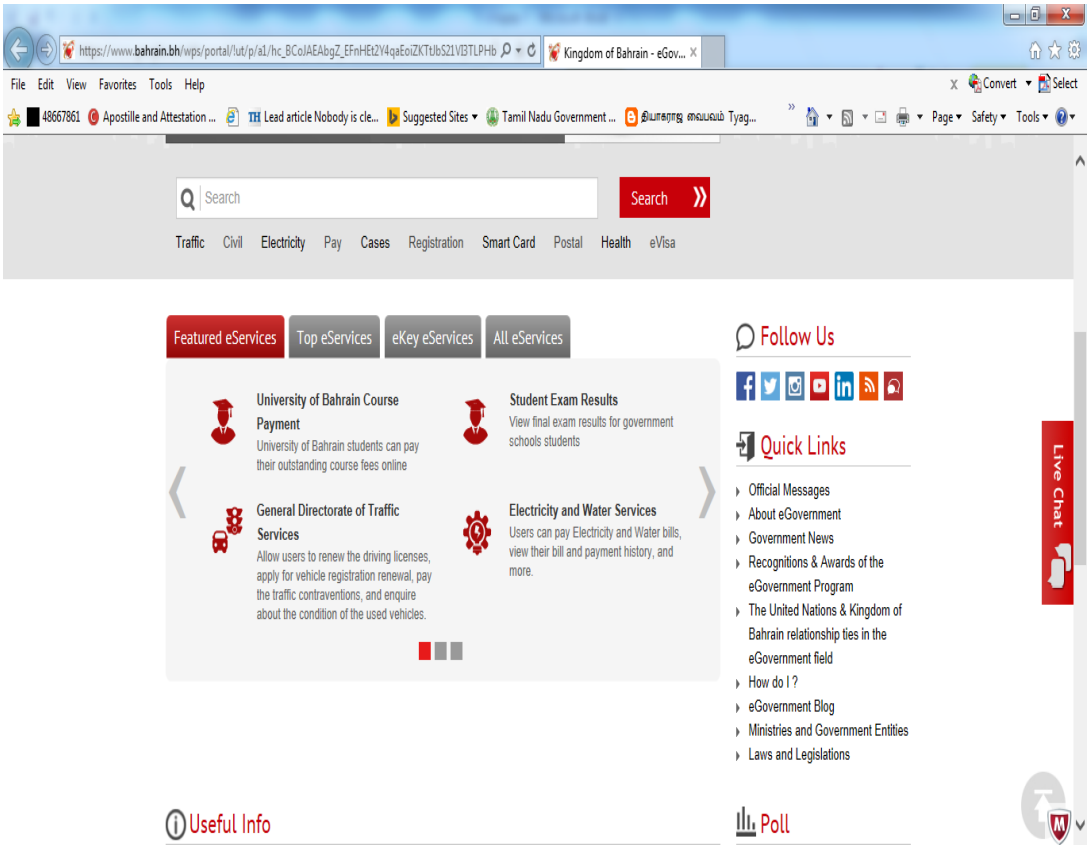

Figure 7.1: E-Government Portal of the Kingdom of Bahrain

However, one could see that chatting facility is displayed in a manner that reading the words “Live Chat” is not easy as the words are not parallel to the eyes. This anomaly could impair user interaction, as some users may not be able to spot the live chat facility due to the manner in which the icon is displayed. Similarly, multiple language facility is not visible in the portal, which restricts the contents to English only. The web design does not provide any link to display the contents in the local language Arabic in this webpage although Arabic version is available. There is a need to make the contents multilingual on the portal, an important need because 50% of the population in Bahrain belong to the expatriate community and the remaining are locals. Hence, lack of this feature could discourage users from using the portal and HCI between the users and the e-Government portal could be constrained. Thus although Bahrain has made great strides in providing one of the best e-Government services to the people by introducing state of the art technology, still it can be seen that certain factors that are user centric, particularly web design quality and HCI are somewhat weak. It is possible to infer that if web design quality is good then HCI must be good and vice-versa. Thus, it can be concluded that the results of this research have been corroborated by practical evidence.

Furthermore, the research reconfirmed the general arguments of researchers that demographic factors may or may not influence e-Government security (see Section 2.6 Chapter 2). From Section

5.3.2, it can be seen that user education and experience are associated with user trust, which implies that demographic factors could influence the relationship between antecedents of e-Government security and e-Government security. The main contribution here is that both user education and experience although not directly related to the linkage 'Trust→e-Government security' when associated with trust is expected to affect how trust influences user centric e-Government security. Trust being a mediator of the relationship 'Technology→Trust→e-Government security', it is implied that when the relationship 'Trust→e-Government security' is affected by the association between trust, user education and user experience, 'Technology→Trust→e-Government security'. This test was conducted in an environment where e-Government services in Bahrain are characterized by the introduction of cloud computing technology. Thus although not fully subjected to rigorous statistical analysis, the findings clearly show that the demographic factors, considered in this research as part of the contextual factors, have the potential to influence the relationship between 'Technology and user centric e-Government security'.

Finally, the researcher confirmed whether the introduction of cloud computing in the e-Government services of Bahrain has affected the users of the e-Government services of Bahrain with regard to their perception on how easy and useful the technology is, their trust in the service, their feeling of risk in using e-Government services, perception of e-Government security and the user centricity of the factors chosen for study in this research. The model SEM2 (see Figure 5.19) was used for the purpose. Results of the research (see Section 5.74 in Chapter 5) clearly show that perceived ease of use and usefulness of the technology have direct influence on the user trust, an antecedent of user centric e-Government security and the relationship between trust, risk and e-Government security. The relationships 'PEOU→Trust→e-Government security', 'PU→Trust→e-Government security', 'PEOU→Trust→Risk→e-Government security' and 'PU→Trust→Risk→e-Government security' have all been found to be statistically significant (see Section 5.7.4 in Chapter 5).

Here it is presumed that testing the above paths could imply testing the technology. It is argued that these relationships can be linked to technology without actually involving technology as a factor, and in reality that is the case as it has been established that the paths 'Trust→e-Government security' and 'Trust→Risk→e-Government security' are determined directly by technology (see above). Thus, any examination of those two paths by relating other user centric factors like PEOU and PU imply that the results could in effect be argued to impact technology as well. In such a case the results of this research in regards to the four paths can be interpreted in a way that users of e-Government in Bahrain appear to have largely felt that the introduction of cloud computing has made the e-Government technology easy to use and useful. This corroboration provides an independent verification of whether cloud computing technology, trust and risk as user centric

factors have really affected the users or not as introduction of cloud computing into e-Government services could not be tangibility felt by users although users can access certain cloud based applications without knowing that they are using those applications due to cloud computing technology (example Facebook icon in Figure 7.1). Hence, this corroborative exercise was needed to understand how change in technology introduced in e-Government services really affects users and user centric factors of e-Government. The contribution here is two-fold. One is that direct linkage of PEOU and PU to user trust is not commonly found in the literature. Knowledge about this linkage is not clear. Hardly anyone has attempted to investigate how PEOU and PU could affect user trust in e-Government or factors influenced by user trust like risk and user centric e-Government security with a notable exception of Ayyash et al. (2013) who empirically tested the relationship between PEOU, PU and user trust in Government. However, the research efforts stop at testing the adoption behavior of users of e-Government using this relationship. If one could ask the question whether PEOU and PU could influence the relationships 'PEOU→Trust→e-Government security', 'PU→Trust→e-Government security', 'PEOU→Trust→Risk→e-Government security' and 'PU→Trust→Risk→e-Government security' in the context of cloud computing, the answer is no. To the knowledge of the researcher this aspect is not investigated yet although literature argues that PEOU and PU of technology need to be understood when technological contexts change (see Section 2.8.1 in Chapter 2). Thus this research contributes to knowledge in terms of the finding that when PEOU is high, then user trust will be high, user felt risk will be low and user centric e-Government security will be high (see Section 5.7.8 in Chapter 5). That is to say, when PEOU changes positively, user trust changes positively, user felt risk changes negatively and user centric e-Government security changes in the positive direction. Similar arguments could be written with regard to PU.

In summary, it can be seen that this research has contributed to knowledge pertaining to user centric e-Government services security in multiple dimensions in the context of a new technology introduced into e-Government services in Bahrain. This knowledge could be very useful in determining how user centric e-Government security and user centric factors could be adjusted and tackled to maximize user centric e-Government security, a vital factor that has direct bearing on the success of e-Government. Further to highlighting the contributions of this research to knowledge, the next section proceeds to look into the theoretical implications of this research.

7.5 Contribution to Theory

An overall look at the synthesis of the theories that could be applied to this research (see Section 2.4 in Chapter 2) shows that as far as this research is concerned and the model that has been developed are concerned (see Chapter 3), it is seen that a number of theories need to be applied to explain how the various relationships have been conceptualized and operationalized. The theories

that could be applied to the various user centric factors and the relationship amongst them include MIS theory, adoption theories, socio-technical theory, HCI and e-GovQual (see Section 2.4 in Chapter 2).

A major contribution to theory is the expansion of the application of socio-technical theory to understand how the concepts of e-Government and e-Government security manifest in reality. The theory states that there needs to be a fit between technical and social sub-systems in an organization if organizations want to succeed. The theory further states that for systems to be successful technical, organizational, and social aspects of the system must be configured in parallel (Bostrom and Heinen, 1977). It can be seen (see Section 3.3 in Chapter 3) that using this theory this research has been able to explain how user behavior with respect to e-Government services security can be explained by relating it to technological changes that occur. Further going by the arguments in the literature, for instance the arguments of Khan et al. (2011) who say that every aspect of e-Government including customer perspective of e-Government services and e-Government security could be understood using socio-technology theory, it is possible to support the relationship between e-Government technological changes and e-Government security leading to a conceptual model. However, it is important to note from the explanations given in Chapter 3 that linkage between e-Government technology change and e-Government security need to include other factors like user trust and user felt risk to gain a deeper understanding of how users behave or how these factors need to be centered around the user behavior. Inclusion of such factors requires the support of auxiliary theories or models (see Section 2.7.3 in Chapter 2. This research contributes to theory by extending the application of socio-technical theory to e-Government services security by combining other models or theories thus developing a new model, an aspect not covered in the extant literature. The findings from statistical analysis given in Chapter 5 provide evidence of the validity of this argument.

Another notable feature of this research is the application of a broad interdisciplinary theory like HCI theory to this research to understand how HCI affects users of e-Government services. Iachello and Hong (2007) argue that in the design field HCI mostly deals with information theory and information exchange. Information exchange is described using mathematics and has no reference to human user. Such a situation has forced the HCI community to focus on economic and behavioral models (Iachello and Hong, 2007) although none of the efforts have addressed e-Government services. Thus, this research extends the application of HCI theory concerning the MIS design aspects affecting users by linking it to behavioral aspects like technology acceptance or adoption, which includes change in technology governing e-Government and its linkage to e-Government security.

Furthermore, this research has applied the concepts of e-govqual which provides a basis to understand how users of e-Government service perceive and evaluate online services. This theory has not been well established as it has been propounded only recently by Papadomichelaki and Mentzas (2011). This research while combining the ideas of e-govqual with socio-technology theory through the integration of web design quality into the linkage between user centric e-Government technology and user centric e-Government security is able to establish the empirical reliability and validity of the e-govqual theory, a theoretical contribution that is one of the first with regard to e-govqual.

As far as contextual factors user education, user experience and user nationality are concerned, this theory has extended existing concepts that provide the basis for relating those factors to the user behavior towards e-Government security when a new technology was introduced in the e-Government services in Bahrain. UTAUT model has been used to derive concepts that could be combined with the socio-technical theory to explain how demographic factors could be related to the linkage between technology and e-Government security. Thus this research confirms the application of UTAUT to the concept of user behavior towards e-Government security as has been done by other researchers (see Section 2.4 in Chapter 2) while combining UTAUT with socio-technology theory to explain user behavior in regards to e-Government security which is not commonly found in the literature.

Additionally this research has used the concepts of UTAUT while linking TAM variables PEOU and PU to 'user trust' – 'e-Government security' linkage to know the perception of users of the e-Government services in Bahrain when a new technology has been introduced. While there are examples of using UTAUT to understand e-Government user behavior in the literature (see Section 2.8.1) the linkage of PEOU and PU to trust in the field of e-Government to address the linkage between user trust and e-Government security by expanding the efforts of Ayyash et al. (2013) contributes to theory. No such effort can be found in the extant literature that has attempted to explain the actual behavior of the users of e-Government services in cloud computing environment with regard to their perception towards the technology-e-Government security linkage mediated by trust and risk. This is a contribution that opens up a way to expand the application of the concepts of PEOU and PU to new user centric behaviors in the field of e-Government.

Finally, this research has been able to expand the concepts posited by Shah et al. (2014) to explain the e-Government security aspects concerning users by involving two new antecedents namely user trust and user felt risk into their conceptualizations as recommended by them. Although their model has not been used in one-to-one correspondence, their conceptualization has been used as the underpinning theory to explain the linkage between technology as an antecedent of e-Government

security and e-Government security mediated by user trust and user felt risk. Thus, this research has come out with a new model that explains the user behavioral aspects with regard to the change in technology in e-Government services, user trust, user felt risk and user centric e-Government security. The underlying theories that have been used are socio-technology and UTAUT. As explained earlier, this research combines socio-technology theory and UTAUT to explain the expansion of the concepts posited by Shah et al. (2014) to e-Government domain, a contribution that enables a better understanding of how users feel about the e-Government security when technology changes, which could help managers or e-Government services and users alike. After understanding the contribution to theory, the discussions proceed to look at the contribution to methodology.

7.6 Contribution to Methodology

This research contributes to methodology primarily with regard to the actual testing of user behavior that has empirical support from the conceptual model developed for answering the research questions. That is the researcher developed the main model (see Figure 3.1) having the linkages 'Technology →Trust →e-Government security', 'Technology→Trust→Risk→e-Government', 'HCI→Technology→Trust→e-Government security', 'HCI→Technology→Trust→Risk→e-Government security', 'Service quality→Trust→e-Government security' and 'Service quality→Trust→Risk→e-Government security'. This model was a theoretical model. Its operation with regard to the linkages 'Technology→Trust→e-Government security' and 'Technology→Trust→Risk→e-Government' was confirmed by the operationalization of the linkages relationships 'PEOU→Trust→e-Government security', 'PU→Trust→e-Government security', 'PEOU→Trust→Risk→e-Government security' and 'PU→Trust→Risk→e-Government security'. This operationalization provides a real picture check on the ground. This kind of verification is not usually adopted in empirical research. Hence, this research contributes to methodology by which a conceptual model is not only tested empirically but also verified for its operation alongside to determine whether research questions can really address the problems stated in Chapter 1. Further to explaining the contribution to methodology, this discussion provides an idea about its contribution to practice.

7.7 Contribution to Practice

Foremost the contributions of this research are expected to be useful to users of e-Government services who can now know that there are user centric factors that affect e-Government security, knowledge vital to their engagement with e-Government services. Henceforth users could be alert with regard to e-Government security when a change in technology is introduced in the e-Government services by checking HCI factors, web design quality factors, type of technology, ease of use of the technology, usefulness of the technology, their trust on the technology and their

feeling of risk involved in the introduction of new technology in the context of Bahrain. Until now, an established model that could provide users with an idea of what factors could inform them of the extent of security built into an e-Government service was not available. This model could be used by users of e-Government service to analyze the extent of e-Government services security built into the service.

While users gain a model to understand the extent of security built into e-Government services in Bahrain when there is a change in technology, it is possible that service providers understand those factors clearly keeping in focus the e-Government service users. User centric factors until now have not been of great concern for mangers of e-Government services as the focus of those dealing with e-Government service security has been technology and engineering in general. Such a situation has not helped to enable users to gain confidence in the e-Government security. As argued by Shah et al. (2014) antecedents of online security, in this case e-Government security, can provide a strong support to managers to understand how to address user centric factors concerning e-Government security. The outcomes of this research can now be implemented by service providers to enhance user support and ensure the success of e-Government services. Especially when a new technology is introduced, it is imperative that they thoroughly analyze the impact on the users taking into account HCI, web design quality, technology, user trust, risk, security, ease of use and usefulness as factors.

Again, the outcome of this research provides support to policy makers to device policies that are user centric and to ensure that service providers and designers of e-Government web portals make it a point to orient their efforts to achieve a high level of e-Government security especially when technology changes. Although this research was conducted in the context of Bahrain, it is important to realize technologically, the outcomes achieved in Bahrain can be replicated in other countries, a notion that gains credibility due to the high ranking Bahrain enjoys in UN surveys related to e-Government.

At this stage, in summary it can be seen that the conclusions derived until now that the aim and objectives set have been achieved and contributions to knowledge, theory, methodology and practice have been highlighted. Further to this, the following sections deal with the limitations of this research and areas that could be considered as having potential for future research.

7.8 Limitations of Research

As is usually the case with most of the research efforts, this research also suffers from certain limitations. For instance, this research was contextualized and conducted in Bahrain. Considering the special nature of this country such as small population, equal proportion of locals and

expatriates and the possibility to control e-Government in a better manner due to the small size of the country, the research outcomes may need to be tested in other territories. Particularly research in an environment where e-Government is characterized by cloud computing and the size of population and area of the territory is large may reveal different results.

Further, since cloud computing is a new technology, and research outcomes concerning e-Government where cloud computing is introduced is sparse, corroborating the research outcomes with similar research produced elsewhere was a problem. In addition, only three factors have been used in the research as moderators of the paths 'Technology→Trust→e-Government security', 'Technology→Trust→Risk→e-Government'. More moderators may need to be brought in and investigated to know whether same results are obtained or different results could emerge.

Apart from the above, in this research user trust and user felt risk have been used as mediators. If they are considered as independent variables, then the results could be different as there is evidence to suggest in the literature that trust and risk could be considered as independent variables. Thus, the results of the current research may not be generalizable due to the above limitations. Taking into account the above limitations, the next section provides recommendation for future research.

7.9 Recommendations for Future Research

The limitations discussed above point towards the need to conduct further research in a different territory that is larger than Bahrain and where cloud computing or similar technological advances have been introduced in e-Government services. Secondly, future research must consider including more user centric moderators of the paths 'Technology→Trust→e-Government security', 'Technology→Trust→Risk→e-Government'. Further future research could consider using trust and risk as independent variables in association with technology, affecting user centric e-Government service security. Such research effort could either enable the consolidation of the outcomes of the current research or produce new knowledge.

References

Aaker, D. A., Kumar, V. and Day, G. S. (2008). Marketing research. John Wiley & Sons.

Abdelsalam, H. M., Reddick, C. G., ElKadi, H. A. and Gama, S. (2012) 'Factors affecting perceived effectiveness of local e-Government in Egypt', *International Journal of Information Communication Technologies and Human Development* (IJICTHD), 4(1), pp.24-38.

Abu-Shanab, E. and Al-Azzam, A. (2012) 'Trust Dimensions and the adoption of E-Government in Jordan', *International Journal of Information Communication Technologies and Human Development (IJICTHD)*, 4(1), pp.39-51.

Abunadi, I. (2015) 'Characteristics of Electronic Integrated System and Trust in the Provider of Service', *International Journal of Computer Applications*, 132, 4(1).

Accenture (2005) 'The Government Executive Series Leadership in Citizen Service: New Expectations', New Experiences, Retrieved July 07, 2009 from http://www.accenture.com/Countries/Canada/Services/By_Subject/Customer_Relationship_Management/R_and_I/LeadershipNewExperiences.htm

Ahmad, Z. S., Harun, N and Shuhaimi, H. (2015) 'Using Technology, Organization, Environment Framework to Investigate the Determinants of the Adoption of Electronic Publishing Amongst Malaysian Publishers', *Australian Journal of Basic and Applied Sciences*, 9(3), pp 37-44.

Ahmed, M. and Hossain, M.A. (2014) 'Cloud computing and security issues in the cloud', *International Journal of Network Security & Its Applications* (IJNSA), 6(1), pp.25-36.

Ajzen, I. (1991) 'The theory of planned behavior', *Organizational Behavior and Human Decision Processes*, 50(2), pp. 179−221.

Al-Adawi, Z., Yousafzai, S. and Pallister, J. (2005) 'Conceptual Model of Citizen Adoption Of E-Government', *The 2005 International Research Conference on Innovations in Information Technology (IIT'05)*, [online]. Available at: http://www.it-innovations.ae/iit005/proceedings/articles/G_6_IIT05-Al-Adawi.pdf (Accessed: June 26, 2009).

Al-Jamal, M. and Abu-Shanab, E. (2015) 'PRIVACY POLICY OF E-GOVERNMENT WEBSITES: AN ITEMIZED CHECKLIST PROPOSED AND TESTED', *Management Research and Practice*, 7(3), p.80.

Al-Shafi, S. (2009) Factors Affecting E-Government Implementation and Adoption in the State of Qatar. Ph.D. Thesis,

Al-Shafi, S., and Weerakkody, V. (2008) 'The Use Of Wireless Internet Parks To Facilitate Adoption And Diffusion Of E-Government Services: An Empirical Study In Qatar', *Proceedings of the 14th Americas Conference on Information Systems (AMCIS 2008)*, Toronto, Ontario.

Al-Shafi, S. and Weerakkody, V. (2010) 'Factors affecting e-Government adoption in the state of Qatar'.

Al-Shehry, A. M. (2009) 'Transformation towards e-government in the Kingdom of Saudi Arabia: technological and organisational perspectives'

Alam, S. S. and Yasin, N. M. (2010a) 'The antecedents of online brand trust: Malaysian evidence', *Journal of Business Economics and Management*, 11(2), 210–226.

Alam, S. S. and Yasin, N. M. (2010b) 'An investigation into the antecedents of customer satisfaction of online shopping, *Journal of Marketing Development and Competitiveness*, 5(1), 71–78.

Alateyah, S. A., Crowder, R. M. and Wills, G. B. (2013) 'Identified Factors Affecting the Intention of Saudi Arabian Citizens to Adopt e-Government Services', *International Journal of Innovation, Management and Technology*, 1(1), pp. 280-286.

AlAwadhi, S. and Morris, A. (2009) 'Factors influencing the adoption of e-Government services', *Journal of Software*, 4(6), pp.584-590.

Alfawaz, S., May, L. and Mohanak, K. (2008) 'E-Government security in developing countries: a managerial conceptual framework, *International Research Society for Public Management Conference'*.

Alharbi, N., Papadaki, M. and Dowland, P. (2014) 'Security Factors Influencing End Users' Adoption of E-Government'.

Alleweldt, F., Kara, S, Fielder, A., Brown, I., Weber, V. and Mcspedden-Brown, N. (2012) Cloud Computing, Policy Department Economic and Scientific Policy European Parliament.

AlKalbani, A., Deng, H. and Kam, B. (2015) 'Organisational security culture and information security compliance for e-Government development: the moderating effect of social pressure', In PACIS 2015 (pp. 1-11). Association for Information Systems (AIS).

Alomari, M. K. (2014) 'Discovering citizens reaction toward e-Government: factors in e-Government adoption', *JISTEM-Journal of Information Systems and Technology Management*, 11(1), pp. 5-20.

Alraja, M. N., Hammami, S. and Alhousary, T. (2015) 'Factors Affecting E-Government Services Adoption: Field Study', *Journal of Theoretical and Applied Information Technology*, 78(1), p.65.

Alrashedi, R., Persaud, A. and Kindra, G. (2015) 'Drivers of eParticipation: Case of Saudi Arabia'.

Alsaghier, H., Ford, M., Nguyen, A. and Hexel, R. (2009) 'Conceptualising Citizen's Trust in e-Government: Application of Q Methodology', *Electronic Journal of e-Government,* 7(4), pp. 295-310.

Alshehri, M. A. and Drew, S. (2010) 'E-Government fundamentals', *in Proc. the IADIS International Conference on ICT, Society and Human Beings*.

Alshehri, M., Drew, S. and Alfarraj, O. (2012) 'A Comprehensive Analysis of E-Government services adoption in Saudi Arabia: Obstacles and Challenges', *Higher education,* 6, 8-2.

AlShihi, H. (2005) 'E-Government development and adoption dilemma: Oman case study', In 6th International We-B (Working for e-Business) Conference.

Al Khattab, A., Al-Shalabi, H., Al-Rawad, M., Al-Khattab, K. and Hamad, F. (2015) 'The Effect of Trust and Risk Perception on Citizen's Intention to Adopt and Use E-Government Services in Jordan', *Journal of Service Science and Management*, 8(03), p.279.

Anderson, J. C. and Gerbing, D. W. (1988) 'Structural equation modeling in practice: a review and recommended two-step approach', *Psychological Bulletin,* 103(3), pp. 411-23.

Andersen, K. V. and Henriksen, H. Z. (2006) 'E-Government maturity models: Extension of the Layne and Lee model', *Government Information Quarterly*, 23(2), pp. 236-248.

Abramson, R., Rahman, S. and Buckley, P. (2005) 'Tricks and traps in structural equation modelling: A GEM Australia example using AMOS graphics', *In ABBSA conference*, Cairns, Australia.

Arbuckle, J. L. (2006) *AMOS (Version 7.0). Computer Program*. Chicago: SPSS.

Arbuckle, J. L. and Wothke, W. (1999) *Amos 4.0 User's Guide. Chicago*, IL: SPSS Inc.

Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. and Zaharia, M. (2010) 'A view of cloud computing', *Communications of the ACM*, 53(4), pp.50-58.

As_Saber, S., Srivastava, A. and Hossain, K. (2006) 'Information technology law and e-Government: A developing country perspective', J*OAAG*, 1(1).

A.T.

Kearney A. T. (2015) Lifting the barriers to ecommerce in ASEAN, Korea

Axelsson and Melin (2008) 'Citizen Participation and Involvement in eGovernment Projects: An Emergent Framework', In Electronic Government, pp. 207-218, Springer Berlin Heidelberg.

Ayyash, M. M., Ahmad, K. and Singh, D.S.V. (2013) 'Investigating the effect of information systems factors on trust in e-Government initiative adoption in Palestinian public sector', *Research Journal of Applied Sciences, Engineering and Technology*, 5(15), pp.3865-3875.

Babbie, E. (2004) The Practice of Social Research, 10th edition. *The US: Wadsworth, Thomson Learning, Inc*.

Bagozzi, R. P., and Yi, Y. (1988) 'On the evaluation of structural equation models', *Journal of the academy of marketing science*, 16(1), pp. 74-94.

Balasubramanian, S., Konana, P., and Menon, N. M. (2003) 'Customer satisfaction in virtual environments: A study of online investing', *Management Science*, 7, 871−889.

Bakker, A. and Gravemeijer, K. P. E. (2006) 'A historical phenomenology of mean and median', *Educational Studies in Mathematics*, 63(1).

Balsley, B. B. (1970) 'A longitudinal variation of electron drift velocity in the equatorial electrojet', *J Geophys Res*, 75, 4291.

Bélanger, F. and Carter, L. (2008) 'Trust and risk in E-Government adoption', *Journal of Strategic Information Systems*, 17 (1), pp. 165–176.

Bélanger, F. and Hiller, J. S. (2006) 'A framework for e-Government: privacy implications', *Business process management journal*, 12(1), pp.48-60.

Bernard, H. R. (1995) *Research Methods in Anthropology*. Second Edition. London: Sage Publications.

Bernhard, I. (2013). E-Government and e-governance: Swedish case studies with focus on the local level.

Berthon, P., Pitt, L., Cyr, D., and Campbell, C. (2008) 'E-readiness and trust: Macro andmicro dualities for e-commerce in a global environment', *International Marketing Review*, 25(6), 700-714.

Bevan, N. (2006) *International Standards for HCI, Based on chapter in Encyclopedia of Human Computer Interaction*. Idea Group Publishing, Chapter Books.

Blakemore, M and Lloyd, P. (2007) 'Think Paper 10. Trust and Transparency: pre-requisites for effective e-Government, Prepared for the eGovernment unit', *DG Information Society and Media, European Commission*, 2(3).

Bollen, K. A. (1989) *Structural Equations with Latent Variable.* New York: John Wiley and Sons.

Bollen, K. A. and Long, J. S. (1993) 'Testing structural equation models', 154, SAGE Publications, Incorporated.

Bonham, G., Seifert, J. and Thorson, S. (2001) 'The Transformational Potential of E-Government: The Role of Political Leadership', *Proceedings of the 4th Pan European International Relations Conference*, Canterbury, 6-10 September 2001, 1-9.

Bostrom, R. P. and Heinen, J. S. (1977) 'MIS problems and failures: A socio-technical perspective part II: The application of socio-technical theory', MIS Quarterly, 1(4), 11–28.

Botterman, M., Schindler, H. R., and Van Dijk, L. V. (2010) 'Trend Analysis (D3) Smart N 2009/0069'.

Bower, K. M. (2003, May) 'Some misconceptions about the normal distribution', In *American Society for Quality, Six Sigma Forum*.

Brown, I. (2015) Regulation and the Internet of Things, GSR discussion paper.

Burda, D. and Teuteberg, F. (2014) 'Understanding The Benefit Structure Of Cloud Storage As A Means Of Personal Archiving-A Choice-Based Conjoint Analysis'.

Burgess, A., 1986. *Ernest Hemingway*. IB Tauris.

Burke, S. (2001) 'Missing values, outliers, robust statistics & non-parametric methods', *LC-GC Europe Online Supplement, Statistics & Data Analysis*, 2, pp. 19-24.

Burns, A. C. and Bush, R. F. (2000) *Marketing research: Online research applications (4th ed).* Prentice Hall, New Jersey.

Burn, J. and Robins, G. (2003) 'Moving towards e-Government: a case study of organizational change processes', *Logistics (Enterprise) Information Management*, 16(1), pp. 25-35.

Burton, L. J. and Mazerolle, S. M. (2011) 'Survey Instrument Validity Part I: Principles of Survey Instrument Development and Validation in Athletic Training Education Research', *Athletic Training Education Journal*, 6(1), pp. 27-35.

Buyya, R., Pandey, S. and Vecchiola, C. (2009) 'Cloudbus toolkit for market-oriented cloud computing', *In Cloud Computing* (pp. 24-44). Springer Berlin Heidelberg.

Bwalya, K.J. and Healy, M. (2010) Harnessing e-Government adoption in the SADC region: a conceptual underpinning. '*Electronic journal of e-Government'*, 8(1), pp.23-32.

Byrne, B. M. (2001) *Structural Equation Modeling with AMOS: Basic Concepts, Applications, and Programming.* Mahway. New Jersey: Lawrence Erlbaum Associates, Publishers.

Byrne, B. M. (2010) *Structural equation modeling with AMOS: Basic concepts, applications, and programming*. Psychology Press.

Campbell, D. (2004) 'A longitudinal and cross-sectional analysis of environmental disclosure in UK companies: A research Note', *The British Accounting Review*, 36(1), pp. 107-117.

Carroll, J. M. and Campbell, R. L. (1989) 'Artifacts as Psychological Theories: the Case of Human-Computer Interaction', *Behaviour and Information Technology*, 8, 247-256.

Carter, L. and Bélanger, F. (2005) 'The utilization of e-Government services: citizen trust, innovation and acceptance factors', *Information Systems Journal*, 15(1), pp. 5–25.

Carter, L., and Weerakkody, V. (2008) 'E-Government Adoption: A Cultural Comparison', *Information Systems Frontiers*, Springer, (10:4), pp. 473-482.

Cassell, C. and Symon, G. (1997) *Qualitative Methods in Organizational Research– A Practical Guide*. SAGE Publications Ltd, London.

Castells, M. and Cardoso, G. eds. (200) The network society: From knowledge to policy (pp. 3-23). Center for Transatlantic Relations, Paul H. Nitze School of Advanced International Studies, Johns Hopkins University.

Chang, H. H. and Chen, S. W. (2009) 'Consumer perception of interface quality, security, and loyalty in electronic commerce', *Information & Management*, 46, pp. 411– 417.

Chang, H. H. and Chen, S. W. (2008) 'The Impact Of Online Store Environment Cues on Purchase Intention Trust and Perceived Risk as A Mediator', Online Information Review, Vol 32(6), 818–841.

Chen, X. Z., Zheng, Q. H., Guan, X. H., Lin, C. G. and Sun, J. (2005) 'Multiple behavior information fusion based quantitative threat evaluation', Computers & Security, 24(3), pp. 218-231.

Chen, Y. C. and Dimitrova, D. V. (2006)', Electronic government and online engagement', *International Journal of Electronic Government Research*, 2(1), pp.54-76.

Chuairuang, S. (2010) 'Methodological Issues in a Study of Relationships between Family Firms and Capital Providers: Empirical Evidence from Small Family Firm in Thailand'.

Choudrie, J. and Papazafeiropoulou, A. (2006) 'Lessons learnt from the broadband diffusion in South Korea and the UK: implications for future government intervention in technology diffusion', *Electronic Government, an International Journal*, 3(4), pp.373-385.

Choudrie, J. and Lee, H. (2004) 'Broadband development in South Korea: institutional and cultural factor', *European Journal of Information Systems*, (13:2), pp. 103-114.

Churchill, G.A. and Iacobucci, D. (2004) *Marketing research: Methodological foundations*. 9th ed, Thomson South-Western, Ohio.

Cohen, J. (1988) *Statistical power analysis for the behavioral sciences*. 2nd ed edition. L. Erlbaum Associates, Hillsdale, N.J..

Colesca, S. E. and Dobrica, L. (2008) 'Adoption and use of e-Government services: the case of Romania', *Journal of Applied Research and Technology*, 6(3), pp. 204-217.

Colesca, S. E. (2009) 'Increasing E-Trust: A Solution To Minimize Risk in E-Government Adoption', *Journal of applied quantitative Methods*, 4(1), pp. 31-44.

Conner, M. and Armitage, C. J. (1998) 'Extending the theory of planned behavior: A review and avenues for further research', *Journal of applied social psychology*, 28, pp.1429-1464.

Cooper, D. R. and Schindler, P. S. (2003) *Business Research Methods*. 8 ed.. The US: McGraw-Hill Companies, Inc.

Corritore, C. L., Kracher, B. and Wiedenbeck, S. (2003) 'On-line trust: concepts, evolving themes, a model', *International Journal of Human-Computer Studies*, 58(6), 737-758.

Cousineau, D. and Chartier, S. (2010) 'Outliers detection and treatment: a review', *International Journal of Psychological Research*, 3(1), pp. 58-67.

Creswell, J. W. (2003) Research design. Qualitative, quantitative and mixed methods approaches. Thousand Oaks, CA: Sage.

Criado, J.I., Sandoval-Almazan, R. and Gil-Garcia, J. R. (2013) 'Government innovation through social media', *Government Information Quarterly*, 30(4), pp.319-326.

Cruz F. A, Tan, J. C. and Yonahn Y. Y (2015) Assisting the Reintegration of Philippine Return Migrants through Mobile Technology (2015) *Policy*: A Submission to the Geneva Challenge.

Curran, K., Carlin, S. and Adams, M. (2011) 'Security issues in cloud computing'. *Elixir*, vol. 38, pp. 4069 –72.

Dahlbom, B. and Mathiassen, L. (1995) 'Computer in context: The philosophy and practice of systems design', *Cambridge, Mass: Blackwell*.

Dally, J. (2006) 'A Consumer Link Survey September Quarter 2006', Unisys Security Index: New Zealand. Available at:
http://www.unisys.com.au/services/security/security__conference/index.htm (Access on: 01 October 2009).

Danila, R. and Abdullah, A. (2014) 'User's Satisfaction on E-Government Services: An Integrated Model', *Procedia-Social and Behavioral Sciences*, 164, pp.575-582.

Davis, F. (1987) 'User acceptance of information system: the Technology acceptance model (TAM)', *Working Paper 529*, University of Michigan, School of Business Administration.

Davis, F. D. (1989) 'Understanding Information Technology Usage: A Test Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology', *MIS Quarterly*, 13(3), pp. 319-340.

Dwivedi, Y and Irani, Z. (2009) 'Understanding the Adopters and Non-adopters of Broadband', *Communications of the ACM*, (52:1), pp. 122-125.

Dwivedi, Y.K. and Lal, B. (2007) 'Socio-economic determinants of broadband adoption', *Industrial Management & Data Systems*, 107(5), pp.654-671.

Dawes S (2009) 'Governance in the digital age: A research and action framework for an uncertain future', *Government Information Quarterly* 26 (2009) 257–264.

De, R. (2008) 'December. Electronic governance theory', *In Proceedings of the 2nd international conference on Theory and practice of electronic governance* (pp. 11-15). ACM.

Dehkordi, L. F., Sarlak, M. Al., Pourezzat, A. A. and Ghorbani A. (2012) 'A Comprehensive Conceptual Framework for the E-Government Realization', *Australian Journal of Basic and Applied Sciences*, 6(8): 50-64.

Dong, C. (2015) Social Media Use in State Government: Understanding the Factors Affecting Social Media Strategies in the Minnesota State Departments.

Duffany, J.L. (2012) 'Cloud Computing Security and Privacy', *In 10th Latin American and Caribbean Conference for Engineering and Technology* (pp. 1-9).

Dyson, S., and Brown, B. (2005) Social theory and applied health research. McGraw-Hill International.

E-Government (2015): https://www.bahrain.bh/wps/portal/!ut/p/a1/04_Sj9CPykssy0xPLMnMz0vMAfGjzOI9_A3MDI0sjLz8g90sDBwtwnzdnSzdjA3cjYEKIoEKDHAARwNC-sP1o8BKDIx8nQ09TYy8DHx9gfosnIJ8QtycDQwsjAgoAJoBVYDbDQW5EQaZno6KAIdXbvQ!/dl5/d5/L0lDUmlTUSEhL3dHa0FKRnNBLzRKVXBDQSEhL2Vu/

Easterby-Smith, M., Thorpe, R. and Lowe, A. (2002) *Management Research: An Introduction*. 2 ed., The UK: SAGE Publications Ltd.

Ebrahim, Z. and Irani, Z. (2005) 'E-Government Adoption: Architecture and Barriers', *Business Process Management Journal*, vol. 11, no. 5, pp. 589.

Elsheikh, Y. and Azzeh, M. (2014) 'What Facilitates the Delivery of Citizen-Centric E-Government Services in Developing Countries: Model Development and Validation

Through Structural Equation Modeling', *International Journal of Computer Science & Information Technology*, 6(1), p.77.

European Commission (2013) 'Digital by default, or by Detour?' Assessing User Centric eGovernment performance in Europe -2012 Benchmark

Evans, D. and Yen, D. C. (2006) 'E-Government: Evolving relationship of citizens and government, domestic, and international development', *Government Information Quarterly*, 23(2), pp. 207−235.

Evely, A. C., Fazey, I, Pinard, M. and Lambin, X. (2008) 'The influence of philosophical perspectives in integrative research: a conservation case study in the Cairngorms National Park', *Ecology and Society*, 13(2), pp. 52,

[Online]. Available at: http://www.ecologyandsociety.org/vol13/iss2/art52/.

Fang, Z. (2002) 'E-Government in digital era: Concept, practice and developmen',

International Journal of the Computer, The Internet, and Information, 20, pp. 193−213.

Featherman, M. S. and Pavlou, P. A. (2003) 'Predicting e-services adoption: a perceived risk facets perspective', *International journal of human-computer studies*, 59(4), pp. 451-474.

Fielder, A., Brown, I., Weber, V. and McSpedden-Brown, N. (2012) 'Cloud Computing', Economic and Scientific Policy, Brussels: Directorate General For Internal Policies.

Finstad, K. (2010) 'Response interpolation and scale sensitivity: Evidence against 5-point scales', *Journal of Usability Studies*, 5(3), pp. 104-110.

Fishbein M and Ajzen I (1975) 'Belief, attitude, intention and behavior: an introduction to theory and research', Addison-Wesley, Boston

Fetaji, M., Loskoska, S., Fetaji, B. and Ebibi, M. (2007) 'Investigating human computer interaction issues in designing efficient virtual learning environments', In Balkan Conference in Informatics (BCI 2007), pp. 313-324.

Fitzgerald, B. and Howcroft, D. (1998) 'Towards Dissolution of the IS Research Debate: From Polarisation to Polarity', *Journal of Information Technology*, 13(4), pp. 313-326.

Fryer, R. J. (1991) 'A model of between-haul variation in selectivity', *ICES J*, 48, pp. 281–290.

Fu, J. R., Farn, C. K. and Chao, W. P. (2006) 'Acceptance of electronic tax filing: A study of taxpayer intentions', *Information & Management*, 43(1), pp.109-126.

Fu, J. R., Chao, W. P. and Farn, C. K. (2004) 'Determinants of taxpayers' adoption of electronic filing methods in Taiwan: An exploratory study', *Journal of Government Information*, 30(5), pp.658-683.

Galliers, R. D. (1992) *Choosing information systems research approaches.* In R. D. Galliers (ed.), Information Systems Research: Issues, Methods and Practical Guidelines (p. 144). Oxford: Blackwell Scientific.

Gefen, D., Rose, G.M., Warkentin, M. and Pavlou, P. (2005) 'Cultural diversity and trust in IT adoption', *Journal of Global Information Management*, 13(1), pp.54-78.

Gefen, D., Karahanna, E. and Straub, D.W. (2003) 'Trust and TAM in online shopping: an integrated model', *MIS quarterly*, 27(1), pp.51-90.

General Accounting Office (2001) *Electronic government: challenges must be addressed with effective leadership and management.* GAO-01-959T, pp. 1-2.

Gharehchopogh, F.S. and Hashemi, S. (2012) 'Security Challenges in cloud computing with more emphasis on trust and privacy', *International Journal of Scientific & Technology Research*, 1(6), pp.2277-8616.

Giddens, A. (1984) The Constitution of Society: Outline of the Structuration Theory.

Giustiniano, L. and 'Bolici, F. (2012) 'Organizational trust in a networked world: Analysis of the interplay between social factors and Information and Communication Technology', *Journal of Information, Communication and Ethics in Society*, Vol. 10, No. 3, pp. 187 – 202.

Gonçalves, G. (2013) 'Thematic Programme Capitalisation', *Analysis report on E-Government services*.

Goodhue, D. L. and Thompson, R. L. (1995) 'Task-Technology Fit and Individual Performancel', *MIS Quarterly*, 19(2), 213-236.

Goswami, S. (2014) 'Understanding adoption of electronic G2C service: An extension to Technology Adoption Model', *Pacific Business Review International*, 6(8).

Gravetter, F. and Wallnau, L. (2013) *Essentials of statistics for the behavioral sciences*. Cengage Learning.

Greunen, D. V., Herselman, M. E., and Niekerk, J. V. (2010) 'Implementation of regulation-based e-procurement in the Eastern Cape provincial administration', African Journal of Business Management, 4(17), pp. 3655–3665.

Guba, E. G. and Lincoln, Y. S. (1989) *Fourth Generation Evaluation*. Sage, CA.

Gulliksen, J. (2014, October) 'Human computer interaction and societal impact: can HCI influence public policy making IT politics?', *In Proceedings of the 13th Brazilian Symposium on Human Factors in Computing System*s (pp. 1-1). Sociedade Brasileira de Computação.

Guo, X. and Chen, G. (2005) 'Internet diffusion in Chinese companies', *Communications of the ACM*, 48(4), pp. 54-58.

Gupta, M. P. and Debashish J. (2003) 'E-Government evaluation: A framework and case study', Government Information Quarterly, 20(4), pp. 365-387.

Haider, Z., Shuwen, C., and Burdey, M. B. (2016) 'E-Government Project Obstacles in Pakistan', *International Journal of Computer Theory and Engineering*, 8(5), pp. 362.

Hair, J.F., Bush, R. P. and Ortinau, D.J. (2003) *Marketing research: Within a changing information environment. 2nd edn*. McGraw-Hill/ Irwin, New York.

Hair, J., Black, W, Babin, B., Anderson, R. and Tatham, R. (2006) *Multivariate data analysis, 6th edn*. Pearson Education, Inc, Upper Saddle River, New Jersey.

Halaris, C., Magoutas, B., Papadomichelaki, X and Mentzas, G. (2007) 'Classification and synthesis of quality approaches in e-Government services', *Internet Research*, 17(4), pp. 378-401.

Haley, S. M. and Osberg, J. S. (1989) 'Kappa coefficient calculation using multiple ratings per subject: a special communication', *Physical Therapy*, 69(11), pp. 970-974.

Hasan, M. M. (2015) 'E-Government Service Research Development: A Literature Review', *International Journal of E-Services and Mobile Applications (IJESMA)*, 7(1), pp.22-49.

Hashim, H. S., Hassan, Z. B. and Hashim, A. S. (2015) 'Factors Influence the Adoption of Cloud Computing: A Comprehensive Review', *International Journal of Education and Research*, Vol. 3(7).

Hashim, H. S. and Hassan, Z.B (2015) 'Factors That Influence The Users' Adoption Of Cloud Computing Services At Iraqi Universities: An Empirical Study', *Australian Journal of Basic and Applied Sciences*, 9(27) August 2015, Pages: 379-390

Heeks, R. (2003) 'Most eGovernment-for-Development Projects Fail: How Can Risks be Reduced?', *Government Working Paper Series*, Paper no. 14.

Heeks, R. (2004) 'Causes of E-Government Success and Failure: Factor Model', Institute for Development Policy and Management, University of Manchester, Manchester.

Helbig, N., Ramón, J. G.-G. and E. Ferro, E. (2009) 'Understanding the complexity of electronic government: Implications from the digital divide literature', Government Information Quarterly, Vol. 26 (1), pp. 89-97.

Holden, S. H., Norris, D. F. and Fletcher, P. D. (2003) 'Electronic government at the local level: Progress to date and future issues', *Public Performance and Management Review*, .344–325 ,(4)26

Irvine, C. E.

Holmes-Smith, P., Coote, L. and Cunningham, E. (2006) *Structural equation modeling: From the fundamentals to advanced topics*. SREAMS, Melbourne.

Hu, L. T. and Bentler, P. M. (1998) 'Fit indices in covariance structure modeling: Sensitivity to underparameterized model misspecification', *Psychological methods*, 3, pp. 424-453.

Hu, L. T. and Bentler, P. M. (1999) 'Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives', *Structural Equation Modeling: A Multidisciplinary Journal*, 6(1), pp. 1-55.

Hussey, J. and Hussey, R. (1997) Business Research: a practical guide for undergraduate and

postgraduate students. London: Macmillan Press.

Hwang, W., Jung, H.-S. and Salvendy, G. (2006) 'Internationalisation of e-commerce: A comparison of online shopping preferences among Korean, Turkish and US populations', *Behaviour and Information Technology*, 25(1), 3–18.

Iachello, G. and Hong, J. (2007) 'End-User Privacy in Human–Computer Interaction', *Human Computer Interaction*, 1(1), pp. 1–137.

IBM (2015) Cloud Computing Simplified: The Thoughts on Cloud Way.

Ibrahim, I. and Pope, J. (2011) 'Compliance costs of electronic tax filing for personal taxpayers in Malaysia', *In International Conference on Management*, pp. 927-940.

Ihmouda, R., Alwi, N.H. M. and Abdullah, I. (2015) 'Successful Factors on E-Government Security Social-Technical Aspect', ARPN Journal of Engineering and Applied Sciences, Vol. 10, No 20.

Ihmouda R. and N.H.M. Alwi (2014) A Comparative Analysis of e-Government security frameworks Social-Technical Security Aspect. International Journal of Management & Information Technology.

Ihmouda R.H. and N.H. Mohd Alwi (2013) 'Penetration Testing For Libyan Government Website', In: Proceedings of the 4th International Conference on Computing and Informatics, ICOCI 2013, 28-29 August, 2013. Sarawak, Malaysia. Universiti Utara Malaysia (http://www.uum.edu.my): Universiti Utara Malaysia (http://www.uum.edu.my).

Irani, Z., Love, P.E.D. and Jones, S. (2008) 'Learning Lessons From Evaluating

Egovernment: Reflective Case Experiences That Support Transformational Government', *The Journal of Strategic Information Systems*, 17(2), 2008, pp. 155-164.

Irvine, C. E. (2000) Security issues for automated information systems, In G. D. Garson (Ed.), Handbook of Public Information Systems. New York: Marcel Dekker, Inc.

Isabella, L. A. (1992) 'Managing the Challenges of Trigger Events: The Mindsets of Governing Adaptation to Change', *Business Horizons*, 35, 59–66.

Janssens, W., Wijnen, K., De Pelsmaker, P. and Van Kenhove, P. (2008) *Marketing research with SPSS*. Essex, England, Pearson Education Limited.

Jarvenpaa, S. L., Tractinsky, N. and Vitale, M. (2000) 'Consumer trust in an Internetstore', *Information Technology and Management*, 1(12), 45–71.

Johnston, J., Eloff, J. and Labuschagne, L. (2003) 'Security and Human Computer Interfaces', *Computers and Security*, 22(8), pp. 675-684.

Jöreskog, K., G. and Sörbom, D. (1984) *LISREL-VI user's guide*. 3rd ed. Mooresville, IN: Scientific Software.

Joshi, J., Ghafoor, A., Aref, W. G., and Spafford, E. H. (2001) 'Digital government security infrastructure design challenges', *IEEE Computer*, 34(2), pp. 66-72.

Kayrouz, A. and Atala, I. (2014) 'E-Government in Lebanon', European Scientific Journal, 10(7).

Keil, M., Beranek, P. M., and Konsynski, B. R. (1995) 'Usefulness and ease of use: field study evidence regarding task considerations', *Decision Support Systems*, 13(1), 75-91.

Kemp Little LLP (2013) Cloud Computing-The Rise of Service-Based Computing.

Khan, G. F., Moon, J., Park, H. W., Swar, B. and Rho, J. J. (2010) 'A socio-technical perspective on e-Government issues in developing countries: A scientometrics approach', Scientometrics, 87(2), pp.267-286.

Khazanchi, D. and Munkvold. B.E. (2002) 'On the Rhetoric and Relevance of IS Research Paradigms: A Conceptual Framework and Some Propositions', *Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS'03).*

Kim. C., Wang Tao, W., Shin, N. and Kim, K. (2010) 'An empirical study of customers' perceptions of security and trust in e-payment systems', *Electronic Commerce Research and Applications*, 9(1), pp. 84-95.

Kline, R. B. (1998) *Principles and Practice of Structural Equation Modeling*. New York: The Guilford Press.

Kumar, V., Mukerji, B., Butt, I. and Persaud, A. (2007) 'Factors for Successful e-Government Adoption: a Conceptual Framework', *The Electronic Journal of e-Government*, 5(1), pp. 63-76. Available online at www.ejeg.com.

Kuhn, T. S. (1977) *The essential tension: selected studies in scientific tradition and change*. University of Chicago Press, Chicago, Illinois, USA.

Lagzian, M. and Naderi, N. (2015) 'An Empirical Study of the Factors Affecting Customers' Acceptance Intention of E-Invoice Services: The Case of Mashhad Electricity Distribution Company.

Lee, G., and Lin, H. (2005) Customer perceptions of e-service quality in online shopping.International Journal of Retail & Distribution Management, 33(2), 161–176.

Lee, J., Kim, H. J. and Ahn, M. J. (2011) 'The willingness of e-Government service adoption by business users: The role of offline service quality and trust in technology', *Government Information Quarterly*, 28(2), pp.222-230.

Lee, J. and Rao, H. R. (2007) 'Perceived risks, counter-beliefs, and intentions to use anti-/counter-terrorism websites: an exploratory study of government–citizens online interactions in a turbulent environment', *Decision Support Systems*, 43(4), pp.1431-1449.

Leedy, P. D. and Ormrod, J. E. (2005) *Practical research: Planning and design*. New Jersey: Prentice Hall.

Legris, P., Ingham, J. and Collerette, P (2003) 'Why Do People Use Information Technology? A Critical Review of the Technology Acceptance Model', *Information and Management*, 49, pp. 191-204.

Li, D. X., (1999) 'Value at Risk based on the volatility', Skewness and Kurtosis. Risk Metrics Group.

Lim, N., Grönlund, Å. and Andersson, A. (2015) 'Cloud Computing: The Beliefs and Perceptions of Swedish School Principals', *Computers & Education*, 84, 90-100.

Loo, W. H., Yeow, P., and Chong, S. C. (2009) 'User acceptance of Malaysian government multipurpose smartcard applications', *Government Information Quarterly*, (26), 2009, pp. 358-367.

Lööf, H. and Heshmati, A. (2008) 'Investment and performance of firms: correlation or causality?', *Corporate Ownership & Control*, 6(2), pp. 268-282.

Luna-Reyes, L., & Gil-Garcia, J. R. (2003) 'eGovernment & Internet Security: Some Technical and Policy Considerations', *Paper presented at the National Conference on Digital Government Research*, organized by the National Science Foundation, Boston, MA, USA.

MacCallum, R. C. (1986) 'Specification searches in covariance structure modeling', *Psychological Bulletin*, 100, pp. 107–120.

Majdalawi, Y. K., Almarabeh, T., Mohammad, H., and Quteshate, W. (2015) 'E-Government Strategy and Plans in Jordan', *Journal of Software Engineering and Applications*, Vol 8(4), 211.

Mathieson, K., Peacock, E. and Chin, W.W. (2001) 'Extending the technology acceptance model: the influence of perceived user resources', *ACM SigMIS Database*, 32(3), pp.86-112.

Mccarthy, J., Strachey, C. And Clark, W. (2014) 'Information Science and Human-Computer Interaction.

Mayer, R. C., Davis, J. H. and Schoorman, F.D. (1995) 'An integrative model of organizational trust', *Academy of management review*, 20(3), pp.709-734.

McNab, C. (2007) *Network Security Assessment*. O'Reilly & Associates, Sebastopol, CA.

Meloun, M. and Militký, J. (2001) 'Detection of single influential points in OLS regression model building', *Analytica Chimica Acta*, 439(2), pp. 169-191.

Melville, N. and Ramirez, R. (2008) 'Information technology innovation diffusion: An information requirements paradigm', *Information Systems Journal*, 18 (3), 247-273.

Millard, J. (2007) *Inclusive e-Government: Survey of Status and Baseline Activities [R/OL]*. Brussels: European Commission Information Society and Media.

Milner, E. M. (2000) Managing Information and Knowledge in the Public Sector. New York: Routledge.

Moody, D. (2002) 'Empirical research methods', [Online]. Available at: ww.idi.ntnu.no/~ekaterip/dif8916/Empirical%20Research%20Methods%20Outline.pdf. (Accessed: November 2011).

Morgan, G. and Smircich, L. (1980) 'The case for qualitative research', *The Academy of Management Review*, 5, pp. 491–500.

Mourao, R. R., Yoo, J., Geise, S., Araiza, J. A., Kilgo, D. K., Chen, V. Y. And Johnson, T. J. (2015) Online News, Social Media, and European Union Attitudes: A Multidimensional Analysis, International *Journal of Communication*, 9, pp.1-20.

Mulaik, S. A., James, L. R., Van Alstine, J., Bennett, N. Lind, S. and Stilwell, C. D. (1989) 'Evaluation of goodness-of-fit indices for structural equation models',. *Psychological Bulletin*, 105, pp. 430–445.

Myeong, S., Kwon, Y. and Seo, H. (2014) 'Sustainable E-Governance: The Relationship among Trust, Digital Divide, and E-Government', *Sustainability*, 6(9), pp. 6049-6069.

Nawafleh, S., Obiedat, R. and Harfoushi, O. (2012) 'E-Government between developed and developing countries', *International Journal of Advanced Corporate Learning (iJAC)*, 5(1), pp.8-13.

Nesbary, D. (2000) *Survey research and the World Wide Web*. USA: Allyn and Bacon.

Approach', *Interdisciplinary Journal of Information, Knowledge, and Management*, 5.

Nosrati, M., Karimi, R. and Hasanvand, H.A. (2012) 'Mobile computing: principles, devices and operating systems', *World Applied Programming*, 2(7), pp.399-408.

Nulty, D. D. (2008) 'The adequacy of response rates to online and paper surveys: what can be done?', *Assessment & Evaluation in Higher Education*, 33(3), pp. 301-314.

Nunnally, J. C., and Bernstein, I. H. (1994) *Psychometric theory*. New York: McGraw-Hill.

Ojo, A., Janowski, T. and Estevez, E. (2011) 'Whole-of-government approach to information technology strategy management: Building a sustainable collaborative technology environment in government', *Information Polity*, 16(3), pp.243-260.

Olatunji, B. O., Williams, N. L., Tolin, D. F., Sawchuk, C. N., Abramowitz, J. S. and Lohr, J. M. (2007) 'The Disgust Scale: Item analysis, factor structure, and suggestions for refinement', *Psychological Assessment*, 19, pp. 281–297.

Omotayo, F. O. and Adebayo, A. K. (2015) 'Factors Influencing Intention to Adopt Internet Banking by Postgraduate Students of the University of Ibadan, Nigeria', *J Internet Bank Commer*, 20(123), p.2.

Ong, C-S. and Wang, S-W. (2009) 'Managing citizen-initiated email contacts', *Government Information Quarterly*, 26, pp. 498–504.

Orlikowski, W. J. and Baroudi, J. J. (1989) 'IS Research Paradigms: Method versus Substance'.

Orlikowski, W. J. and Baroudi, J. J. (1991) 'Studying Information Technology in Organizations: Research Approaches and Assumptions', *Information Systems Research*, 2(1), pp. 1-8.

Osman, I. H., Anouze, A. L., Azad, B., Daouk, L., Zablith, F., Hindi, N. M, Irani, Z., Lee, H. and Weerakkody, V. (2013) 'The elicitation of key performance indicators of e-Government providers: A bottom-up approach'.

Ouyang, Y.C. and Lee, T.C. (2015) 'The Human Resource Development Strategies on Information Technology Semi-Professionals Adoption of the Local Government', J Socialomics, 4 (129), pp.2167-0358.

Pallant, J. (2010) *SPSS survival manual: A step by step guide to data analysis using SPSS*. Open University Press.

Papadomichelaki, X. and Mentzas, G. (2012) 'e-GovQual: A multiple-item scale for assessing e-Government service quality', *Government information quarterly*, 29(1), pp.98-109.

Parahoo, A. K. (1997) *Nursing Research*. Principles. Process and Issues. London, MacMillan.

Parent, M., Vandebeek, C. A., and Gemino, A. C. (2005) 'Building citizen trust through e-Government', *Government Information Quarterly*, 22(4), pp. 720−736.

Patel, S. C., Graham, J. H. and Ralston, P. A. (2008) 'Quantitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements', *International Journal of Information Management*, 28(6), pp. 483-491.

Pavlou, P. A. (2003) 'Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model', *International Journal of Electronic Commerce*, 7(3), pp. 69-103.

Pavlou, P. A. and Gefen, D. (2004) 'Building effective online marketplaces withinstitution-based trust.

Peterson, D., Meinert, D., Criswell, J. and Crossland, M. (2007) 'Consumer trust: privacy policies and third-party seals', *Journal of Small Business and Enterprise Development*, Vol 14(4), pp.654-669.

Peikari, H. R. (2010a) 'Does nationality matter in the B2C environment? Results from a two nation study', *Communications in Computer and Information Science*, 92,149–159.

Peikari, H. R. (2010c) 'The influence of security statement, technical protection, and privacy on satisfaction and loyalty', *Communications in Computer and Information Science*, 92, 223–231.

Persaud, Ajax and Priya Persaud (2013) 'Rethinking E-Government Adoption: A User-Centered Model', *International Journal of Electronic Government Research*, 9(4): 56–74.

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y. and Podsakoff, N. P. (2003) 'Common method biases in behavioral research: a critical review of the literature and recommended remedies', *Journal of applied psychology*, 88(5), pp. 879.

Ranaweera, H. M. B. P. (2016) 'Perspective of trust towards e-Government initiatives in Sri Lanka', *SpringerPlus*, 5(1), pp.1-11.

Cook, T. D. and Reichardt, C. S. (Eds.). (1979) *Qualitative and quantitative methods in evaluation research, 1(1)*. Beverly Hills eCA CA: Sage publications.

Renny, Guritno S. and Siringoringo, H. (2013) 'Perceived Usefulness, Ease of use, and Attitude Towards Online Shopping Usefulness Towards Online Airlines Ticket Purchase', *Procedia - Social and Behavioral Sciences 81*, pp. 212 – 216.

Ribbink, D., van Riel, A. C. R., Liljander, V., and Streukens, S. (2004) 'Comfort your onlinecustomer: Quality, trust and loyalty on the internet', *Managing Service Quality*, pp14, 446–456.

Robinson, J. P., Shaver, P. R. and Wrightsman, L. S. (1991) 'Criteria for scale selection and evaluation', *Measures of personality and social psychological attitudes*, 1, pp. 1-16.

Rogers, E. M., (1995). *Diffusion of Innovations (4th Edition)*. The Free Press, New York, USA.

Roscoe, J. T. (1975) *Fundamental research statistics for the behavioral sciences* (2ed).New York: Holt, Rinehart and Winston.

Rotter, J. B. (1971) 'Generalized expectancies for interpersonal trust', American Psychologist, 26, pp. 443–452.

Roy, J. (2003) 'The relational dynamics of e-governance: A case study of the City of Ottawa', *Public Performance and Management Review*, 26(4), 391–403.

Ryan, P. and Falvey, S. (2012) '*Trust in the clouds*', Computer Law and Security Reviews, 28, 513 521. http://dx.doi.org/10.1016/j.clsr.2012.07.002.

Sarabdeen, J. and Ishak, M.M.M. (2015) Impediment of privacy in the use of clouds by educational institutions.

Saunders, M., Lewis, P. and Thornhill, A. (2007) *Research Methods for Business Students*. The UK: Pearson Education Limited.

Sapsford, R. and Jupp, V., eds. (2006) *Data collection and analysis*. Sage,.

Schreiber, J. B., Nora, A., Stage, F. K., Barlow, E. A. and King, J. (2006) 'Reporting structural equation modeling and confirmatory factor analysis results: A review', *The Journal of Educational Research*, 99(6), pp. 323-338.

Schumacker, R. E. and Lomax, R. G. (1996) 'A beginner's guide to structural equation modeling, *Mahwah, New Jersey: Lawrence Erlbaum Associates*, pp. 288, 144.

Schwester, R. (2009) 'Examining the Barriers to E Government Adoption', Elec. J, e-Govt., 7 (1), pp:113-122

Sekaran, U. (2006*) Research methods for business*. John Wiley & Sons.

Shah, M. H., Peikari, H. R., and Yasin, N. M. (2014) 'The determinants of individuals' perceived e-security: Evidence from Malaysia', *International Journal of Information Management*, 34(1), pp. 48-57.

Shang, S. S. (2014) 'Assessment of E-Government Service Quality under User Satisfaction Orientation: The Establishment of E-Govqual Model', *Asian Journal of Business Management*, 6(2), pp.111-118.

Shanks G. and Parr A. (2003) 'Positivist single case study research in information systems: a critical analysis', *In Proceedings of the Eleventh European Conference on Information Systems*, pp. 1760-1774.

Shareef, A., Kumar, U., Kumar, V. and Dwivedi, Y. (2009) 'Identifying Critical Factors for Adoption of E-Government', *Electronic Government, an International Journal*, 6(1), pp. 70–96.

Shareef, M. A., Kumar, V., Kumar, U. and Dwivedi, Y. K. (2011) 'e-Government Adoption Model (GAM): Differing service maturity levels', *Government Information Quarterly*, 28(1), 17-35.

Sharma, S. (1995). Applied multivariate techniques. John Wiley & Sons, Inc.

Shipps, B. (2013) 'Social networks, interactivity and satisfaction: assessing socio-technical behavioral factors as an extension to technology acceptance', *Journal of theoretical and applied electronic commerce research,* 8(1), pp.35-52.

Siponen, M. T. and Oinas-Kukkonen, H. (2007) 'A review of information security issues and respective research contributions', *SIGMIS Database*, 38(1), pp. 60-80.

Soat, J. (2003). Privacy, security, identity still matter. *Information Week*, 936, 75.

Srivastava, S. C., and Teo, T. (2005) 'Citizen trust development for e-Government adoption: Case of Singapore', *PACIS 2005 Proceedings*, 59.

Srivastava, S. C. and T. S. H. Teo (2009) 'Citizen Trust Development for E-Government Adoption And Usage: Insights From Young Adults In Singapore', Commun. Assoc. Inform. Syst., Vol 25(1): 31.

Steiger, J. H. (2000) 'Point estimation, hypothesis testing, and interval estimation using the RMSEA: Some comments and a reply to Hayduk and Glaser', *Structural Equation Modeling*, 7, pp. 149–162.

Stoddard, O. and Leibbrandt, A. (2014) 'An experimental study on the relevance and scope of nationality as a coordination device', *Economic Inquiry*, 52(4), pp.1392-1407.

Supreme Committee for Information and Communication Technology–SCICT (2015) eGovernment STRATEGY 2016, Kingdom Of Bahrain.

Taylor, S. and Todd, P. (1995a) 'Assessing it usage: the role of prior experience', *MIS Quarterly,* 19(4), pp. 561-70.

Ten Berge, J. M. and Sočan, G. (2004) 'The greatest lower bound to the reliability of a test and the hypothesis of unidimensionality', *Psychometrika*, 69(4), pp. 613-625.

Teo, T. S., Srivastava, S. C., and Jiang, L. (2008) 'Trust and electronic government success: An empirical study', *Journal of Management Information Systems*, 25(3), 99-132.

Thao, V. T. T, and Trong h. V (2015) 'Examining the Influence of Society and Technology in Vietnam E-Government Adoption, 3(10.

Compeau, D. R., and Higgins, C. A. (1995) 'Computer Self-Efficacy: Development of a Measure and Initial Test', *MIS Quarterly*, (19:2), 1995, pp. 189-211.

Ticehurst, G. W. Veal, A. J. (2000) *Business research methods: a managerial approach*. Pearson Education Australia, NSW.

Tweneboah-Koduah, S., Endicott-Popovsky, B., and Tsetse, A. (2014) 'Barriers to Government Cloud Adoption', *International Journal of Managing Information Technology* (IJMIT) Vol.6, No.3, August 2014

Ullman, J. B. (2006) 'Structural equation modeling: Reviewing the basics and moving forward', *Journal of Personality Assessment*, 87(1), pp. 35-50.

UNPAN (2014) *UN e-Government Survey 2014*, E-Government for the Future We Want. New York: UNPAN. Retrieved June 25, 2014.

Usunier J.C. (1993) *Marketing across Culture*s, Hemel, Hempsted, Prentice Hall.

Väätäjä, H. (2014) Framing the User Experience in Mobile Newsmaking with Smartphones. Tam

van Velsen, L., van der Geest, T., ter Hedde, M. and Derks, W. (2009) 'Requirements engineering for e-Government services: A citizen-centric approach and case study', *Government Information Quarterly*, 26(3), pp.477-486.

Vassilakis, C., Lepouras, G. and Halatsis, C. (2007) 'A knowledge-based approach for developing multi-channel e-Government services', *Electronic Commerce Research and Applications*, 6, pp. 113–124.

Veal, A. J. (2005) *Business research method: a managerial approach (2nd ed)*. Frenchs Forest: Pearson Addison Wesley.

Venkatesh, V., Thong, J.Y. and Xu, X., (2012) 'Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology', *MIS quarterly*, 36(1), pp.157-178.

Venkatesh, V. and Davis, F. D. (2000) 'A Theoretical Extension of The Technology Acceptance Model: Four Longitudinal Field Studies', *Management Science*, 46(2), pp. 186-204.

Venkatesh, V., Morris, M., and Ackerman, P.L. (2000) ‘, A Longitudinal Field Investigation of Gender Differences in Individual Technology Adoption Decision Making Processes’, *Organizational Behavior and Human Decision Processes* , (83:1), pp. 33-60.

Venkatesh, V., Morris, M. G., Davis, G. B. and Davis, F. D. (2003) ‘User acceptance of information technology: toward a unified view’, *MIS Quarterly*, pp. 425–478.

Verma, R. and Goodale, J. C. (1995) ‘Statistical power in operations management research’, Journal of Operations Management, 13(2), pp. 139-152.

Voorsluys, W., Broberg, J. and Buyya, R. (2011) ‘Introduction to cloud computing’, *Cloud computing: Principles and paradigms*, pp.1-44.

Voutinioti, A. (2013) ‘Determinants of User Adoption of e-Government Services in Greece and the Role of Citizen Service Centres’, *Procedia Technology*, 8, pp.238-244.

Walsham, G. (2006) ‘Doing Interpretive Research, European’, *Journals of Information Systems*, 15, pp. 320-330.

Warkentin, M., Gefen, D., Pavlou, P. and Rose, G. (2002) ‘Encouraging citizen adoption of e-Government by building trust’, Electronic Markets, 12 (3), pp. 157–162.

Weerakkody, V., El-Haddadeh, R. and Al-Shafi, S. (2011) ‘Exploring the Complexities of e-Government Implementation and Diffusion in a Developing Country: Some Lessons from the State of Qatar’, *Journal of Enterprise Information Management*, 24, pp. 172-196. http://dx.doi.org/10.1108/17410391111106293

Wei, X. and Zhao, J. (2005, August) ‘Citizens' requirement analysis in Chinese e-Government’, *In Proceedings of the 7th international Conference on Electronic Commerce*, pp. 525-428. ACM.

Weisstein, E. W. (2004) ‘Moore-Penrose Matrix Inverse’, http://mathworld.wolfram.com/Moore-PenroseMatrixInverse.html.

Welch, E. W., Hinnant, C. C. Moon, M. J. (2005) ‘Linking citizen satisfaction with e-Government and trust in government’, *Journal of Public Administration Research and Theory*, 15(3), pp. 371-391.

West, D. M. (2001) WMRC global e-Government survey, Taubman Center for Public Policy, Brown University.

West, D. M. (2006) Global E-Government, To order raw e-Government data.

Williams, P. A. (2008) ‘In a ‘trusting’ environment, everyone is responsible for information security’, *Information Security Technical Report*, 13(4), pp. 207-215.

Wischnevsky, J. D (2004) 'Change as the Winds Change: The Impact of organisational Transformation on Firm Survival in a Shifting Environment', *Organisational Analysis*, Vol 12, No, 4., pp.361-377.

Woodward, R. (2009) 'The Organization for economic co-operation and development (OECD)', 35, Routledge.

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*, Vol 1(1), pp. 1-20.

Yaghoubi, N. M., Baqer Kord, B. and Shakeri, R. (2010) 'E-Government Services and user Acceptance: The Unified Models' Perspective', *European Journal of Economics, Finance and Administrative Sciences*, 24(1).

Yan, H. and Yang, Z. (2015) 'Examining Mobile Payment User Adoption from the Perspective of Trust', *International Journal of u-and e-Service, Science and Technology*, 8(1), pp.117-130.

Zait, A. and Bertea, P., E. (2011) 'Methods for testing discriminant validity', *Management & Marketing*, 9(2), pp. 217-224.

Zeithaml, V.A., Parasuraman, A., and Malhotra, A. (2002) 'Service quality delivery through web sites: A critical review of extant knowledge', *Journal of the Academy of Marketing Science*, 30(4), pp. 362-375.

Zhang, P., Galletta, D. Li, N. and Sun, H. (2009) 'Human-Computer Interaction, in Wayne Huang (ed.)', *Management Information Systems*, Tsinghua, University Press, Beijing, China.

Zhang, N., Guo, X. and Chen, G. (2007) 'Diffusion and Evaluation of E-Government Systems: A field study in China', *PACIS 2007 Proceedings*, 2.

Ziemba, E. Tomasz Papaj, T. and Jadamus-Hacura, M. (2015) 'E-Government Success Factors: A Perspective on Government Units', Issues in Information Systems, Volume 16, Issue II, pp. 16-27.

Zikmund, W. G. and Babin, B., J. (2007) *Exploring Marketing Research (9th Edition).* Thomson

South-Western, Mason.

Žilinskas, G. and Gaulė, E. (2013) 'E-governance in Lithuanian Municipalities: External Factors Analysis of the Websites Development', *Public Policy And Administration*, 12(1), pp.80-93.

Appendix A: Literature Review Chapter Support Document

Table A1: Online Services offered by governments across the world by region (percentage) (West 2006)						
	2001	**2002**	**2003**	**2004**	**2005**	**2006**
North America	28%	41%	45%	53%	56%	71%
Pacific Ocean Islands	19	14	17	43	24	48
Asia	12	26	26	30	38	42
Middle East	10	15	24	19	13	31
Western Europe	9	10	17	29	20	34
Eastern Europe	--	2	6	8	4	12
Central America	4	4	9	17	15	11
South America	3	7	14	10	19	30
Russia/Central Asia	2	1	1	2	3	11
Africa	2	2	5	8	7	9

Appendix B: Research Ethics

Appendix B1: Permission for participating in the online survey pursued by email communication

Brunel Business School

Research Ethics

Participant Information Sheet

1. Title of Research: Factors Determining e-Government Security

2. Researcher: Hasan Razzaqi, Degree of Doctor of Philosophy in information system, Brunel Business School, Brunel University.

3. Contact Email: cspghhr2@brunel.ac.uk/ hrazzaqi@ahlia.edu.bh

4. Purpose of the research*:* Develop an e-Government security mechanism from user perspective to comprehend the users the level of security built into the e-Government services websites, and to increase the trust and satisfaction level of the users have in the e-Government services.

5. What is involved?

Participants would evaluate the level of security available in e-Government services portals from users' perspective which involves the following security factors (Human Computer Interactivity-HCI, information privacy, quality of services, trust and risk).

6. Voluntary nature of participation and confidentiality.

Participation in this project is voluntary. Completion of this survey indicates your consent to participate in this research. The provided answers will be kept in strict confidence and will be used for the purpose of this research only.

Dear Colleague,

I would be grateful to you if you could participate in my PhD research survey. Please use the URL links below (Arabic/English) to participate in the survey;

English: http://www.ahlia.edu.bh/survey/index.php?sid=26979&lang=en

(**Please try to answer all the questions and click on the Submit button**).

Please forward a copy of this email to your friends who might be interested in participating in the research survey.

Thank you for your cooperation.

Best regards

Appendix C: Questions Survey and Statistical Analysis Tables

Table C1: Questionnaire for Measuring the Security of E-Government Services

No.	Code	Demographic factor	Option				
1	DF1	Gender:	Female (1)		Male (2)		
2	DF2	Age:	<20	21-30	31-40	41-50	>51
3	DF3	Occupation:	Private Sector	Government	Students	Un-employed	Retiree
4	DF4	Education:	No Education	Middle School	Higher School	College	Post-Graduate
5	DF5	Income (B.D):	<400	401-750	751-1150	11501-1550	>1551
6	DF6	No. of years of internet experience:	No- Experience	<3 years	3-6 years	6-10 years	>10 years
7	DF7	Country (please choose from the options below):					
8	DF8	Type of online services used recently (please choose from the options below):					

1. Abnormal Load Permission for Public Works
2. Accredited Missions in the Country
3. Agency Registration Inquiry
4. Application for Eid AlElm Ceremony
5. Application for Social Assistance
6. Apply for an e-Visa
7. Apply for Building Permit
8. Apply for Visit e-NOC
9. Appointment for Driving Training Class
10. Appointment for Smart Card/Passport
11. Aviation Licensing
12. Center of Studies & Research Library Reservation
13. Country Embassies Abroad
14. Country Events Calendar
15. Country Laws
16. Country Locator
17. Country Municipal – Geoexplorer
18. Body Mass Index (BMI)
19. Building Maintenance Request
20. Check Appointment
21. Check status of e-Visa
22. Check your Blood Record
23. Civil Service Employee Services
24. Commercial Registration Application Follow up
25. Commercial Registration Inquiry

26. Consumer Protection Complaints
27. Contact Details for Hospitals, Clinics, Pharmacies & Health ...
28. Contractor Prequalification
29. Court Case Enquiry
30. Covenant Deed: "Swords of Loyalty" and the "Sword of Youth"
31. Crown Prince Award
32. Culture Events
33. Customer Care Services
34. Customs Clearing Services
35. Daily Price Index
36. Delivery Date Calculator
37. Disconnection Services
38. Drugs Prices
39. Electricity and Water Outage Complaints
40. Employer Submission for Job Vacancies
41. Employer's Account Statements
42. Endorsement, Accreditation and Validation of Academic Qualification
43. Enkiru Kids Club
44. e-Visa sponsor
45. e-Visa sponsor login
46. e-Weather
47. Flight Information
48. Formation of Regulation Cases
49. Gasoline Octane Inquiry
50. General Complaints of High Consumption
51. Hajj and Umrah Agencies Directory
52. Hajj Services
53. Health immunization and vaccines
54. Hotel Directory
55. Housing Services Eligibility Criteria
56. Insurance for job seekers
57. Issuance of Disability Cards for Disabled People
58. Issuance of Insurance policies for King Fahad Causeway
59. Issue of Advertisement Permits
60. Issue of Notary Certificates
61. Issue of Wealth Distribution Certificates
62. Issuing Copies of Student Certificates
63. Country State Budget
64. Labour Complaints
65. Legality of Foreign Worker
66. Letter Submission for Housing Services
67. Levy Calculator
68. Materials Testing Results (QC)
69. Municipal Land for Investors
70. Municipality Services
71. National Enterprise Architecture Framework
72. Payment and Enquiry of Court Execution Ruling
73. Payment of Criminal Orders
74. Payment of Electricity & Water Bill
75. Payment of Mailboxes
76. Payment of Traffic Contraventions
77. Payment of University Course
78. Personal Information
79. Pilgrim Registration Enquiry
80. Pilgrims Feedback on the Hajj Travel Agencies
81. Pre-Employment Health Check-up Appointment

82. Principal Business Activity Details
83. Private Appointment
84. Public Libraries Services
85. Purchase Survey and Land Registration Bureau Maps
86. Radiology Result Status
87. Refuse Bags Status Tracking
88. Registration and Renewal of Lawyers, Experts and Brokers Lic...
89. Registration and Renewal of Hajj Travel Agents Licenses
90. Registration for Continuous Education Programs
91. Registration for Qudara'at Training Program
92. Registration in Summer Clubs
93. Registration of Hajj Agencies Medical Staff
94. Registration of Quran Competitors
95. Registration of Quran Students
96. Registration of Quran Teachers
97. Registration Service for Students abroad
98. Renewal of Commercial Registration License
99. Renewal of Driving License
100. Renewal of Mailboxes
101. Renewal of Vehicle Registration
102. Request for Birth Certificate
103. Request for Gift Letter Certificate
104. Sanitary Complaints
105. Sanitary Connections
106. Scholarships Application and Results
107. Standards & Metrology Complaints
108. Student Exam Results
109. Submit Meter Reading of Electricity and Water
110. Tender Awards
111. Tender Notices
112. Tendering Online
113. Tenders - Live opening
114. Tenders Opened
115. Tenders' to be opened
116. Tracking of Postal Packages
117. Traffic Diversion Request
118. Traffic Signal Service Requests
119. Training for Job Seekers
120. Unemployed Job Search
121. Unemployment Registration
122. Unit Maintenance Request
123. Update Yearly salaries
124. Visit e-NOC enquiry
125. Website Registration
126. Others

No.	Code	Question	Scale

The following questionnaire has a scale with seven options for each question ranging from 1 to 7. The options are as follows:

1= Strongly Disagree; 2= Disagree; 3= Somewhat Disagree; 4= Neither; 5= Somewhat Agree; 6= Agree;

7= Strongly Agree

Please choose the option you think is the most appropriate.

9	EEOU1	Most of the e-Government websites are easy to use.	①	②	③	④	⑤	⑥	⑦
10	EEOU2	It is easy to learn how to interact with e-Government websites.	①	②	③	④	⑤	⑥	⑦
11	EEOU3	Most of the e-Government websites are flexible to interact with.	①	②	③	④	⑤	⑥	⑦
12	EEOU4	Communication with the government agency is easier through its official websites.	①	②	③	④	⑤	⑥	⑦
13	EU1	I perceived that the usage of e-Government websites enables user transactions faster.	①	②	③	④	⑤	⑥	⑦
14	EU2	I perceived that the usage of e-Government websites can enhance the effectiveness of users' transactions with government.	①	②	③	④	⑤	⑥	⑦
15	EU3	Most of e-Government websites are useful for searching government services.	①	②	③	④	⑤	⑥	⑦
16	EU4	Most of e- Government websites are useful for conducting government transactions.	①	②	③	④	⑤	⑥	⑦
17	EWQ1	Most of the e-Government websites are easy to navigate.	①	②	③	④	⑤	⑥	⑦
18	EWQ2	Most of the e-Government websites' contents are easily accessible.	①	②	③	④	⑤	⑥	⑦
19	EWQ3	Most of the e-Government websites are intuitive.	①	②	③	④	⑤	⑥	⑦
20	EWQ4	Most of the e-Government websites provide sufficient information to search.	①	②	③	④	⑤	⑥	⑦
21	EWQ5	Most of the e-Government websites are easy to read.	①	②	③	④	⑤	⑥	⑦
22	EWQ6	Most of the e-Government websites are visually pleasing.	①	②	③	④	⑤	⑥	⑦
23	EWQ7	Most of the e-Government websites are professionally designed.	①	②	③	④	⑤	⑥	⑦
24	EWQ8	Most of the e-Government websites show users how to contact and communicate with them.	①	②	③	④	⑤	⑥	⑦
25	EHCI1	I felt comfortable using the interface available in most of e-Governments websites.	①	②	③	④	⑤	⑥	⑦
26	EHCI2	If I have to use the e-Government services in the future and an interface such as this is available, I would be very likely to use it.	①	②	③	④	⑤	⑥	⑦
27	EHCI3	I did not find the information I was looking for easily in most of e-Government websites.	①	②	③	④	⑤	⑥	⑦

28	EP1	My personal information given to an e-Government website may be shared with other e-Government agents to whom I do not want to provide the information.	①	②	③	④	⑤	⑥	⑦
29	EP2	The e-Government websites may allow another party to access my personal information without my consent.	①	②	③	④	⑤	⑥	⑦
30	EP3	My personal information could have been used in an unintended way by the e-Government agency.	①	②	③	④	⑤	⑥	⑦
31	EP4	Someone could have snatched my personal information while I am sending the information to an e-Government website.	①	②	③	④	⑤	⑥	⑦
32	EP5	Hackers may be able to intrude governmental websites and steal my personal information stored on the website.	①	②	③	④	⑤	⑥	⑦
33	EQ1	Generally, the e-Government services provide useful information.	①	②	③	④	⑤	⑥	⑦
34	EQ2	Generally, the e-Government services are effectively delivered.	①	②	③	④	⑤	⑥	⑦
35	EQ3	Generally, the e-Government services provide significant user interaction (communication).	①	②	③	④	⑤	⑥	⑦
36	EQ4	Generally, the e-Government services provide feedback mechanisms.	①	②	③	④	⑤	⑥	⑦
37	ET1	I believe that e-Government websites are competent and effective in providing government services.	①	②	③	④	⑤	⑥	⑦
38	ET3	Most e-Government websites provide effective platforms for users to interact with their government.	①	②	③	④	⑤	⑥	⑦
39	ET4	I believe that most e-Government websites are truthful in their dealings with the users.	①	②	③	④	⑤	⑥	⑦
40	ET5	I believe that most e-Government websites would keep data confidential.	①	②	③	④	⑤	⑥	⑦
41	ET6	I believe that most e-Government websites are genuine.	①	②	③	④	⑤	⑥	⑦
42	ET7	I believe that most of the times e-Government websites act in the users' best interest.	①	②	③	④	⑤	⑥	⑦
43	ET8	If the users required help, e-Government websites administration would do their best to help them.	①	②	③	④	⑤	⑥	⑦
44	ET9	I believe that most e-Government websites are interested in the users well-being, not just their own.	①	②	③	④	⑤	⑥	⑦

45	ER1	When using e-Government websites to transact with government departments and agencies, I feel that it is not secure to send sensitive information.	①	②	③	④	⑤	⑥	⑦
46	ER2	When using credit card to pay for government services through e-Government websites I feel that credit card details are likely to be stolen.	①	②	③	④	⑤	⑥	⑦
47	ER3	As I consider transactions with government department and agencies via e-Government websites, I worry about whether they will perform as they are supposed to.	①	②	③	④	⑤	⑥	⑦
48	ER4	If I were to transact with government departments and agencies via e-Government websites, I would be concerned that they would not provide the level of services that I would be expecting.	①	②	③	④	⑤	⑥	⑦
49	ER5	I am not confident about the ability of e-Government websites to perform as claimed.	①	②	③	④	⑤	⑥	⑦
50	ER6	Considering the possible problems associated with e-Government websites performance, a lot of risk would be involved with searching and requesting government services via e-Government websites.	①	②	③	④	⑤	⑥	⑦
51	ER7	It would be risky to rely on the information provided in e-Government websites.	①	②	③	④	⑤	⑥	⑦
52	ER8	Using e-Government websites to search and request government services could lead to an inefficient use of my time.	①	②	③	④	⑤	⑥	⑦
53	ESe1	I perceive e-Government service websites as secure to send sensitive information.	①	②	③	④	⑤	⑥	⑦
54	ESe2	I perceive the information (e.g. security information) relating to users of e-Government service as secure.	①	②	③	④	⑤	⑥	⑦
55	ESe3	The information I provided previously on e-Government service websites is helpful in secure transactions.	①	②	③	④	⑤	⑥	⑦
56	ESe4	I do not fear security incidents (e.g, hacker invasions) related to e-Government service websites.	①	②	③	④	⑤	⑥	⑦
57	ESe5	Overall, I would feel e-Government service websites are a safe place to transmit sensitive information.	①	②	③	④	⑤	⑥	⑦
58	Any other comments									

Table C2: Pilot Study Data Correlation

		Education	Experience	Country	ET1	ET2	ET3	ET4	ET5	ET6	ET7	ET8	ET9
Education	Pearson Correlation	1	.430	.012	.278	.145	.246	.280	.164	-.055	.121	.093	.129
	Sig. (2-tailed)		.003	.938	.061	.336	.100	.059	.276	.714	.425	.537	.394
	Sum of Squares and Cross-products	15.304	9.435	.609	8.087	4.435	7.217	9.478	7.565	-2.304	5.174	4.043	5.043
	Covariance	.340	.210	.014	.180	.099	.160	.211	.168	-.051	.115	.090	.112
Experience	Pearson Correlation	.430	1	-.069	.280	-.035	.255	.203	.068	.244	.136	.086	.362
	Sig. (2-tailed)	.003		.648	.059	.819	.087	.177	.652	.102	.367	.569	.013
	Sum of Squares and Cross-products	9.435	31.478	-5.130	11.696	-1.522	10.739	9.826	4.522	14.565	8.391	5.348	20.348
	Covariance	.210	.700	-.114	.260	-.034	.239	.218	.100	.324	.186	.119	.452
Country	Pearson Correlation	.012	-.069	1	-.248	-.248	-.142	-.228	-.073	-.157	-.139	.001	-.082
	Sig. (2-tailed)	.938	.648		.097	.096	.347	.127	.630	.296	.357	.997	.586
	Sum of Squares and Cross-products	.609	-5.130	174.717	-24.326	-25.630	-14.065	-26.043	-11.370	-22.109	-20.152	.087	-10.913
	Covariance	.014	-.114	3.883	-.541	-.570	-.313	-.579	-.253	-.491	-.448	.002	-.243
ET1	Pearson Correlation	.278	.280	-.248	1	.279	.481	.647	.420	.436	.478	.460	.388
	Sig. (2-tailed)	.061	.059	.097		.060	.001	.000	.004	.002	.001	.001	.008
	Sum of Squares and Cross-products	8.087	11.696	-24.326	55.239	16.196	26.848	41.565	36.804	34.413	38.978	37.870	28.870
	Covariance	.180	.260	-.541	1.228	.360	.597	.924	.818	.765	.866	.842	.642
ET2	Pearson Correlation	.145	-.035	-.248	.279	1	.209	.042	.098	.182	.057	.131	.183
	Sig. (2-tailed)	.336	.819	.096	.060		.164	.782	.517	.227	.706	.384	.223
	Sum of Squares and Cross-products	4.435	-1.522	-25.630	16.196	60.978	12.239	2.826	9.022	15.065	4.891	11.348	14.348
	Covariance	.099	-.034	-.570	.360	1.355	.272	.063	.200	.335	.109	.252	.319
ET3	Pearson Correlation	.246	.255	-.142	.481	.209	1	.554	.607	.342	.682	.688	.534
	Sig. (2-tailed)	.100	.087	.347	.001	.164		.000	.000	.020	.000	.000	.000
	Sum of Squares and Cross-products	7.217	10.739	-14.065	26.848	12.239	56.370	35.913	53.761	27.283	56.196	57.174	40.174
	Covariance	.160	.239	-.313	.597	.272	1.253	.798	1.195	.606	1.249	1.271	.893
ET4	Pearson Correlation	.280	.203	-.228	.647	.042	.554	1	.660	.605	.761	.605	.529
	Sig. (2-tailed)	.059	.177	.127	.000	.782	.000		.000	.000	.000	.000	.000
	Sum of Squares and Cross-products	9.478	9.826	-26.043	41.565	2.826	35.913	74.609	67.174	55.522	72.130	57.783	45.783

	Covariance	.211	.218	-.579	.924	.063	.798	1.658	1.493	1.234	1.603	1.284	1.017
ET5	Pearson Correlation	.164	.068	-.073	.420	.098	.607	.660	1	.367	.805	.764	.590
	Sig. (2-tailed)	.276	.652	.630	.004	.517	.000	.000		.012	.000	.000	.000
	Sum of Squares and Cross-products	7.565	4.522	-11.370	36.804	9.022	53.761	67.174	138.978	45.935	104.109	99.652	69.652
	Covariance	.168	.100	-.253	.818	.200	1.195	1.493	3.088	1.021	2.314	2.214	1.548
ET6	Pearson Correlation	-.055	.244	-.157	.436	.182	.342	.605	.367	1	.560	.408	.460
	Sig. (2-tailed)	.714	.102	.296	.002	.227	.020	.000	.012		.000	.005	.001
	Sum of Squares and Cross-products	-2.304	14.565	-22.109	34.413	15.065	27.283	55.522	45.935	112.804	65.326	47.957	48.957
	Covariance	-.051	.324	-.491	.765	.335	.606	1.234	1.021	2.507	1.452	1.066	1.088
ET7	Pearson Correlation	.121	.136	-.139	.478	.057	.682	.761	.805	.560	1	.755	.616
	Sig. (2-tailed)	.425	.367	.357	.001	.706	.000	.000	.000	.000		.000	.000
	Sum of Squares and Cross-products	5.174	8.391	-20.152	38.978	4.891	56.196	72.130	104.109	65.326	120.457	91.739	67.739
	Covariance	.115	.186	-.448	.866	.109	1.249	1.603	2.314	1.452	2.677	2.039	1.505
ET8	Pearson Correlation	.093	.086	.001	.460	.131	.688	.605	.764	.408	.755	1	.572
	Sig. (2-tailed)	.537	.569	.997	.001	.384	.000	.000	.000	.005	.000		.000
	Sum of Squares and Cross-products	4.043	5.348	.087	37.870	11.348	57.174	57.783	99.652	47.957	91.739	122.435	63.435
	Covariance	.090	.119	.002	.842	.252	1.271	1.284	2.214	1.066	2.039	2.721	1.410
ET9	Pearson Correlation	.129	.362	-.082	.388	.183	.534	.529	.590	.460	.616	.572	1
	Sig. (2-tailed)	.394	.013	.586	.008	.223	.000	.000	.000	.001	.000	.000	
	Sum of Squares and Cross-products	5.043	20.348	-10.913	28.870	14.348	40.174	45.783	69.652	48.957	67.739	63.435	100.435
	Covariance	.112	.452	-.243	.642	.319	.893	1.017	1.548	1.088	1.505	1.410	2.232

Table C3: Descriptive data Analysis (From Main Survey)

	N	Range	Minimum	Maximum	Sum	Mean		Std. Deviation	Variance	Skewness		Kurtosis	
	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
Q1	309	6	1	7	1531	4.95	.057	.999	.998	-.892	.139	1.967	.276
Q2	309	6	1	7	1545	5.00	.058	1.013	1.026	-1.151	.139	2.607	.276
Q3	309	6	1	7	1537	4.97	.059	1.035	1.071	-.762	.139	1.307	.276
Q4	309	6	1	7	1542	4.99	.062	1.089	1.185	-.847	.139	1.393	.276
Q5	309	6	1	7	1555	5.03	.057	1.006	1.012	-.604	.139	1.621	.276
Q6	309	6	1	7	1556	5.04	.057	1.011	1.021	-.888	.139	2.011	.276
Q7	309	6	1	7	1546	5.00	.058	1.021	1.042	-.799	.139	1.653	.276
Q8	309	6	1	7	1534	4.96	.056	.985	.970	-.832	.139	2.120	.276
Q9	309	6	1	7	1539	4.98	.058	1.025	1.052	-.961	.139	1.996	.276
Q10	309	6	1	7	1543	4.99	.057	1.006	1.013	-.776	.139	1.558	.276
Q11	309	5	2	7	1528	4.94	.054	.957	.916	-.762	.139	1.158	.276
Q12	309	6	1	7	1516	4.91	.059	1.029	1.059	-.908	.139	1.697	.276
Q13	309	6	1	7	1524	4.93	.056	.986	.973	-.926	.139	1.936	.276
Q14	309	6	1	7	1490	4.82	.061	1.071	1.147	-.965	.139	1.868	.276
Q15	309	6	1	7	1529	4.95	.057	1.002	1.004	-.832	.139	1.820	.276
Q16	309	6	1	7	1507	4.88	.059	1.031	1.063	-.807	.139	1.441	.276
Q17	309	6	1	7	1508	4.88	.055	.971	.943	-.849	.139	2.059	.276
Q18	309	6	1	7	1545	5.00	.055	.970	.942	-.858	.139	1.907	.276
Q19	309	6	1	7	1535	4.97	.053	.929	.863	-.694	.139	2.053	.276
Q21	309	6	1	7	1142	3.70	.070	1.237	1.531	.285	.139	.640	.276
Q22	309	6	1	7	1140	3.69	.071	1.251	1.566	.435	.139	.653	.276
Q23	309	6	1	7	1134	3.67	.072	1.269	1.611	.276	.139	.303	.276
Q24	309	6	1	7	1119	3.62	.069	1.218	1.483	.160	.139	.452	.276
Q25	309	6	1	7	1149	3.72	.072	1.259	1.586	.367	.139	.544	.276
Q26	309	6	1	7	1554	5.03	.056	.991	.983	-.884	.139	1.768	.276
Q27	309	6	1	7	1528	4.94	.058	1.023	1.046	-1.045	.139	2.245	.276
Q28	309	6	1	7	1528	4.94	.062	1.090	1.189	-.723	.139	1.014	.276
Q29	309	6	1	7	1509	4.88	.064	1.119	1.253	-.929	.139	1.513	.276
Q30	309	6	1	7	1531	4.95	.060	1.047	1.095	-.987	.139	1.725	.276
Q32	309	6	1	7	1512	4.89	.064	1.122	1.258	-.844	.139	1.022	.276
Q33	309	6	1	7	1538	4.98	.059	1.036	1.074	-.835	.139	1.424	.276
Q34	309	6	1	7	1528	4.94	.063	1.114	1.240	-.771	.139	.878	.276
Q35	309	6	1	7	1533	4.96	.062	1.098	1.206	-.826	.139	1.431	.276
Q36	309	6	1	7	1529	4.95	.059	1.043	1.088	-.950	.139	1.897	.276
Q37	309	6	1	7	1512	4.89	.064	1.119	1.252	-.754	.139	.565	.276
Q38	309	6	1	7	1523	4.93	.061	1.064	1.131	-.721	.139	1.099	.276
Q39	309	6	1	7	1102	3.57	.071	1.253	1.571	.247	.139	.322	.276
Q40	309	6	1	7	1055	3.41	.072	1.273	1.620	.393	.139	.228	.276

Q41	309	6	1	7	1074	3.48	.070	1.234	1.523	.296	.139	.063	.276
Q42	309	6	1	7	1070	3.46	.070	1.223	1.496	.247	.139	.112	.276
Q43	309	6	1	7	1096	3.55	.072	1.265	1.599	.243	.139	.005	.276
Q44	309	6	1	7	1043	3.38	.070	1.223	1.495	.324	.139	.035	.276
Q45	309	6	1	7	1056	3.42	.068	1.191	1.419	.342	.139	.371	.276
Q46	309	6	1	7	1071	3.47	.073	1.275	1.626	.275	.139	.059	.276
Q47	309	6	1	7	1526	4.94	.061	1.066	1.136	-.865	.139	1.683	.276
Q48	309	6	1	7	1528	4.94	.062	1.081	1.169	-1.054	.139	1.536	.276
Q49	309	6	1	7	1548	5.01	.062	1.083	1.172	-1.039	.139	1.812	.276
Q50	309	6	1	7	1490	4.82	.069	1.210	1.465	-1.136	.139	1.611	.276
Q51	309	6	1	7	1527	4.94	.060	1.058	1.120	-1.041	.139	2.067	.276
Valid N (listwise)	309												

Table C4: Maximum Percentage of Outliers

	EEOU	EU	HCI	Privacy	Quality	Technology	Trust	Risk	Security
1	57.315	38.302	33.310	48.083	28.048	65.423	45.932	45.222	41.735
2	32.300	34.425	29.555	46.355	25.509	55.866	43.954	44.118	39.812
3	30.395	32.416	26.685	42.375	24.761	51.164	43.573	36.289	38.903
4	29.444	32.400	26.147	33.356	22.584	46.794	42.505	35.541	37.944
5	24.776	28.405	26.147	25.721	22.331	46.575	41.828	33.314	36.756
6	24.280	28.071	25.984	22.215	19.631	36.433	40.541	32.767	36.118
7	22.787	27.075	24.539	21.597	19.584	36.066	38.932	32.210	33.092
8	21.056	24.993	18.278	20.558	19.109	33.057	36.416	30.746	32.465
9	20.009	21.051	18.222	20.541	18.910	31.801	36.196	29.411	27.430
10	18.761	19.683	17.642	19.163	18.344	31.485	33.394	29.201	26.955
11	18.562	19.683	16.391	17.652	16.896	29.403	32.256	27.928	24.898
12	17.222	19.528	16.231	17.068	16.896	29.030	29.247	26.106	20.665
13	16.832	19.097	15.723	16.203	16.122	28.799	27.317	25.061	19.343
14	16.318	18.983	15.469	15.609	16.041	28.059	26.843	24.605	19.327
15	15.119	17.628	14.882	15.138	15.849	26.835	26.576	23.280	18.711
16	14.908	16.927	14.882	14.393	15.829	26.201	25.895	23.122	18.414
17	14.811	16.506	14.795	14.240	15.609	26.188	23.733	22.404	17.756
18	14.429	16.194	13.133	13.818	14.492	26.121	23.601	22.282	17.470
19	14.055	15.339	12.168	12.101	14.454	24.958	21.680	22.010	17.292
20	13.595	15.058	11.560	11.836	13.938	24.415	21.348	20.986	16.449
21	13.413	14.463	11.492	11.418	13.711	22.713	21.006	20.706	15.618
22	12.925	13.060	11.463	11.250	13.566	22.551	20.239	20.397	14.284
23	12.865	12.478	10.514	11.171	12.237	22.469	20.239	20.276	13.824
24	11.835	12.330	10.136	11.073	11.974	22.188	20.110	19.797	13.758
25	11.253	11.407	9.666	10.953	11.721	21.754	19.963	19.435	13.491
26	11.148	10.989	9.568	10.801	11.631	21.713	19.710	19.142	13.433
27	11.148	10.989	8.835	10.782	11.513	21.605	19.087	18.993	13.425
28	11.077	10.989	8.576	10.631	11.197	21.356	18.861	18.855	13.038
29	10.910	10.989	7.576	10.555	10.610	20.503	18.758	18.826	12.277
30	10.905	10.589	7.576	10.528	10.569	20.230	18.693	18.543	12.264
31	10.835	10.339	7.266	10.498	10.503	20.165	18.412	18.103	11.856
32	10.656	9.027	7.266	10.275	10.503	20.135	18.282	17.984	11.744
33	10.656	9.027	7.186	10.000	10.503	19.538	17.998	17.683	11.744
34	10.656	8.647	6.505	9.721	10.222	19.112	17.870	17.518	10.613
35	10.656	8.620	6.505	9.286	10.222	18.950	17.521	17.186	10.436
.	.	.	.	.	.	.	.	.	.
309	0.006	0.011	0.032	0.099	0.028	0.061	0.020	0.266	0.033

Table C5: Squared Multiple Correlations**: (Group number 1 - Default model) (Original CFA) i.e: minimum is 0.4**	
	Estimate
ESe5	.713
ESe4	.564
ESe3	.588
ESe2	.708
ESe1	.646
ER1	.606
ER2	.629
ER3	.670
ER4	.667
ER5	.559
ER6	.664
ER7	.637
ER8	.478
ET9	.667
ET8	.639
ET7	.691
ET6	.681
ET5	.671
ET4	.744
ET3	.705
ET1	.719
EQ1	.663
EQ2	.747
EQ3	.734
EQ4	.669
EP4	.749
EP3	.819

Table C5: Squared Multiple Correlations**: (Group number 1 - Default model) (Original CFA) i.e: minimum is 0.4**	
	Estimate
EP2	.776
EP1	.725
EHCI1EWQ1	.764
EHCI2EWQ2	.714
EHCI3EWQ3	.692
EHCI4EWQ4	.715
EHCI5EWQ5	.775
EHCI6EWQ6	.649
EHCI7EWQ7	.727
EHCI8EWQ8	.697
EHCI11	.217
EHCI10	.667
EHCI9	.736
EU4	.754
EU3	.813
EU2	.723
EU1	.765
EEOU4	.628
EEOU1	.715
EEOU2	.759
EEOU3	.752

Table C6: Residual Covariances (Group number 1 - Default model)

	ESe5	ESe3	ESe2	ESe1	ER1	ER3	ER4	ER5	ER6	ER8	ET9	ET8	ET7	ET6	ET4	ET3	ET1	EQ1	EQ2	EQ3	EQ4	EP4	EP3	EP2	EP1	EHCI1EWQ1	EHCI2EWQ2	EHCI3EWQ3	EHCI4EWQ4	EHCI5EWQ5	EHCI6EWQ6	EHCI7EWQ7	EHCI8EWQ8	EHCI10	EHCI9
ESe5	0																																		
ESe3	0.013	0																																	
ESe2	-0.019	-0.011	0																																
ESe1	0.033	-0.042	0.016	0																															
ER1	0.033	0.155	0.008	0	0																														
ER3	-0.057	0.097	0.028	-0.013	0.05	0																													
ER4	-0.05	0.057	-0.061	-0.031	-0.047	-0.011	0																												
ER5	-0.023	0.107	0.01	0.019	0.011	-0.012	0.027	0																											
ER6	-0.103	0.1	-0.014	-0.049	-0.052	0.011	0.032	-0.029	0																										
ER8	-0.053	0.061	0.045	-0.005	0.02	-0.004	-0.002	0.002	0.005	0																									
ET9	-0.039	0.023	-0.021	-0.04	0.095	0.037	0.071	-0.002	0.007	0.039	0																								
ET8	-0.058	0.021	0.008	-0.026	0.029	0.052	0.04	0.002	-0.011	-0.041	0.131	0																							
ET7	0.019	0.066	0.033	0.024	0.05	0.02	-0.017	-0.043	-0.046	-0.075	0.012	-0.004	0																						
ET6	0.03	0.059	0.057	0.062	0.014	-0.015	-0.062	-0.018	-0.071	-0.105	-0.011	-0.072	0.009	0																					
ET4	-0.061	0.021	0.004	-0.036	0.03	0.006	-0.041	-0.018	-0.019	-0.096	0.005	0.008	0.014	0.016	0																				
ET3	-0.018	0.089	0.067	-0.014	0.062	0.008	0.018	0.019	-0.019	0.011	-0.011	-0.001	-0.06	0.005	-0.017	0																			
ET1	-0.062	0.019	-0.045	-0.034	0.036	0.054	0.033	-0.019	-0.008	-0.103	-0.044	-0.018	0.031	-0.009	0.035	-0.028	0																		
EQ1	-0.004	0.009	-0.018	-0.046	0.13	0.077	0.093	0.054	0.029	0.007	-0.007	-0.061	-0.019	-0.002	-0.004	-0.043	0.046	0																	
EQ2	0.01	0.084	0.024	-0.023	0.029	0.021	0	-0.032	-0.026	-0.1	-0.006	-0.035	-0.012	0.01	-0.004	0.034	0.039	0.039	0																
EQ3	-0.017	0.018	-0.014	-0.062	0.039	-0.027	0	0.045	-0.049	-0.085	-0.015	0.012	-0.034	0.022	0.001	0.03	-0.024	0.001	0.001	0															
EQ4	-0.022	0.058	0.047	-0.019	0.018	-0.066	-0.072	-0.009	-0.058	-0.03	-0.005	0.06	0.026	-0.04	-0.039	0.079	-0.018	-0.042	-0.026	0.013	0														
EP4	-0.057	0.049	-0.106	-0.048	0.135	0.016	0.077	0.082	0.04	0.025	0.062	0.029	-0.036	-0.093	-0.068	0.011	-0.007	0.074	-0.033	-0.026	-0.116	0													
EP3	0.002	0.042	0.034	0.014	0.05	-0.031	-0.028	-0.027	0.018	0.005	0.011	-0.023	0.042	-0.028	-0.024	0.031	-0.003	0.109	-0.005	-0.026	-0.042	-0.021	0												
EP2	-0.016	0.048	0.015	-0.03	0.03	-0.106	-0.031	-0.005	0.029	-0.106	0.003	-0.021	0.033	-0.015	-0.007	0.032	0.02	0.097	-0.013	0.011	-0.066	-0.013	0.022	0											
EP1	-0.001	0.045	0.027	0.015	0.064	-0.12	-0.042	-0.001	0.015	-0.062	0.019	0.008	0.026	-0.016	-0.011	0.025	0.026	0.121	-0.006	0.004	-0.084	0.013	0.004	-0.006	0										
EHCI1EWQ1	0.018	0.026	0.028	-0.015	0.044	0.021	-0.036	-0.007	-0.043	-0.069	-0.002	-0.025	0.026	0.015	-0.035	0.005	-0.002	0.025	-0.029	0.001	0.008	-0.063	0.009	-0.018	0.023	0									
EHCI2EWQ2	-0.033	0.057	0.046	-0.063	0.075	0.023	0.018	-0.034	-0.017	-0.073	-0.069	-0.049	0.023	0.065	0.001	0.077	0.012	0.017	-0.01	0.022	0.032	-0.002	0.104	0.094	0.06	0.012	0							
EHCI3EWQ3	-0.045	0.032	-0.004	-0.022	0.018	0.068	0.024	0.04	-0.012	-0.046	-0.008	0.051	0.063	-0.023	0.037	0.004	0.037	0.018	0.042	0.016	0.035	-0.049	0.01	0.007	0.02	0.034	-0.011	0						
EHCI4EWQ4	-0.025	0.052	0.012	-0.052	0.031	0.017	-0.069	-0.005	-0.031	-0.028	-0.012	-0.031	0.005	0.027	-0.041	0.058	-0.033	-0.014	-0.001	-0.003	0.006	-0.016	0.069	0.028	0.001	-0.009	0.012	-0.014	0					
EHCI5EWQ5	-0.014	0.064	0.013	-0.044	0.087	0.043	0.044	0.025	-0.006	-0.093	-0.004	-0.057	0.028	0.028	-0.057	0.01	-0.002	0.028	0.019	0.002	-0.043	0.012	0.083	0.083	0.053	-0.018	0.022	0.026	-0.013	0				
EHCI6EWQ6	0.011	0.068	0.032	-0.039	0.04	0.035	-0.05	-0.056	-0.09	-0.073	0	0.043	0.019	0.019	-0.044	0.039	0.001	-0.019	-0.04	-0.028	0.014	-0.07	-0.048	-0.059	-0.105	-0.009	-0.042	-0.032	0.059	-0.017	0			
EHCI7EWQ7	-0.063	0.056	0.006	-0.087	0.041	0.05	0.009	0.047	-0.014	-0.076	-0.033	-0.049	-0.036	0.009	-0.015	0.047	0.017	0.004	-0.025	0.003	0.03	-0.068	-0.043	-0.008	-0.086	-0.034	0.012	0.011	-0.034	0.016	-0.001	0		
EHCI8EWQ8	-0.015	0.09	0.035	-0.016	0.044	0.043	-0.037	-0.041	-0.053	-0.086	0.017	-0.009	-0.04	0.054	-0.056	0.022	-0.019	-0.056	-0.056	0.001	0.018	-0.066	-0.035	-0.06	-0.07	0.015	-0.032	-0.042	0	0	0.053	0.034	0	
EHCI10	0.022	-0.002	-0.009	-0.033	0.127	0.101	-0.013	0.009	-0.005	-0.086	0.023	-0.074	-0.009	0.066	-0.017	-0.04	0.015	0.074	-0.008	-0.008	-0.065	0.047	0.079	0.103	0.102	0.02	-0.001	-0.052	0.015	0.008	-0.022	-0.022	0.016	0
EHCI9	-0.007	0.01	0.01	-0.002	0.041	0.036	-0.054	-0.029	-0.043	-0.059	-0.039	-0.063	-0.006	0.042	0.009	0.016	0.037	0.022	0.012	-0.008	-0.025	-0.055	-0.034	-0.031	-0.075	0.008	-0.009	-0.026	0.033	-0.015	0.025	0.012	-0.004	0	0

Table C7: Standardized Residual Covariances (Group number 1 - Default model)

	ESe5	ESe3	ESe2	ESe1	ER1	ER3	ER4	ER5	ER6	ER8	ET9	ET8	ET7	ET6	ET4	ET3	ET1	EQ1	EQ2	EQ3	EQ4	EP4	EP3	EP2	EP1	EHCI1EWQ1	EHCI2EWQ2	EHCI3EWQ3	EHCI4EWQ4	EHCI5EWQ5	EHCI6EWQ6	EHCI7EWQ7	EHCI8EWQ8	EHCI10	EHCI9
ESe5	0																																		
ESe3	0.162	0																																	
ESe2	-0.241	-0.137	0																																
ESe1	0.425	-0.544	0.202	0																															
ER1	0.426	1.991	0.099	0.002	0																														
ER3	-0.763	1.257	0.368	-0.169	0.483	0																													
ER4	-0.668	0.743	-0.804	-0.414	-0.453	-0.109	0																												
ER5	-0.302	1.366	0.131	0.244	0.106	-0.113	0.262	0																											
ER6	-1.384	1.315	-0.183	-0.653	-0.511	0.11	0.314	-0.283	0																										
ER8	-0.691	0.77	0.566	-0.058	0.197	-0.036	-0.018	0.018	0.051	0																									
ET9	-0.529	0.317	-0.286	-0.55	1.247	0.492	0.949	-0.029	0.099	0.501	0																								
ET8	-0.756	0.268	0.102	-0.345	0.359	0.656	0.507	0.024	-0.136	-0.506	1.617	0																							
ET7	0.264	0.921	0.452	0.334	0.675	0.272	-0.236	-0.572	-0.636	-0.986	0.161	-0.046	0																						
ET6	0.401	0.78	0.74	0.826	0.174	-0.198	-0.809	-0.231	-0.924	-1.307	-0.135	-0.868	0.114	0																					
ET4	-0.851	0.292	0.054	-0.502	0.405	0.079	-0.562	-0.237	-0.263	-1.273	0.062	0.105	0.19	0.198	0																				
ET3	-0.229	1.142	0.848	-0.182	0.773	0.099	0.234	0.235	-0.243	-0.135	0.129	0.013	-0.748	0.061	-0.214	0																			
ET1	-0.855	0.255	-0.608	-0.466	0.473	0.736	0.456	0.254	-0.113	-1.346	-0.569	-0.226	0.407	-0.118	0.455	-0.338	0																		
EQ1	-0.056	0.137	-0.266	-0.673	1.827	1.101	1.336	0.754	0.412	0.096	-0.102	-0.812	-0.265	-0.022	-0.057	-0.571	0.648	0																	
EQ2	0.143	1.185	0.333	-0.328	0.397	0.292	0	-0.437	-0.368	-1.344	-0.076	-0.444	-0.158	-0.131	-0.049	-0.425	-0.515	-0.56	0																
EQ3	-0.227	0.232	-0.175	-0.821	0.498	-0.349	-0.006	-0.575	-0.638	-1.067	-0.192	-0.146	-0.431	-0.26	-0.016	-0.355	-0.299	-0.008	-0.012	0															
EQ4	-0.283	0.756	-0.6	-0.245	0.228	-0.838	-0.919	-0.109	-0.747	-0.372	-0.059	-0.708	-0.328	-0.472	-0.49	-0.917	-0.219	-0.556	-0.324	-0.156	0														
EP4	-0.756	0.642	-1.384	-0.629	1.424	-0.171	-0.823	-0.858	-0.432	-0.262	-0.083	-0.367	-0.49	-1.209	-0.934	-0.138	-0.093	-1.068	-0.459	-0.338	-1.476	0													
EP3	-0.03	-0.522	-0.423	-0.177	-0.505	-0.316	-0.281	-0.27	-0.187	-0.053	-0.143	-0.281	-0.543	-0.354	-0.31	-0.38	-0.046	-1.509	-0.066	-0.323	-0.512	-0.185	0												
EP2	-0.21	-0.615	-0.189	-0.38	-0.311	-1.09	-0.32	-0.05	-0.299	-1.08	-0.034	-0.26	-0.434	-0.19	-0.1	-0.399	-0.259	-1.36	-0.17	-0.136	-0.81	-0.11	-0.188	0											

	2			7		4	6			3		6		3					9		3	9														
EP1	-0.008	0.582	0.35	0.201	0.662	-1.253	-0.44	-0.012	0.163	-0.642	0.248	0.097	0.353	-0.202	-0.152	0.317	0.344	1.71	-0.084	0.054	-1.059	0.125	0.031	-0.058	0										
EHCI1EWQ1	0.245	0.357	0.383	-0.213	0.604	0.287	-0.494	-0.09	0.594	-0.928	-0.029	-0.326	0.363	0.195	-0.486	0.066	-0.032	0.357	-0.402	0.009	0.098	-0.87	0.123	-0.238	0.309	0									
EHCI2EWQ2	-0.468	0.809	0.646	-0.911	1.035	0.321	0.262	-0.471	0.236	-0.991	0.971	-0.655	0.329	0.875	0.017	1.011	0.165	0.252	-0.146	0.289	0.42	-0.027	1.407	1.284	0.835	0.17	0								
EHCI3EWQ3	-0.676	0.488	-0.061	-0.336	0.257	1.001	0.357	0.585	-0.179	-0.665	-0.117	0.718	0.94	-0.33	0.555	0.053	0.544	0.277	0.625	0.219	0.48	-0.723	0.139	0.105	0.294	0.489	-0.162	0							
EHCI4EWQ4	-0.347	0.727	0.163	-0.729	0.424	0.233	-0.963	-0.068	-0.435	-0.376	-0.165	-0.403	0.064	0.359	-0.57	0.752	-0.448	-0.197	-0.02	-0.035	0.074	-0.216	0.916	0.374	0.015	-0.122	0.162	-0.202	0						
EHCI5EWQ5	-0.202	0.928	0.185	-0.643	1.23	0.612	0.636	0.354	-0.09	-1.289	0.055	-0.772	0.408	0.384	-0.81	0.126	-0.034	0.41	0.276	0.03	-0.562	0.178	1.144	1.163	0.752	-0.249	0.31	0.398	-0.183	0					
EHCI6EWQ6	0.153	0.922	0.427	-0.526	0.526	0.457	-0.662	-0.722	-1.202	-0.934	0.003	0.548	0.251	0.25	-0.594	0.482	0.016	-0.263	-0.532	0.352	0.176	-0.925	0.616	-0.765	-1.371	-0.114	-0.564	-0.463	0.779	-0.229	0				
EHCI7EWQ7	-0.896	0.804	0.091	-1.246	0.569	0.701	0.131	0.654	-0.196	-1.036	-0.455	-0.662	-0.513	0.12	-0.211	0.614	0.242	0.054	-0.354	0.044	0.397	-0.958	-0.585	-0.107	-1.204	-0.463	0.169	0.158	-0.474	0.225	-0.014	0			
EHCI8EWQ8	-0.209	1.252	0.478	-0.229	0.596	0.593	-0.513	-0.555	-0.738	-1.148	-0.232	-0.12	-0.557	0.713	-0.773	0.281	-0.261	-0.811	-0.769	-0.015	0.225	-0.911	-0.459	-0.797	-0.948	0.206	-0.438	-0.622	-0.002	0	0.698	0.475	0		
EHCI10	0.326	-0.026	-0.13	-0.494	1.832	1.474	-0.194	0.128	-0.079	-1.21	-0.34	-1.053	-0.13	0.955	-0.261	-0.567	0.233	1.178	-0.125	-0.118	-0.908	0.685	1.115	1.148	1.473	0.298	-0.021	-0.837	0.217	0.12	-0.318	-0.338	0.245	0	
EHCI9	-0.105	0.15	0.145	-0.027	0.582	0.529	-0.787	-0.406	-0.639	-0.838	-0.567	-0.885	-0.087	0.594	-0.139	-0.219	0.536	0.347	-0.174	-0.114	-0.346	-0.807	-0.485	-0.447	-1.086	0.108	-0.139	-0.412	0.48	-0.228	0.355	0.177	-0.053	0	0

Table C8: Sample Correlation

	ESe5	ESe3	ESe2	ESe1	ER1	ER3	ER4	ER5	ER6	ER8	ET9	ET8	ET7	ET6	ET4	ET3	ET1	EQ1	EQ2	EQ3	EQ4	EP4	EP3	EP2	EP1	EHCI1EWQ1	EHCI2EWQ2	EHCI3EWQ3	EHCI4EWQ4	EHCI5EWQ5	EHCI6EWQ6	EHCI7EWQ7	EHCI8EWQ8	EHCI10	EHCI9	EU4	EU3	EU1	EEOU4	EEOU1	EEOU2	EEOU3
ESe5	1																																									
ESe3	0.664	1																																								
ESe2	0.692	0.638	1																																							
ESe1	0.711	0.586	0.69	1																																						
ER1	-0.134	-0.03	-0.152	-0.151	1																																					
ER3	-0.212	-0.081	-0.146	-0.17	0.661	1																																				
ER4	-0.207	-0.111	-0.214	-0.185	0.599	0.66	1																																			
ER5	-0.173	-0.063	-0.147	-0.134	0.586	0.607	0.633	1																																		
ER6	-0.247	-0.076	-0.176	-0.197	0.587	0.667	0.682	0.589	1																																	
ER8	-0.182	-0.086	-0.108	-0.139	0.543	0.56	0.563	0.52	0.56	1																																
ET9	0.521	0.528	0.533	0.495	-0.043	-0.093	-0.067	-0.113	-0.114	-0.074	1																															
ET8	0.494	0.513	0.545	0.496	-0.091	-0.081	-0.09	-0.108	-0.125	-0.129	0.766	1																														
ET7	0.58	0.573	0.588	0.558	-0.077	-0.107	-0.136	-0.146	-0.158	-0.16	0.69	0.66	1																													
ET6	0.582	0.557	0.6	0.583	-0.104	-0.132	-0.168	-0.125	-0.173	-0.177	0.662	0.596	0.687	1																												
ET4	0.532	0.556	0.587	0.528	-0.098	-0.124	-0.161	-0.132	-0.142	-0.181	0.714	0.701	0.732	0.724	1																											
ET3	0.553	0.592	0.619	0.53	-0.072	-0.118	-0.111	-0.101	-0.136	-0.097	0.677	0.669	0.642	0.69	0.71	1																										
ET1	0.522	0.545	0.534	0.521	-0.092	-0.084	-0.1	-0.131	-0.131	-0.184	0.659	0.667	0.735	0.69	0.771	0.69	1																									
EQ1	0.546	0.511	0.529	0.481	-0.008	-0.056	-0.043	-0.067	-0.095	-0.096	0.652	0.588	0.648	0.657	0.693	0.633	0.73	1																								
EQ2	0.594	0.611	0.602	0.536	-0.097	-0.11	-0.128	-0.142	-0.147	-0.184	0.695	0.653	0.697	0.709	0.737	0.745	0.765	0.738	1																							
EQ3	0.568	0.548	0.568	0.503	-0.091	-0.147	-0.127	-0.084	-0.162	-0.168	0.685	0.693	0.677	0.717	0.74	0.739	0.706	0.698	0.743	1																						
EQ4	0.537	0.556	0.59	0.514	-0.101	-0.169	-0.174	-0.118	-0.162	-0.123	0.661	0.698	0.696	0.633	0.669	0.743	0.677	0.626	0.684	0.716	1																					
EP4	-0.282	-0.179	-0.317	-0.263	0.534	0.483	0.526	0.489	0.495	0.415	-0.126	-0.149	-0.205	-0.244	-0.238	-0.17	-0.187	-0.098	-0.197	-0.189	-0.247	1																				
EP3	-0.246	-0.196	-0.221	-0.226	0.497	0.474	0.477	0.438	0.501	0.42	-0.174	-0.194	-0.153	-0.203	-0.211	-0.164	-0.192	-0.08	-0.182	-0.196	-0.199	0.77	1																			
EP2	-0.254	-0.185	-0.229	-0.253	0.473	0.411	0.461	0.44	0.495	0.339	-0.175	-0.188	-0.154	-0.188	-0.193	-0.158	-0.169	-0.084	-0.183	-0.165	-0.211	0.754	0.81	1																		
EP1	-0.234	-0.18	-0.212	-0.211	0.48	0.386	0.439	0.428	0.471	0.354	-0.157	-0.162	-0.153	-0.183	-0.19	-0.157	-0.159	-0.059	-0.172	-0.164	-0.22	0.747	0.773	0.746	1																	
EHCI1EWQ1	0.612	0.568	0.617	0.554	-0.095	-0.121	-0.166	-0.132	-0.17	-0.169	0.636	0.601	0.67	0.651	0.641	0.656	0.662	0.694	0.683	0.711	0.683	-0.256	-0.207	-0.222	-0.184	1																
EHCI2EWQ2	0.548	0.581	0.617	0.493	-0.067	-0.115	-0.119	-0.15	-0.146	-0.17	0.555	0.562	0.649	0.678	0.657	0.701	0.656	0.667	0.681	0.71	0.685	-0.201	-0.126	-0.128	-0.148	0.742	1															
EHCI3EWQ3	0.526	0.552	0.562	0.522	-0.109	-0.074	-0.111	-0.088	-0.14	-0.149	0.602	0.643	0.68	0.588	0.683	0.627	0.672	0.659	0.724	0.694	0.679	-0.238	-0.197	-0.193	-0.176	0.753	0.687	1														
EHCI4EWQ4	0.558	0.578	0.588	0.507	-0.102	-0.121	-0.19	-0.128	-0.158	-0.135	0.611	0.581	0.634	0.646	0.619	0.686	0.617	0.639	0.692	0.69	0.664	-0.212	-0.155	-0.182	-0.196	0.724	0.723	0.687	1													
EHCI5EWQ5	0.59	0.612	0.612	0.533	-0.061	-0.104	-0.103	-0.108	-0.143	-0.192	0.642	0.579	0.681	0.672	0.627	0.668	0.67	0.706	0.74	0.721	0.646	-0.197	-0.15	-0.143	-0.161	0.743	0.762	0.756	0.729	1												
EHCI6EWQ6	0.57	0.57	0.583	0.5	-0.092	-0.103	-0.167	-0.16	-0.197	-0.163	0.599	0.621	0.622	0.615	0.593	0.644	0.624	0.61	0.631	0.642	0.646	-0.246	-0.237	-0.24	-0.269	0.698	0.647	0.643	0.742	0.699	1											
EHCI7EWQ7	0.53	0.59	0.591	0.48	-0.096	-0.096	-0.129	-0.088	-0.146	-0.174	0.6	0.571	0.603	0.638	0.652	0.686	0.673	0.665	0.679	0.705	0.695	-0.258	-0.246	-0.212	-0.269	0.71	0.734	0.722	0.691	0.769	0.696	1										
EHCI8EWQ8	0.565	0.609	0.606	0.537	-0.092	-0.099	-0.163	-0.155	-0.174	-0.179	0.635	0.597	0.589	0.667	0.602	0.651	0.627	0.594	0.637	0.69	0.671	-0.252	-0.235	-0.249	-0.251	0.744	0.678	0.655	0.711	0.739	0.733	0.755	1									

EHCI10	0.585	0.513	0.551	0.505	-0.008	-0.035	-0.131	-0.103	-0.123	-0.171	0.569	0.467	0.545	0.609	0.562	0.522	0.585	0.655	0.605	0.605	0.523
EHCI9	0.612	0.575	0.624	0.589	-0.091	-0.101	-0.177	-0.145	-0.167	-0.159	0.564	0.529	0.603	0.641	0.646	0.629	0.662	0.658	0.686	0.665	0.617
EU4	0.537	0.542	0.614	0.521	-0.081	-0.104	-0.156	-0.123	-0.132	-0.155	0.608	0.589	0.605	0.638	0.686	0.684	0.666	0.7	0.736	0.7	0.668
EU3	0.529	0.546	0.556	0.505	-0.042	-0.068	-0.087	-0.122	-0.1	-0.158	0.595	0.515	0.622	0.634	0.614	0.604	0.644	0.696	0.697	0.665	0.591
EU1	0.493	0.521	0.533	0.468	-0.009	-0.002	-0.062	-0.083	-0.052	-0.164	0.542	0.485	0.614	0.609	0.586	0.567	0.655	0.699	0.677	0.614	0.557
EEOU4	0.512	0.559	0.571	0.537	-0.132	-0.163	-0.219	-0.116	-0.2	-0.163	0.487	0.487	0.554	0.6	0.555	0.582	0.572	0.575	0.63	0.623	0.588
EEOU1	0.547	0.571	0.605	0.592	-0.06	-0.09	-0.179	-0.124	-0.153	-0.139	0.562	0.463	0.646	0.655	0.589	0.567	0.613	0.621	0.624	0.597	0.582
EEOU2	0.6	0.586	0.643	0.568	-0.069	-0.114	-0.194	-0.162	-0.186	-0.133	0.582	0.547	0.621	0.642	0.594	0.572	0.613	0.65	0.661	0.626	0.596
EEOU3	0.633	0.606	0.605	0.567	-0.116	-0.14	-0.167	-0.195	-0.177	-0.188	0.6	0.55	0.612	0.636	0.581	0.585	0.602	0.643	0.671	0.652	0.62

EHCI10	-0.115	-0.098	-0.072	-0.068	0.679	0.638	0.573	0.657	0.675	0.597	0.628	0.656	1								
EHCI9	-0.217	-0.206	-0.199	-0.23	0.731	0.693	0.664	0.739	0.717	0.704	0.728	0.699	0.71	1							
EU4	-0.185	-0.145	-0.186	-0.169	0.742	0.773	0.718	0.734	0.736	0.631	0.739	0.715	0.666	0.719	1						
EU3	-0.205	-0.149	-0.177	-0.135	0.732	0.727	0.728	0.73	0.774	0.606	0.695	0.685	0.678	0.672	0.779	1					
EU1	-0.149	-0.119	-0.144	-0.102	0.677	0.686	0.626	0.655	0.703	0.554	0.678	0.58	0.692	0.685	0.719	0.809	1				
EEOU4	-0.287	-0.216	-0.253	-0.265	0.651	0.661	0.604	0.712	0.659	0.639	0.672	0.673	0.563	0.656	0.712	0.649	0.638	1			
EEOU1	-0.204	-0.142	-0.172	-0.124	0.712	0.629	0.632	0.697	0.702	0.633	0.627	0.616	0.683	0.684	0.652	0.701	0.709	0.689	1		
EEOU2	-0.247	-0.199	-0.223	-0.184	0.769	0.659	0.663	0.651	0.705	0.667	0.643	0.641	0.654	0.733	0.684	0.688	0.701	0.66	0.757	1	
EEOU3	-0.255	-0.234	-0.234	-0.222	0.789	0.658	0.71	0.693	0.714	0.673	0.647	0.676	0.663	0.698	0.668	0.725	0.703	0.651	0.715	0.784	1

Table C9: Variance Extracted (Variable and Items code)

Variable& Items code	Std. loadin	(Std. loadin)²	(Σ Std. loadin)²	Σ (Std. loadin)²	Std. Error	Σ Std. Error	Constrc Relbty A/A+B	Varianc Extrctd C/C+B
Variable & Items code	Standard loading	(Standard Loading)^2	(Σ Standard loading) (A)	Σ (Standard loading)² (C)	Standard Error	Σ Standard Error (B)	Construct Reliability A/A+B	Variance extracted C/C+B
EEOU3	.868	0.753424			.026			
EEOU2	.871	0.758641			.025			
EEOU1	.845	0.714025			.027			
EEOU4	.793	0.628849			.039			
EU1	.859	0.737881			.027			
EU3	.899	0.808201			.023			
EU4	.876	0.767376			.023			
EHCI9	.873	0.762129			.028			
EHCI10	.813	0.660969			.031			
EHCI8EWQ8	.835	0.697225			.028			
EHCI7EWQ7	.852	0.725904			.024			
EHCI6EWQ6	.805	0.648025			.034			
EHCI5EWQ5	.880	0.7744			.020			
EHCI4EWQ4	.847	0.717409			.026			
EHCI3EWQ3	.832	0.692224			.024			
EHCI2EWQ2	.845	0.714025			.025			
EHCI1EWQ1	.874	0.763876			.022			
EP1	.852	0.725904			.042			
EP2	.881	0.776161			.038			
EP3	.904	0.817216			.035			
EP4	.866	0.749956			.039			
EQ4	.814	0.662596			.036			
EQ3	.857	0.734449			.028			
EQ2	.866	0.749956			.024			
EQ1	.817	0.667489			.028			
ET1	.853	0.727609			.027			

ET3	.837	0.700569			.034			
ET4	.867	0.751689			.025			
ET6	.819	0.670761			.035			
ET7	.828	0.685584			.030			
ET8	.801	0.641601			.039			
ET9	.819	0.670761			.033			
ER8	.688	0.473344			.075			
ER6	.809	0.654481			.051			
ER5	.752	0.565504			.064			
ER4	.819	0.670761			.050			
ER3	.816	0.665856			.051			
ER1	.769	0.591361			.060			
ESe1	.808	0.652864			.039			
ESe2	.838	0.702244			.036			
ESe3	.774	0.599076			.044			
ESe5	.843	0.710649			.034			
Total	A=35.064	C=29.343	1229.484	29.343	B= 1.449	1.449	0.9988	0.953

Note: The readings for computing A were extracted from Table **Standardized Regression Weights: (Group number 1 - Default model)** for Figure 5.2 reported by AMOS. Similarly readings for computing C were extracted from the Table **Squared Multiple Correlations: (Group number 1 - Default model)** for Figure 5.2 reported by

Table C10: Sample Correlation for SEM1.0

	ET9	ESe5	ESe3	ESe1	ESe2	ER8	ER6	ER5	ER4	ER3	ER1	ET1	ET3	ET4	ET6	ET7	ET8	EHCI8EWQ8	EHCI7EWQ7	EHCI6EWQ6	EHCI5EWQ5	EHCI4EWQ4	EHCI3EWQ3	EHCI2EWQ2	EHCI1EWQ1
ET9	1																								
ESe5	0.521	1																							
ESe3	0.528	0.664	1																						
ESe1	0.495	0.711	0.586	1																					
ESe2	0.533	0.692	0.638	0.69	1																				
ER8	-0.074	-0.182	-0.086	-0.139	-0.108	1																			
ER6	-0.114	-0.247	-0.076	-0.197	-0.176	0.56	1																		
ER5	-0.113	-0.173	-0.063	-0.134	-0.147	0.52	0.589	1																	
ER4	-0.067	-0.207	-0.111	-0.185	-0.214	0.563	0.682	0.633	1																
ER3	-0.093	-0.212	-0.081	-0.17	-0.146	0.56	0.667	0.607	0.66	1															
ER1	-0.043	-0.134	-0.03	-0.151	-0.152	0.543	0.587	0.586	0.599	0.661	1														
ET1	0.659	0.522	0.545	0.521	0.534	-0.184	-0.131	-0.131	-0.1	-0.084	-0.092	1													
ET3	0.677	0.553	0.592	0.53	0.619	-0.097	-0.136	-0.101	-0.111	-0.118	-0.072	0.69	1												
ET4	0.714	0.532	0.556	0.528	0.587	-0.181	-0.142	-0.132	-0.161	-0.124	-0.098	0.771	0.71	1											
ET6	0.662	0.582	0.557	0.583	0.6	-0.177	-0.173	-0.125	-0.168	-0.132	-0.104	0.69	0.69	0.724	1										
ET7	0.69	0.58	0.573	0.558	0.588	-0.16	-0.158	-0.146	-0.136	-0.107	-0.077	0.735	0.642	0.732	0.687	1									
ET8	0.766	0.494	0.513	0.496	0.545	-0.129	-0.125	-0.108	-0.09	-0.081	-0.091	0.667	0.669	0.701	0.596	0.66	1								
EHCI8EWQ8	0.635	0.565	0.609	0.537	0.606	-0.179	-0.174	-0.155	-0.163	-0.099	-0.092	0.627	0.651	0.602	0.667	0.589	0.597	1							
EHCI7EWQ7	0.6	0.53	0.59	0.48	0.591	-0.174	-0.146	-0.088	-0.129	-0.096	-0.096	0.673	0.686	0.652	0.638	0.603	0.571	0.76	1						
EHCI6EWQ6	0.599	0.57	0.57	0.5	0.583	-0.163	-0.197	-0.16	-0.167	-0.103	-0.092	0.624	0.644	0.593	0.615	0.622	0.621	0.73	0.7	1					
EHCI5EWQ5	0.642	0.59	0.612	0.533	0.612	-0.192	-0.143	-0.108	-0.103	-0.104	-0.061	0.67	0.668	0.627	0.672	0.681	0.579	0.74	0.77	0.7	1				
EHCI4EWQ4	0.611	0.558	0.578	0.507	0.588	-0.135	-0.158	-0.128	-0.19	-0.121	-0.102	0.617	0.686	0.619	0.646	0.634	0.581	0.71	0.69	0.74	0.73	1			
EHCI3EWQ3	0.602	0.526	0.552	0.522	0.562	-0.149	-0.14	-0.088	-0.111	-0.074	-0.109	0.672	0.627	0.683	0.588	0.68	0.643	0.66	0.72	0.64	0.76	0.69	1		
EHCI2EWQ2	0.555	0.548	0.581	0.493	0.617	-0.17	-0.146	-0.15	-0.119	-0.115	-0.067	0.656	0.701	0.657	0.678	0.649	0.562	0.68	0.73	0.65	0.76	0.72	0.69	1	
EHCI1EWQ1	0.636	0.612	0.568	0.554	0.617	-0.169	-0.17	-0.132	-0.166	-0.121	-0.095	0.662	0.656	0.641	0.651	0.67	0.601	0.74	0.71	0.7	0.74	0.72	0.75	0.74	1

Figure C1: SEM1

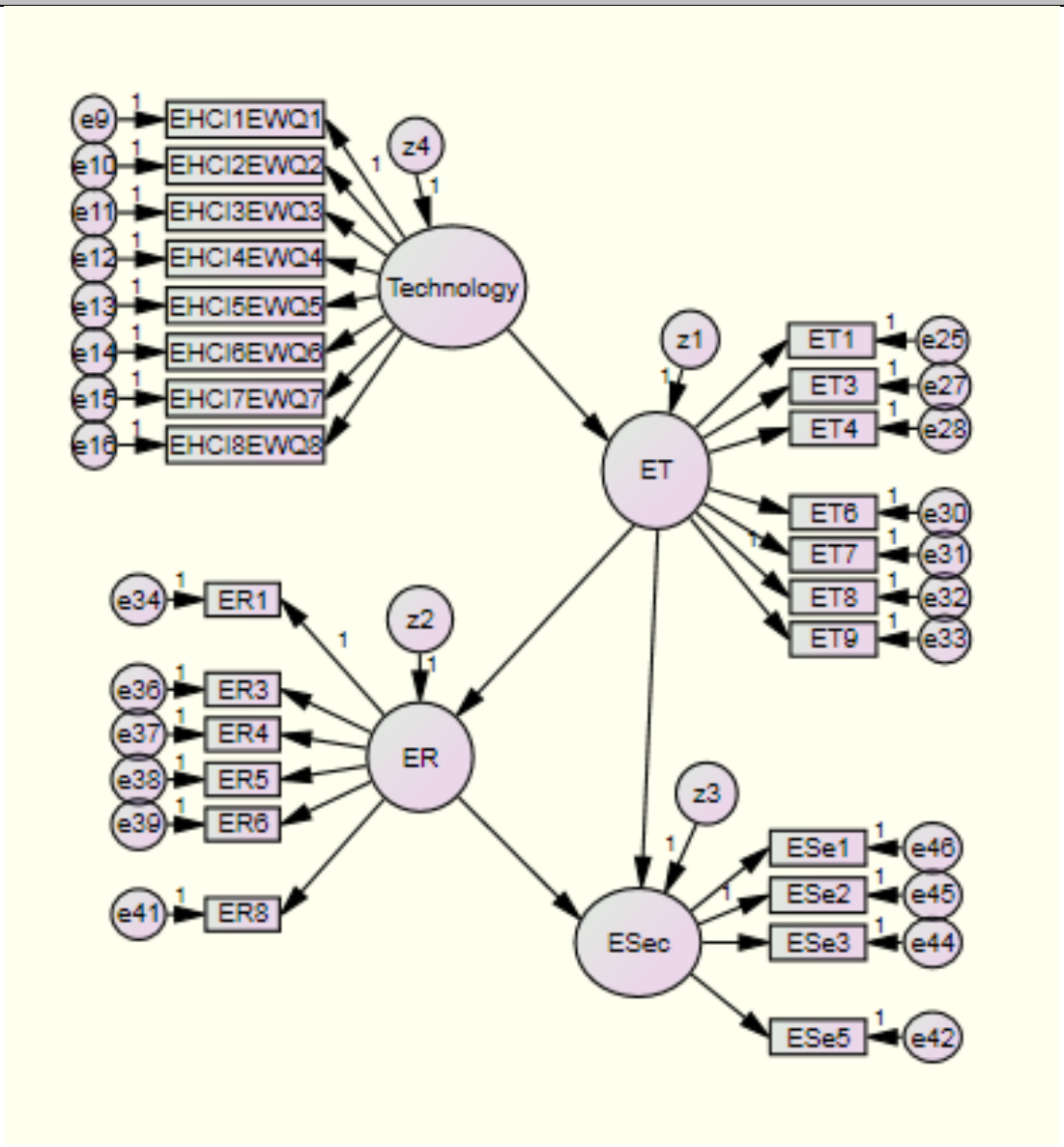

Table C11: Sample Correlations – Estimates for SEM1.1

	ET9	ESe5	ESe3	ESe1	ESe2	ER8	ER6	ER5	ER4	ER3	ER1	ET1	ET3	ET4	ET6	ET7	ET8	EHCI8EWQ8	EHCI7EWQ7	EHCI6EWQ6	EHCI5EWQ5	EHCI4EWQ4	EHCI3EWQ3	EHCI2EWQ2	EHCI1EWQ1
ET9	1																								
ESe5	0.521	1																							
ESe3	0.528	0.664	1																						
ESe1	0.495	0.711	0.586	1																					
ESe2	0.533	0.692	0.638	0.69	1																				
ER8	-0.074	-0.182	-0.086	-0.139	-0.108	1																			
ER6	-0.114	-0.247	-0.076	-0.197	-0.176	0.56	1																		
ER5	-0.113	-0.173	-0.063	-0.134	-0.147	0.52	0.589	1																	
ER4	-0.067	-0.207	-0.111	-0.185	-0.214	0.563	0.682	0.633	1																
ER3	-0.093	-0.212	-0.081	-0.17	-0.146	0.56	0.667	0.607	0.66	1															
ER1	-0.043	-0.134	-0.03	-0.151	-0.152	0.543	0.587	0.586	0.599	0.661	1														
ET1	0.659	0.522	0.545	0.521	0.534	-0.184	-0.131	-0.131	-0.1	-0.084	-0.092	1													
ET3	0.677	0.553	0.592	0.53	0.619	-0.097	-0.136	-0.101	-0.111	-0.118	-0.072	0.69	1												
ET4	0.714	0.532	0.556	0.528	0.587	-0.181	-0.142	-0.132	-0.161	-0.124	-0.098	0.771	0.71	1											
ET6	0.662	0.582	0.557	0.583	0.6	-0.177	-0.173	-0.125	-0.168	-0.132	-0.104	0.69	0.69	0.724	1										
ET7	0.69	0.58	0.573	0.558	0.588	-0.16	-0.158	-0.146	-0.136	-0.107	-0.077	0.735	0.642	0.732	0.687	1									
ET8	0.766	0.494	0.513	0.496	0.545	-0.129	-0.125	-0.108	-0.09	-0.081	-0.091	0.667	0.669	0.701	0.596	0.66	1								
EHCI8EWQ8	0.635	0.565	0.609	0.537	0.606	-0.179	-0.174	-0.155	-0.163	-0.099	-0.092	0.627	0.651	0.602	0.667	0.589	0.597	1							
EHCI7EWQ7	0.6	0.53	0.59	0.48	0.591	-0.17	-0.14	-0.08	-0.12	-0.09	-0.09	0.673	0.686	0.652	0.638	0.603	0.571	0.755	1						

						4	6	8	9	6	6													
EHCI6EWQ6	0.599	0.57	0.57	0.5	0.583	-0.163	-0.197	-0.16	-0.167	-0.103	-0.092	0.624	0.644	0.593	0.615	0.622	0.621	0.733	0.696	1				
EHCI5EWQ5	0.642	0.59	0.612	0.533	0.612	-0.192	-0.143	-0.108	-0.103	-0.104	-0.061	0.67	0.668	0.627	0.672	0.681	0.579	0.739	0.769	0.699	1			
EHCI4EWQ4	0.611	0.558	0.578	0.507	0.588	-0.135	-0.158	-0.128	-0.19	-0.121	-0.102	0.617	0.686	0.619	0.646	0.634	0.581	0.711	0.691	0.742	0.729	1		
EHCI3EWQ3	0.602	0.526	0.552	0.522	0.562	-0.149	-0.14	-0.088	-0.111	-0.074	-0.109	0.672	0.627	0.683	0.588	0.68	0.643	0.655	0.722	0.643	0.756	0.687	1	
EHCI2EWQ2	0.555	0.548	0.581	0.493	0.617	-0.17	-0.146	-0.15	-0.119	-0.115	-0.067	0.656	0.701	0.657	0.678	0.649	0.562	0.678	0.734	0.647	0.762	0.723	0.687	1
EHCI1EWQ1	0.636	0.612	0.568	0.554	0.617	-0.169	-0.17	-0.132	-0.166	-0.121	-0.095	0.662	0.656	0.641	0.651	0.67	0.601	0.744	0.71	0.698	0.743	0.724	0.753	0.742	1

Table C12: Residual Covariances for SEM1.1

	ET9	ESe5	ESe3	ESe1	ESe2	ER8	ER6	ER5	ER4	ER3	ER1	ET1	ET3	ET4	ET6	ET7	ET8	EHCI8EWQ8	EHCI7EWQ7	EHCI6EWQ6	EHCI5EWQ5	EHCI4EWQ4	EHCI3EWQ3	EHCI2EWQ2	EHCI1EWQ1
ET9	0																								
ESe5	-0.052	0																							
ESe3	0.01	0.015	0																						
ESe1	-0.056	0.032	-0.044	0																					
ESe2	-0.036	-0.017	-0.011	0.013	0																				
ER8	0.044	-0.053	0.062	-0.003	0.045	0																			
ER6	0.013	-0.104	0.099	-0.049	-0.015	0.004	0																		
ER5	0.003	-0.024	0.107	0.019	0.01	0	-0.025	0																	
ER4	0.077	-0.05	0.057	-0.03	-0.061	-0.007	0.033	0.027	0																
ER3	0.044	-0.056	0.098	-0.01	0.03	-0.015	0.006	-0.018	-0.021	0															

ER1	0.099	0.03	0.153	-0.001	0.006	0.025	-0.04	0.022	-0.038	0.052	0														
ET1	-0.035	-0.07	0.009	-0.045	-0.055	-0.098	-0.004	-0.015	0.038	0.06	0.038	0													
ET3	-0.002	-0.026	0.079	-0.026	0.057	0.016	-0.015	0.023	0.023	0.014	0.065	-0.012	0												
ET4	0.009	-0.073	0.008	-0.051	-0.01	-0.091	-0.014	-0.013	-0.035	0.013	0.034	0.045	-0.006	0											
ET6	-0.014	0.013	0.041	0.041	0.037	-0.098	-0.064	-0.012	-0.055	-0.007	0.019	-0.006	0.009	0.015	0										
ET7	0.007	0	0.047	0.002	0.012	-0.068	-0.04	-0.036	-0.01	0.029	0.056	0.032	-0.06	0.011	-0.002	0									
ET8	0.135	-0.069	0.008	-0.041	-0.005	-0.036	-0.006	0.007	0.045	0.059	0.032	-0.007	0.01	0.015	-0.073	-0.007	0								
EHCI8EWQ8	0.009	0.037	0.136	0.03	0.086	-0.103	-0.073	-0.061	-0.057	0.024	0.023	-0.022	0.019	-0.063	0.041	-0.055	-0.016	0							
EHCI7EWQ7	-0.038	-0.009	0.105	-0.039	0.059	-0.093	-0.034	0.028	-0.011	0.03	0.02	0.017	0.047	-0.019	-0.001	-0.048	-0.053	0.034	0						
EHCI6EWQ6	-0.008	0.063	0.115	0.008	0.083	-0.09	-0.11	-0.075	-0.07	0.016	0.019	-0.002	0.036	-0.051	0.006	0.004	0.037	0.049	-0	0					
EHCI5EWQ5	-0.011	0.038	0.112	0.002	0.064	-0.11	-0.027	0.006	0.024	0.024	0.066	-0.005	0.007	-0.063	0.016	0.014	-0.063	-0	0.016	-0.02	0				
EHCI4EWQ4	-0.015	0.031	0.103	-0.001	0.067	-0.046	-0.053	-0.026	-0.09	-0.003	0.009	-0.03	0.061	-0.043	0.019	-0.005	-0.032	0.002	-0.03	0.062	-0.01	0			
EHCI3EWQ3	-0.017	0.001	0.074	0.019	0.041	-0.062	-0.03	0.023	0.006	0.051	-0.001	0.033	0	0.029	-0.037	0.047	0.043	-0.05	0.009	-0.04	0.022	-0.01	0		
EHCI2EWQ2	-0.077	0.018	0.103	-0.018	0.096	-0.09	-0.037	-0.053	-0.001	0.004	0.054	0.01	0.075	-0.005	0.053	0.009	-0.054	-0.03	0.012	-0.04	0.02	0.015	-0.02	0	
EHCI1EWQ1	-0.007	0.074	0.077	0.035	0.084	-0.088	-0.064	-0.027	-0.057	0.001	0.022	-0.001	0.006	-0.038	0.005	0.015	-0.027	0.016	-0.03	-0.01	-0.02	-0	0.033	0.014	0

Table C13: Standardized Residual Covariance for SEM1.1

	ET9	ESe5	ESe3	ESe1	ESe2	ER8	ER6	ER5	ER4	ER3	ER1	ET1	ET3	ET4	ET6	ET7	ET8	EHCI8EWQ8	EHCI7EWQ7	EHCI6EWQ6	EHCI5EWQ5	EHCI4EWQ4	EHCI3EWQ3	EHCI2EWQ2	EHCI1EWQ1
ET9	0																								

ESe5	-0.702	0																				
ESe3	0.13	0.187	0																			
ESe1	-0.767	0.419	-0.575	0																		
ESe2	-0.481	-0.212	-0.136	0.17	0																	
ER8	0.573	-0.688	0.779	-0.041	0.575	0																
ER6	0.169	-1.4	1.307	-0.652	-0.192	0.041	0															
ER5	0.038	-0.314	1.361	0.248	0.125	0	-0.24	0														
ER4	1.03	-0.672	0.747	-0.401	-0.8	-0.067	0.327	0.266	0													
ER3	0.588	-0.747	1.279	-0.136	0.391	-0.143	0.056	-0.173	-0.206	0												
ER1	1.298	0.391	1.965	-0.016	0.071	0.248	-0.392	0.213	-0.373	0.5	0											
ET1	-0.462	-0.962	0.128	-0.621	-0.737	-1.285	-0.058	-0.201	0.521	0.817	0.51	0										
ET3	-0.021	-0.336	1.015	-0.336	0.716	0.194	-0.189	0.287	0.299	0.179	0.809	-0.147	0									
ET4	0.115	-1.009	0.116	-0.707	-0.129	-1.2	-0.194	-0.17	-0.482	0.175	0.455	0.595	-0.078	0								
ET6	-0.171	0.166	0.535	0.545	0.481	-1.221	-0.839	-0.15	-0.713	-0.088	0.239	-0.075	0.104	0.184	0							
ET7	0.091	-0.001	0.646	0.026	0.164	-0.893	-0.543	-0.483	-0.132	0.391	0.748	0.417	-0.738	0.142	-0.022	0						
ET8	1.676	-0.901	0.108	-0.535	-0.067	-0.44	-0.074	0.084	0.579	0.742	0.403	-0.091	0.122	0.187	-0.875	-0.086	0					
EHCI8EWQ8	0.117	0.521	1.935	0.426	1.196	-1.377	-1.019	-0.816	-0.788	0.335	0.316	-0.301	0.241	-0.867	0.534	-0.762	-0.205	0				
EHCI7EWQ7	-0.527	-0.133	1.526	-0.564	0.85	-1.277	-0.49	0.383	-0.158	0.429	0.275	0.243	0.616	-0.264	-0.017	-0.678	-0.706	0.47	0			
EHCI6EWQ6	-0.105	0.875	1.583	0.109	1.129	-1.156	-1.476	-0.974	-0.93	0.206	0.254	-0.02	0.446	-0.683	0.081	0.05	0.467	0.65	-0	0		
EHCI5EWQ5	-0.16	0.564	1.641	0.037	0.933	-1.531	-0.385	0.082	0.348	0.339	0.936	-0.064	0.098	-0.893	0.213	0.204	-0.846	-0	0.23	-0.3	0	
EHCI4EWQ4	-0.206	0.448	1.467	-0.018	0.944	-0.619	-0.733	-0.344	-1.257	-0.044	0.127	-0.415	0.787	-0.589	0.255	-0.07	-0.416	0.03	-0.4	0.81	-0.1	0
EHCI3EWQ	-	0.01	1.13	0.29	0.62	-	-	0.33	0.09	0.75	-	0.48	-	0.43	-	0.70	0.61	-0.7	0.13	-0.5	0.34	-0.2

3	0.249	9	4	3	1	0.887	0.451	4	2	1	0.016	3	0.006	8	0.521	8	2												
EHCI2EWQ2	-1.069	0.269	1.497	-0.256	1.38	-1.223	-0.52	-0.735	-0.015	0.058	0.752	0.137	0.984	-0.065	0.708	0.132	-0.726	-0.5	0.18	-0.6	0.28	0.2	-0.2	0					
EHCI1EWQ1	-0.089	1.053	1.09	0.507	1.168	-1.174	-0.897	-0.369	-0.79	0.007	0.303	-0.015	0.083	-0.524	0.072	0.206	-0.357	0.22	-0.4	-0.1	-0.2	-0	0.48	0.19	0				

Table C14, Baseline Comparisons					
Model	NFI Delta1	RFI rho1	IFI Delta2	TLI rho2	CFI
Default model	.926	.918	.965	.961	.965
Saturated model	1.000		1.000		1.000
Independence model	.000	.000	.000	.000	.000

Table C15, RMR, GFI				
Model	RMR	GFI	AGFI	PGFI
Default model	.045	.888	.866	.740
Saturated model	.000	1.000		
Independence model	.550	.141	.070	.130

Table C16, RMSEA				
Model	RMSEA	LO 90	HI 90	PCLOSE
Default model	.052	.045	.059	.323
Independence model	.264	.258	.269	.000

Table C17: Residual Covariances for SEM1.0 after deleting EP1, EP2, EP3, EP4 and EP5

	EQ4	EQ3	EQ2	EQ1	ET9	ESe5	ESe3	ESe1	ESe2	ER8	ER6	ER5	ER4	ER3	ER1	ET1	ET3	ET4	ET6	ET7	ET8	EHCI9	EHCI10	EHCI8EWQ8	EHCI7EWQ7	EHCI6EWQ6	EHCI5EWQ5	EHCI4EWQ4	EHCI3EWQ3	EHCI2EWQ2	EHCI1EWQ1
EQ4	0																														
EQ3	0.011	0																													
EQ2	-0.021	0.002	0																												
EQ1	-0.043	-0.004	0.041	0																											
ET9	0.058	0.046	0.057	0.046	0																										
ESe5	0.016	0.019	0.049	0.028	-0.053	0																									
ESe3	0.093	0.05	0.12	0.038	0.009	0.014	0																								
ESe1	0.015	-0.03	0.012	-0.017	-0.057	0.032	-0.044	0																							
ESe2	0.085	0.022	0.063	0.013	-0.037	-0.017	-0.011	0.014	0																						
ER8	-0.036	-0.09	-0.106	0.002	0.044	-0.053	0.062	-0.003	0.045	0																					
ER6	-0.066	-0.056	-0.034	0.022	0.012	-0.104	0.099	-0.049	-0.015	0.004	0																				
ER5	-0.016	0.038	-0.04	0.048	0.003	-0.024	0.107	0.019	0.01	0	-0.025	0																			
ER4	-0.079	-0.006	-0.007	0.087	0.077	-0.005	0.057	-0.003	-0.061	-0.007	0.033	0.027	0																		
ER3	-0.072	-0.033	0.015	0.072	0.044	-0.056	0.098	-0.001	0.003	-0.015	0.006	-0.018	-0.021	0																	
ER1	0.01	0.031	0.02	0.123	0.099	0.003	0.153	-0.001	0.006	0.025	-0.004	0.022	-0.038	0.052	0																
ET1	0.048	0.004	0.105	0.102	-0.036	-0.075	0.005	-0.049	-0.006	-0.097	-0.003	-0.014	0.039	0.061	0.039	0															
ET3	0.149	0.099	0.104	0.016	-0.001	-0.031	0.075	-0.003	0.052	0.017	-0.014	0.024	0.024	0.015	0.066	-0.016	0														
ET4	0.026	0.065	0.062	0.051	0.012	-0.076	0.006	-0.053	-0.012	-0.009	-0.014	-0.013	-0.035	0.013	0.034	0.044	-0.008	0													
ET6	0.017	0.076	0.067	0.046	-0.013	0.008	0.037	0.038	0.033	-0.097	-0.064	-0.011	-0.054	-0.006	0.019	-0.001	0.005	0.014	0												
ET7	0.082	0.002	0.044	0.028	0.012	-0.001	0.046	0.002	0.012	-0.068	-0.004	-0.037	-0.001	0.029	0.056	0.032	-0.059	0.014	0	0											

ET8	0.129	0.079	0.033	-0.003	0.141	-0.069	0.009	-0.04	-0.005	-0.036	-0.006	0.006	0.045	0.058	0.032	-0.006	0.013	0.02	-0.07	0	0										
EHCI9	-0.027	-0.013	0.013	0.019	-0.076	0.069	0.08	0.069	0.086	-0.071	-0.057	-0.042	-0.067	0.024	0.026	-0.001	-0.023	-0.029	-0.004	-0.049	-0.099	0									
EHCI10	-0.061	-0.007	-0.002	0.076	-0.006	0.095	0.066	0.036	0.065	-0.097	-0.019	-0.04	-0.026	0.088	0.113	-0.013	-0.07	-0.047	0.029	-0.043	-0.1	0	0								
EHCI8EWQ8	0.007	-0.013	-0.063	-0.067	0	0.024	0.125	0.019	0.074	-0.101	-0.071	-0.058	-0.054	0.027	0.026	-0.035	0.005	-0.074	0.028	-0.064	-0.023	0.005	0.03	0							
EHCI7EWQ7	0.017	-0.014	-0.036	-0.011	-0.053	-0.026	0.089	-0.054	0.042	-0.09	-0.03	-0.031	-0.007	0.034	0.024	-0.002	0.027	-0.035	-0.02	-0.063	-0.067	0.018	-0.011	0.05	0						
EHCI6EWQ6	0.001	-0.045	-0.05	-0.032	-0.019	0.049	0.102	-0.005	0.069	-0.087	-0.107	-0.072	-0.066	0.019	0.023	-0.017	0.019	-0.064	-0.009	-0.007	0.027	0.032	-0.01	0.07	0.013	0					
EHCI5EWQ5	-0.058	-0.016	0.008	0.012	-0.025	0.022	0.096	-0.013	0.048	-0.107	-0.023	0.009	0.028	0.027	0.07	-0.023	-0.012	-0.079	-0.002	0.001	-0.076	-0.011	0.018	0.015	0.027	-0.004	0				
EHCI4EWQ4	-0.01	-0.022	-0.014	-0.03	-0.034	0.011	0.084	-0.02	0.047	-0.042	-0.048	-0.021	-0.086	0.002	0.014	-0.054	0.037	-0.064	-0.004	-0.024	-0.05	0.038	0.024	0.014	-0.023	0.071	-0.003	0			
EHCI3EWQ3	0.016	-0.007	0.026	-0.001	-0.032	-0.016	0.058	0.003	0.024	-0.058	-0.026	-0.027	-0.01	0.055	0.003	-0.013	-0.021	-0.012	-0.056	-0.032	-0.029	-0.027	-0.047	-0.034	0.016	-0.026	0.031	-0.01	0		
EHCI2EWQ2	0.014	0	-0.026	-0.001	-0.094	-0.001	0.085	-0.035	0.078	-0.086	-0.032	-0.049	-0.003	0.009	0.058	-0.012	-0.052	-0.024	-0.031	-0.008	-0.071	-0.008	-0.005	-0.021	0.02	-0.033	0.028	0.018	-0.01	0	
EHCI1EWQ1	-0.008	-0.018	-0.041	-0.009	-0.024	-0.054	-0.059	-0.017	-0.064	-0.084	-0.06	-0.023	-0.052	-0.005	-0.027	-0.023	-0.016	-0.058	-0.016	-0.002	-0.044	-0.013	-0.031	0.031	-0.022	0.004	-0.007	0.001	0.039	0.019	0

Table C18: Standardized Residual Covariances for SEM1.0 after deleting EP1, EP2, EP3, EP4 and EP5

	EQ4	EQ3	EQ2	EQ1	ET9	ESe5	ESe3	ESe1	ESe2	ER8	ER6	ER5	ER4	ER3	ER1	ET1	ET3	ET4	ET6	ET7	ET8	EHCI9	EHCI10	EHCI8EWQ8	EHCI7EWQ7	EHCI6EWQ6	EHCI5EWQ5	EHCI4EWQ4	EHCI3EWQ3	EHCI2EWQ2	EHCI1EWQ1
EQ4	0																														
EQ3	0.132	0																													
EQ2	-0.27	0.024	0																												
EQ1	-0.57	-0.05	0.581	0																											
ET9	0.736	0.586	0.782	0.655	0																										
ESe5	0.217	0.257	0.7	0.416	-0.721	0																									

ESe3	1.217	0.672	1.701	0.562	0.118	0.178	0																						
ESe1	0.202	-0.398	0.165	-0.26	-0.771	0.418	-0.569	0																					
ESe2	1.096	0.294	0.876	0.189	-0.49	-0.218	-0.135	0.18	0																				
ER8	-0.445	-1.136	-1.428	0.029	0.572	-0.685	0.779	-0.043	0.575	0																			
ER6	-0.847	-0.734	-0.481	0.32	0.167	-1.397	1.308	-0.653	-0.192	0.041	0																		
ER5	-0.2	0.488	-0.54	0.67	0.036	-0.312	1.362	0.246	0.125	0.001	-0.239	0																	
ER4	-1.012	-0.082	-0.104	1.252	1.028	-0.669	0.748	0.402	-0.8	-0.067	0.327	0.266	0																
ER3	-0.917	-0.422	0.203	1.031	0.586	-0.744	1.28	-0.138	0.391	-0.143	0.056	-0.173	-0.206	0															
ER1	0.119	0.392	0.276	1.726	1.297	0.394	1.966	-0.018	0.071	0.248	-0.392	0.213	-0.373	0.5	0														
ET1	0.613	0.517	1.434	1.464	-0.462	-1.033	0.066	-0.677	-0.799	-1.275	-0.047	-0.19	0.533	0.828	0.521	0													
ET3	1.774	1.185	1.337	0.211	-0.015	-0.401	0.957	-0.387	0.658	0.202	-0.179	0.297	0.309	0.189	0.819	-0.202	0												
ET4	0.328	0.834	0.847	0.735	0.155	-1.045	0.087	0.729	-0.158	1.198	-0.191	0.168	0.479	0.177	0.457	0.573	-0.093	0											
ET6	0.208	0.939	0.885	0.632	-0.157	0.107	0.485	0.501	0.431	-1.214	0.83	-0.142	0.705	-0.079	0.247	-0.121	0.065	0.178	0										
ET7	1.047	0.255	0.611	0.405	0.155	-0.017	0.637	0.025	0.158	-0.896	0.546	-0.486	0.134	0.388	0.746	0.421	-0.728	0.187	-0.004	0									
ET8	1.553	0.967	0.436	-0.04	1.756	-0.903	0.112	-0.524	-0.06	-0.445	-0.079	0.078	0.573	0.736	0.398	-0.072	0.147	0.246	-0.844	-0.005	0								
EHCI9	-0.366	-0.176	0.188	0.295	-1.098	1.034	1.201	1.036	1.273	-1	-0.843	-0.594	-0.985	0.348	0.375	-0.01	-0.308	-0.422	-0.062	-0.72	-1.359	0							
EHCI10	-0.85	-0.094	-0.031	1.21	-0.091	1.468	1.009	0.548	0.979	-1.373	-0.281	-0.058	0.39	1.294	1.629	-0.192	-0.971	-0.699	-0.417	-0.642	-1.42	0	0						
EHCI8EWQ8	0.091	-0.164	-0.868	-0.97	-0.004	0.344	1.77	0.268	1.025	-1.345	-0.982	-0.781	-0.751	0.372	0.35	-0.481	0.067	-1.007	0.367	-0.878	-0.305	0.08	0.45	0					
EHCI7EWQ7	0.218	-0.182	-0.499	-0.155	-0.729	-0.383	1.288	-0.791	0.603	-1.228	-0.434	-0.435	-0.101	0.486	0.328	-0.028	0.352	-0.495	-0.266	-0.878	-0.886	0.27	-0.17	0.7	0				
EHCI6EWQ6	0.015	-0.557	-0.659	-0.451	-0.255	0.671	1.396	-0.072	0.933	-1.119	-1.433	-0.934	-0.886	0.25	0.294	-0.231	0.241	-0.855	-0.113	-0.1	0.335	0.45	-0.15	0.93	0.17	0			
EHCI5EWQ5	-0.756	-0.218	0.107	0.179	-0.354	0.317	1.409	-0.186	0.693	-1.484	-0.331	-0.133	0.403	0.394	0.987	-0.323	-0.153	-1.11	-0.029	0.008	-1.015	-0.16	0.27	0.21	0.39	-0.06	0		
EHCI4E	-	-	-	-	-	0.1	1.1	-	0.6	-	-	-	-	0.0	0.1	-	0.4	-	-	-	-	0.5	0.36	0.2	-0.32	0.95	-0.04	0	

WQ4	0.124	0.282	0.189	0.423	0.461	5	87	0.291	52	0.561	0.666	0.282	1.188	24	9	0.731	69	0.87	0.048	0.326	0.647	5									
EHCI3E WQ3	0.217	-0.093	0.387	-0.014	-0.471	-0.246	0.884	0.047	0.361	-0.835	-0.392	0.389	0.152	0.811	0.04	0.192	-0.283	0.183	-0.784	0.48	0.407	-0.42	-0.76	-0.5	0.25	-0.37	0.47	-0.14	0		
EHCI2E WQ2	0.177	-0.004	-0.358	-0.02	-1.298	-0.011	1.233	-0.511	1.102	-1.169	-0.457	-0.676	0.048	0.122	0.811	-0.165	0.684	-0.331	0.42	-0.106	-0.936	-0.12	0.08	-0.29	0.28	-0.45	0.41	0.25	-0.14	0	
EHCI1E WQ1	-0.095	-0.233	-0.563	0.131	-0.323	0.767	0.828	0.247	0.891	-1.12	-0.834	-0.311	-0.726	0.072	0.363	-0.315	-0.208	-0.784	-0.209	-0.031	-0.568	0.18	0.45	0.42	-0.3	0.06	-0.1	0.02	0.56	0.27	0

Table C19, RMR, GFI for Model SEM1.0-Initial model-after deleting EP

Model	RMR	GFI	AGFI	PGFI
Default model	.046	.840	.814	.723
Saturated model	.000	1.000		
Independence model	.571	.106	.046	.099

Table C20, Baseline Comparisons for Model SEM1.0-Initial model-after deleting EP

Model	NFI Delta1	RFI rho1	IFI Delta2	TLI rho2	CFI
Default model	.899	.890	.944	.938	.943
Saturated model	1.000		1.000		1.000
Independence model	.000	.000	.000	.000	.000

Table C21, RMSEA for Model SEM1.0-Initial model-after deleting EP

Model	RMSEA	LO 90	HI 90	PCLOSE
Default model	.061	.055	.066	.001
Independence model	.245	.241	.250	.000

Table C22: Sample Correlations - Estimates

	ET9	ESe5	ESe3	ESe1	ESe2	ER8	ER6	ER5	ER4	ER3	ER1	ET1	ET3	ET4	ET6	ET7	ET8	EU4	EU3	EU1	EEOU 1	EEOU 2	EEOU 3	EEOU 4
ET9	1																							
ESe5	0.521	1																						
ESe3	0.528	0.664	1																					
ESe1	0.495	0.711	0.586	1																				
ESe2	0.533	0.692	0.638	0.69	1																			
ER8	-0.074	-0.182	-0.086	-0.139	-0.108	1																		
ER6	-0.114	-0.247	-0.076	-0.197	-0.176	0.56	1																	
ER5	-0.113	-0.173	-0.063	-0.134	-0.147	0.52	0.589	1																
ER4	-0.067	-0.207	-0.111	-0.185	-0.214	0.563	0.682	0.633	1															
ER3	-0.093	-0.212	-0.081	-0.17	-0.146	0.56	0.667	0.607	0.66	1														
ER1	-0.043	-0.134	-0.03	-0.151	-0.152	0.543	0.587	0.586	0.599	0.661	1													
ET1	0.659	0.522	0.545	0.521	0.534	-0.184	-0.131	-0.131	-0.1	-0.084	-0.092	1												
ET3	0.677	0.553	0.592	0.53	0.619	-0.097	-0.136	-0.101	-0.111	-0.118	-0.072	0.69	1											
ET4	0.714	0.532	0.556	0.528	0.587	-0.181	-0.142	-0.132	-0.161	-0.124	-0.098	0.771	0.71	1										
ET6	0.662	0.582	0.557	0.583	0.6	-0.177	-0.173	-0.125	-0.168	-0.132	-0.104	0.69	0.69	0.724	1									
ET7	0.69	0.58	0.573	0.558	0.588	-0.16	-0.158	-0.146	-0.136	-0.107	-0.077	0.735	0.642	0.732	0.687	1								
ET8	0.766	0.494	0.513	0.496	0.545	-0.129	-0.125	-0.108	-0.09	-0.081	-0.091	0.667	0.669	0.701	0.596	0.66	1							
EU4	0.608	0.537	0.542	0.521	0.614	-0.155	-0.132	-0.123	-0.156	-0.104	-0.081	0.666	0.684	0.686	0.638	0.605	0.589	1						
EU3	0.595	0.529	0.546	0.505	0.556	-0.158	-0.1	-0.122	-0.087	-0.068	-0.042	0.644	0.604	0.614	0.634	0.622	0.515	0.779	1					
EU1	0.542	0.493	0.521	0.468	0.533	-0.164	-0.052	-0.083	-0.062	-0.002	-0.009	0.655	0.567	0.586	0.609	0.614	0.485	0.719	0.809	1				
EEOU 1	0.562	0.547	0.571	0.592	0.605	-0.139	-0.153	-0.124	-0.179	-0.09	-0.06	0.613	0.567	0.589	0.655	0.646	0.463	0.652	0.701	0.709	1			
EEOU 2	0.582	0.6	0.586	0.568	0.643	-0.133	-0.186	-0.162	-0.194	-0.114	-0.069	0.613	0.572	0.594	0.642	0.621	0.547	0.684	0.688	0.701	0.757	1		
EEOU 3	0.6	0.633	0.606	0.567	0.605	-0.188	-0.177	-0.195	-0.167	-0.14	-0.116	0.602	0.585	0.585	0.636	0.612	0.55	0.668	0.725	0.703	0.715	0.784	1	
EEOU 4	0.487	0.512	0.559	0.537	0.571	-0.163	-0.2	-0.116	-0.219	-0.163	-0.132	0.572	0.582	0.555	0.6	0.554	0.487	0.712	0.649	0.638	0.689	0.66	0.651	1

Table C23: Variance Extracted AVE for SEM 1.0

			Estimate (A)		S.E. (B)
EHCI1EWQ1	<---	Technology-	0.861	0.741321	0.024
EHCI2EWQ2	<---	Technology-	0.841	0.707281	0.026
EHCI3EWQ3	<---	Technology-	0.829	0.687241	0.025
EHCI4EWQ4	<---	Technology-	0.84	0.7056	0.027
EHCI5EWQ5	<---	Technology-	0.872	0.760384	0.021
EHCI6EWQ6	<---	Technology-	0.806	0.649636	0.034
EHCI7EWQ7	<---	Technology-	0.85	0.7225	0.024
EHCI8EWQ8	<---	Technology-	0.831	0.690561	0.028
EHCI10	<---	HCI_(Interaction)	0.8	0.64	0.033
EHCI9	<---	HCI_(Interaction)	0.887	0.786769	0.041
ET8	<---	ET	0.793	0.628849	0.03
ET7	<---	ET	0.833	0.693889	0.034
ET6	<---	ET	0.825	0.680625	0.026
ET4	<---	ET	0.862	0.743044	0.035
ET3	<---	ET	0.831	0.690561	0.028
ET1	<---	ET	0.847	0.717409	0.062
ER1	<---	ER	0.762	0.580644	0.051
ER3	<---	ER	0.823	0.677329	0.051
ER4	<---	ER	0.82	0.6724	0.065
ER5	<---	ER	0.751	0.564001	0.053
ER6	<---	ER	0.805	0.648025	0.075
ER8	<---	ER	0.692	0.478864	0.037
ESe2	<---	ESec	0.839	0.703921	0.039

A	649.842064
B	1.133
C	21.00892
A+B	650.975064
A/(A+B)	0.998259534
C+B	22.14192

ESe1	<---	ESec	0.808	0.652864	0.045
ESe3	<---	ESec	0.772	0.595984	0.035
ESe5	<---	ESec	0.844	0.712336	0.034
ET9	<---	ET	0.816	0.665856	0.028
EQ1	<---	Service_Quality	0.813	0.660969	0.03
EQ2	<---	Service_Quality	0.858	0.736164	0.026
EQ3	<---	Service_Quality	0.863	0.744769	0.029
EQ4	<---	Service_Quality	0.818	0.669124	0.037
			25.492	21.00892	1.133
			649.842064		

C/(C+B)	0.948830092

Table C24: Variance Extracted AVE for SEM 2.0

			Estimate	
EP	<-->	Service_Quality	0.227	0.051529
EP	<-->	ET	0.246	0.060516
EP	<-->	ESe	0.324	0.104976
EP	<-->	ER	-0.669	0.447561
ER	<-->	ESe	-0.244	0.059536
ET	<-->	ER	-0.181	0.032761
ET	<-->	ESe	0.803	0.644809
HCI_(Interface)	<-->	Service_Quality	0.889	0.790321
HCI_(Interface)	<-->	EP	0.219	0.047961
HCI_(Interface)	<--	ET	0.833	0.693889

	>			
HCI_(Interface)	<-->	Technology-	0.947	0.896809
HCI_(Interface)	<-->	ER	-0.181	0.032761
HCI_(Interface)	<-->	ESe	0.832	0.692224
PEOU	<-->	ER	-0.225	0.050625
PEOU	<-->	Technology-	0.937	0.877969
PEOU	<-->	Service_Quality	0.877	0.769129
PEOU	<-->	PU	0.92	0.8464
PEOU	<-->	HCI_(Interface)	0.939	0.881721
PEOU	<-->	EP	0.286	0.081796
PEOU	<-->	ET	0.826	0.682276
PEOU	<-->	ESe	0.842	0.708964
PU	<-->	ER	-0.132	0.017424
PU	<-->	Technology-	0.938	0.879844
PU	<-->	Service_Quality	0.905	0.819025
PU	<-->	HCI_(Interface)	0.917	0.840889
PU	<-->	EP	0.202	0.040804
PU	<-->	ET	0.833	0.693889
PU	<-->	ESe	0.738	0.544644
Service_Quality	<-->	ER	-0.18	0.0324
Service_Quality	<-->	ET	0.991	0.982081
Service_Quality	<-->	ESe	0.802	0.643204
Technology-	<--	ER	-0.194	0.037636

Technology-	<-->	Service_Quality	0.952	0.906304
Technology-	<-->	ESe	0.814	0.662596
Technology-	<-->	ET	0.898	0.806404
Technology-	<-->	EP	0.272	0.073984