An Information Security Model for E-Government Adoption in Uganda

by

Khanyako Eseri
BEM (Mak)
Reg. No: 2009/HD18/16322U
E-mail: Khanyakoesther8.last@yahoo.com, (+256 0712216602)

A Dissertation Submitted to the College of Computing and Information Sciences in Partial Fulfillment of the Requirements for the Award of the Degree of Master of Information Technology of Makerere University

June, 2014

Declaration

I Khanyako Eseri, do hereby declare that this Dissertation is original and has not been published or submitted for any other degree award to any other University before.

Signed……. Date…….

Khanyako Eseri

Approval

Signed ……. Supervisor Date: …….

Gilbert Maiga (PhD)
Department of Information Technology
Makerere University

Acknowledgement

I extend my deep gratitude to all the people who helped me in all ways to get this report done, for had it not been with your help it would have been impossible for me to achieve this goal. I am very grateful to the Almighty God for having brought you all in my life, and for His continued provision and protection all through this journey.

First of all my deep thanks go to my supervisor Dr. Gilbert Maiga who through his tireless effort and continued support guided me in the right direction. I appreciate all the good advice he gave me during this period.

I am also grateful to the principal personnel officer ministry of local government, registrar ministry of ICT, deputy chief administrative officer Sironko district, assistant engineer and probation officer Mbale district through whose assistance I was granted permission to conduct the survey in the field. And to all the respondents who participated in the survey availing me with valuable comments and several important ideas, I say thank you so much.

On a personal note I would like to specially thank my parents Mr. and Mrs. Wanyisi as well as my brothers and sisters for the moral support and constant encouragement given to me to ensure I finish this course. I am blessed to have you in my life and I am glad that you believed in me all the way. To all my friends' thanks for all the support rendered to me.

My humble prayer is that God blesses each and every one of you and again thanks.

List of Acronyms

CAO	Chief Administrative Officer
E-Government	Electronic Government
ICT Information	Communication and Technology
IFMS	Integrated Financial Management System
IT	Information Technology
InfoSec	Information Security
LoGICS	Local Governments Information Communication System
MDAs	Government Ministries, Departments, Agencies
MoICT	Ministry of Information and Communications Technology
NITA-U	National Information Technology Authority-Uganda

Table of Contents

List of Tables

List of Figures

Abstract

Information security is important as it enables new technologies to include e-government systems to be adopted. It determines the intended adopters and implementers' trust in the new technology. It assures security of the information exchanged over the e-government platform which strengthens services to include user authentication, accountability, reliability and authorization. It also enables the active participation and inclusion of users in the e-government system. Despite these benefits, the important role of information security in the adoption and continued use of e-government services remains little understood. Thus its effective incorporation into e-government for its successful adoption is still problematic. This is mainly due to the problem of lack of an appropriate information security e-government adoption model to guide the government in successful e-government adoption in Uganda. This study aimed to address the above problem by creating a model for e-government adoption that explains the relationship between information security factors and the successful adoption of e-government in Uganda.

A field survey was conducted to obtain requirements for the model. Data was collected using questionnaires that were administered on government employees in the selected units of Mbale, Sironko districts as well as ICT and Local government ministry headquarters Kampala. Correlation and Regression analyses were performed to test relationships suggested between the incorporated information security factors and e-government adoption as well as to evaluate the developed model. The tests confirmed the assumed relationships and the results got were used to extend an existing model so as to develop one suitable for the study context. The model demonstrates that confidentiality, accountability and trust are factors that can be used to predict the e-government adoption process. The results also contribute to e-government literature by providing a model for improved understanding of the information security issues vital for increasing e-government services adoption and usage in Uganda. The model's potential is that it is generic and may find application in other technologically developing countries.

CHAPTER ONE

Introduction

1.1 Background

Improving service delivery remains a major driving goal of adopting e-government for any country (Löfstedt, 2005; UN, 2010). To achieve the full range of benefits of e-government adoption, the adopting countries need to attain the different levels of e-government processes. These are the emerging, enhanced, interactive, transactional and connected levels of e-government services (UN, 2008). At the emerging level of e-government services much information is static and there is little interaction with citizens. At the enhanced level, there is more information provision on public policy and governance. The interactive level has governments delivering online services such as downloadable forms for tax payments and the websites are interactive. The transactional level, is a two-way interaction between citizens and services access online is 24/7 and finally the connected (most sophisticated) stage where government is a connected entity with an integrated back office infrastructure (*Ibid*).

The benefits of adoption and use of e-government remain elusive in the developing countries due to its low adoption rates (Al-adawi *et al*., 2005). In the case of Uganda, the e-government development index in 2012 was at 0.3185 (UN, 2012). In terms of e-government services offered Uganda is at stage 2 (Wangwe *et al*., 2012, p.30). Uganda's total online service index value as of 2012 was at 26% out 100% with the emerging level achieved 100% and the transactional level least achieved 8% (UN, 2012). This performance remains poor compared to the overall world average of 0.4882 with Uganda positioned at 143 and ranked in the bottom 50 countries in the world in terms of e-government development index out of 190 countries surveyed (*Ibid*). Identified among the problems hindering successful e-government adoption in Uganda are: the uneven integration of information, communication and technology (ICT) within government, the expensive and inadequate resources to dedicate to installing ICT programs (Rwangoga & Baryayetunga, 2007). Uneven integration of ICTs within government leads to frequent lack of co-ordination in government initiatives (Rwangoga and Baryayetunga, 2007). It constitutes one of the key challenges of a one-stop government implementation (UN, 2012).

Regardless of the level of e-government development, successful adoption still depends on user acceptance of the implemented systems. Successful adoption of e-government still depends on gaining user trust, a factor dependant on the security of transactions via the e-government system. Information Security (InfoSec) has thus been identified as yet another essential factor for the successful adoption of new technologies including e-government systems (Wangwe *et al*., 2012, p.11; UN, 2012). This is attributed to the fact that information security determines trust and security assurance for the new technology by the intended adopters and implementers (Conklin, 2007). Security of an e-government system traditionally encompasses properties of confidentiality, integrity, availability and accountability (Alfawaz *et al*., 2008). The major information security services are the protection of these security properties. Ensuring these properties in e-government systems addresses the aspect of perceived risk leading to security assurance. This enables trust of the adopters to be gained enhancing e-government adoption (Tassabehji, 2005). The role of information security in e-government adoption therefore remains important as systems advance from the interaction to transactional levels of implementation. Information security can be enhanced by application of proper electronic controls, that suite the adopting country context (Conklin, 2007).

Uganda has embraced e-government in public administration with the purpose of improving public service delivery and democratic processes, enhancing attainment of the millennium development goals and other international obligations. The government has installed the national data transmission and e-government backbone infrastructure spanning through 28 districts. The National Information Technology Authority-Uganda (NITA-U) is a lead agency for the development of national e-government strategies and implementation plans (MoICT, 2010b). The benefits perceived to result from embracing e-government as a form of administration include improved services delivered with convenience to citizens, improved productivity of government agencies, facilitation of online business, public empowerment through availing them with information and records in possession of the state so that they effectively scrutinize and participate in government decisions that affect them, creation of a more accountable government leading to good governance and broadening public participation and democracy promotion (*Ibid*).

To ensure an enabling e-government environment, the government of Uganda has set up different policies, laws and initiatives to include the national development plan 2010 (MoICT, 2011), the

national IT policy (MoICT, 2010a), the national e-Government framework (MoICT, 2010b) and the national information security strategy (MoICT, 2011).The national development plan, 2010 under section 328 objective 2, calls for enhancement of use and application of ICT services in business and service delivery (MoICT, 2011). The national IT policy (2010) was also drafted to promote the efficient utilization of information technology in transforming Uganda's economy (MoICT, 2010a). The IT policy states that IT security is a lacking area in the country with many government MDAs and local governments running websites as tools to disseminate information to the public yet these are not secured which has resulted in cases of security breach. The national e-Government framework (2010) has also been drafted to enhance and promote the efficiency and transparency in the functioning of government through the increased use of ICT for online service delivery to citizens and business (MoICT, 2010b). The national e-Government framework states one of the challenges and threats to e-government implementation as cyber crime and cyber terrorism. The framework further identifies accessibility and choice, trust, confidence and security and accountability among the principles to guide the way in which e-government transformation is to be approached (*Ibid*). The national information security strategy (2011) has been drafted to provide a guideline that will reduce the probability of successful information security breaches and lower the risk of consequential damage within the national digital infrastructure (MoICT, 2011). The information security strategy states that Uganda's information security maturity growth based on ISM^3 (Information Security Management Maturity Model) is at level 1 with security not acknowledged as a desirable property of the organization (*Ibid*).

Legislation has also been put in place in Uganda towards the goal of an enabling e-government environment to include the *constitution* of the Republic of Uganda (Republic of Uganda, 1995), the *Electronic transactions Act* (Parliament of Uganda, 2011a), the *Electronic signatures Act* (Parliament of Uganda, 2011b) and the *Computer misuse Act* (Parliament of Uganda, 2010). The *constitution* of the Republic of Uganda states in section 27 subsection 2 that: "No person shall be subjected to interference with the privacy of that person's home, correspondence, communication or other property" (Republic of Uganda, 1995). This deals with ensuring privacy of information exchanged though at individual level and not organizational or corporate level. The Electronic *transactions Act* aims at making provision for using, securing, facilitation and regulation of electronic communications and transactions; encouraging the use of e-Government services and providing for related matters (Parliament of Uganda, 2011a). The *Electronic signatures Act* is

aimed at governing the use of electronic signatures and certification authorities (Parliament of Uganda, 2011b). Finally the *Computer misuse Act* which aims at making provision for the safety and security of electronic transactions and information systems; preventing unlawful access, abuse or misuse of information systems including computers and making provision for securing the conduct of electronic transactions in a trustworthy electronic environment and to provide for other related matters (Parliament of Uganda, 2010). Despite all these initiatives and legal efforts in place there is frequent lack of co-ordination in these government initiatives, few implementations and lack of a comprehensive national framework for information security in e-government (Wangwe *et al*., 2012, p.73,75). Even the existing initiatives such as national websites are inadequate in issues to do with information security and legislation. Asiimwe & Lim (2010) in their study state that ministry websites in Uganda are rather weak in stating legal policies which impacts on users' trust of these websites. Their study showed that all the four ministry websites of ministries of Health, Education and sports, Justice and constitutional affairs and Foreign affairs did not provide any privacy policy or terms and conditions of use (*Ibid*).

Although information security is an important process in as regards to the protection and securing of e-government systems, in Uganda, its implementation has not been uniform with government ministries, departments, agencies and local governments having different levels of ICT development and information security implementations with some more advanced than others (MoICT, 2011; Wangwe *et al*., 2012, p.73). This situation has been worsened by the lack of a national co-ordination approach for handling information security incidents. Currently few government ministries, departments and agencies have information security strategies in place. Also prevalent is limited top management support and too little financial support in implementing information security measures (MoICT, 2011).

Analysis of the soft information security controls in place in government ministries, departments and agencies in Uganda indicate there is still a challenge in as regards to their implementation with review and updating of it security policy rated at 55%, developing and rolling out a security awareness program at 36%, security updates and alerts knowledge management at 40%, drafting IT security incident management procedures at 36%, password and access control procedures hardening and enforcing at 82% and quality assurance/ IT audit on the organizational environment at 36% (MoICT, 2011).

Based on key indicators currently existent in Uganda that determine information security maturity continuity of operations management is rated at 16%, information security incident management at 25%, physical and environmental security controls in place at 44%, human resource security considerations at 36%, information security governance structure in place at 32.5% and existence of a security norms framework that is applied at 10 % (MOICT, 2011). With regards to these statistics, information security management in Uganda is still inadequate and a challenge that needs to be addressed for the realization of e-government adoption. It is therefore important to investigate information security in as regards to e-government adoption so as to determine how to attain the desired information security management maturity needed for successful e-government adoption in Uganda.

1.2 Statement of the Problem

E-Government implementation and adoption processes bring along with them observed benefits of easy information access and sharing, accountability and transparency (MoICT, 2010b). Despite the effort to implement e-government systems in Uganda, the adoption and full realization of its benefits has not been attained. This is largely attributed to the low adoption rates as evidenced by poor e-government performance at the different service and maturity levels (Al-adawi *et al*., 2005). E-government performance in Uganda remains poor with rates of 100% for emerging service (maturity) level, 33% for the enhanced level, 8% at the transactional, 22% for the connected information services (UN, 2012).With an e-government development index of 0.3185, Uganda in the world is positioned at number 143 (*Ibid*).

Lack of trust in the security of information is a key factor that explains the low adoption and usage of e-government services in Uganda (MoICT, 2011; UN, 2012; Wangwe *et al*., 2012). This is mainly due to the lack of an appropriate national information security e-government model to guide the government in successful e-government adoption in Uganda (MoICT, 2011; Mivule & Turner, 2011; Wangwe *et al*., 2012, p.11). Even existing e-government adoption models and studies do not emphasize the important aspect of information security and are more tailored to developed countries. Only a few of the existing models and studies have attempted to address the important aspect of information security (Löfstedt, 2005; Conklin; 2007; Alfawaz *et al*., 2008; Wangwe *et al*., 2012; Olupot & Mayoka, 2013). Of these, Löfstedt (2005) and Conklin (2007) identify it as an area for further research. Alfawaz *et al*. (2008) consider information security as a

key factor for adoption and success of information management systems. Olupot & Mayoka (2013) identify improvement of information security as a requirement for adoption of e-CRM. Wangwe *et al*. (2012, p.11) in their study state that there are no national information security frameworks adopted in the East African community.

In the case of Uganda, there are no studies reported that examine the relationships between information security factors and the success of the e-government adoption process. The role that information security factors plays toward the e-government adoption process in Uganda therefore remains an unanswered question worthy of empirical investigation.

1.3 General Objective

The research aimed to create a model that explains the relationship between information security factors and the successful adoption of e-government in Uganda.

1.4 Research Questions

In order to achieve the general objective, this research was guided by the following questions

i. What are the information security factors that affect adoption of e-government in Uganda?
ii. How can security of e-government services be improved to increase public trust hence adoption of e-government?

1.4.1 Specific Objectives

The above research aim was addressed through these specific objectives

1. To determine the information security factors affecting the e-government adoption process in Uganda.
2. To develop a model for e-government adoption that relates the information security factors to the adoption process in the Ugandan context.

1.5 Scope of the Study

This research sought to address the information security perspective for the e-government adoption process in Uganda. It focused on information security to include e-government as well

as its importance, e-government adoption plus the existing adoption models, information security and its measures, e-government security, e-government in Uganda and the issues in its adoption. A mixed research methodology was adopted with the categories of respondents including departmental heads and staff as employees of Mbale and Sironko districts as well as Local government and ICT ministries Kampala, in Uganda. The research sought to create a valid model of e-government adoption for Uganda that explains the relationship between information security factors and the successful adoption of e-government.

1.6 Justification of the Study

Information security has an important role to play for successful e-government adoption (Conklin, 2007). The important role of information security in the adoption and continued use of e-government services remains little understood. This study therefore contributes to information technology adoption, research and practice by addressing the information security perspective of e-government adoption. The study aimed at creating understanding of the information security factors affecting the e-government adoption process in Uganda and their importance. As a result, the study also developed a model that explains how information security factors relate to the e-government adoption process in the Ugandan context. This study thus is essential and significantly contributes to e-government adoption in the following ways.

1.6.1 Contribution to Theory and Practice

Information security factors affecting the e-government adoption process in Uganda that were not known were determined. These include the factors confidentiality, accountability and trust. Government ministries, departments, agencies and local government district units need to incorporate the factors of confidentiality, accountability and trust in e-government to improve the adoption rates.

A model for e-government adoption that relates information security factors to e-government adoption process in the Ugandan context was developed. This is the main contribution of the study. Regression and correlation analyses were used to evaluate the developed model and the results supported the assumed relationships between information security factors and e-government adoption. By confirming the relationships, the study thus extended knowledge.

The model of information security factors for e-government adoption provides a useful theoretical base. This model may also be used in practice by guiding successful e-government implementation and adoption in Uganda from an information security view.

1.7 Definition of Key Terms as used for this Research

E-government according to this study is the use of information and communication technologies (ICTs) and the internet to enhance the access to and delivery of all facets of government services and operations for the benefit of citizens, businesses, employees and other stakeholders (Srivastava and Teo, 2007; Alshomrani, 2012).

E-government Adoption is the intention to use e-government services to include e-tax, e-health, e-commerce and e-banking Belanger and Carters' study (as cited in Anthopoulose *et al*., 2010).

Trust is the expectation that the promise of an individual or group can be relied upon. Rotter's study (as cited in Belanger & Carter, 2008). Trust is dependent on security of the e-government system.

Security is the protection / defense of transactions via the e-government system. Ensuring the security of information in e-government is achieved through information security (Conklin, 2007).

Information security is the process, by which an organization protects and secures its systems, media and facilities that maintain information vital to its operations with security, as an ongoing procedure and not a state at a point in time (FFIEC, 2006).

1.8 Dissertation Outline

The rest of this dissertation is arranged as follows in the next chapters: Chapter 2 presents literature review on the main concepts of information security and e-government adoption. Chapter 3 discusses the methodology used to investigate the study problem so as to answer the research questions and achieve the study objectives. Chapter 4 presents the data analysis and results description. Chapter 5 presents the discussion of results and conclusions.

CHAPTER TWO

Literature Review

2.1 Introduction

This chapter provides the literature on an Information Security model for E-Government Adoption in Uganda. The chapter therefore evidently brought out literature on topics of E-Government and its importance, E-Government Adoption Process, Information Security, E-government in Uganda as well as the issues in its adoption and a Conceptual Model for the E-Government Adoption Process.

2.2 E-Government

E-Government is the use of information and communication technology (ICT) in public administration to change structures and processes of government organizations so as to improve access and delivery of all aspects of services and operations for the benefit of all its constituents (Srivastava & Teo, 2007; Alshomrani, 2012). E-Government categories based on relationship with government include government-to-citizen (G2C), (G2E) government-to-employee, government-to-government (G2G) and (G2B) government-to-business (Gant, 2008).

The definition of e-government varies based on the community's values, goals and culture as it is more than a website, electronic mail or processing transactions via internet (Lowery, 2001). Thus e-government should be addressed based on three key areas of service provision, digital democracy and use of technology. Addressing it from such a perspective enables avoiding the overlooked broad implications of e-government thereby realizing its true benefits and being well prepared to serve the emerging digital citizenry.

The aim of e-government is improved service delivery (UN, 2008). However, e-government as an aspect of digital government is not an aim in itself, but an enabler tool for improved service delivery as well as a process with different stages to be attained for achievement of successful adoption and should be treated as a reform process integrating government systems to achieve the desired information society and improve service delivery. E-Government is therefore use of

information and communication technologies to promote more efficient and effective government, so as to make it more accessible and accountable to the citizens and it has characteristics of electronic service delivery, electronic workflow, electronic voting and electronic productivity (AlAwadhi & Morris, 2009).

2.2.1 Importance of E-Government

The need for e-government bases its origin into a broader factor related to good governance with governance mainly referring to the mode in which power is exercised by governments, in managing a country's social and economic resources (UNESCO, 2005; Nkwe, 2012). A paradigm shift has been realized by governments and independent policy makers throughout the whole world of the importance of e-government as a strong tool for responsive governance (Bwalya, 2009). E-Government is about transformation to help citizens and businesses find new opportunities in the world's knowledge economy (PCIP, 2002; MoICT, 2010b). E-Government is not only important as a profound tool for transformation in the way the government interacts with the governed but also the reinvention of its internal processes and organization (Al-Mushayt *et al*., 2009; Verma *et al*., 2012).

E-Government advantages are many (Almarabeh & AbuAli, 2010). These include improved service delivery and convenience to the people there by enhancing their quality of life, well being and minimizing the national digital divide, improved productivity of government agencies by forming a backbone of initiatives that enable them to meet the needs for rural and urban administrations to access public services, to communicate and transact with government through mechanisms appropriate to their respective situations. Another advantage is strengthened good governance by creating a government more accountable and transparent through the practice of aggregating data and development of shared service centers. This empowering of public access to information and records in possession of the state also enables the public to effectively scrutinize them and participate in government decisions that affect them which enables fighting the corruption problem and permits promotion of democracy. E-Government facilitates commerce as well as services for businesses online through increased exposure as well as market share and also makes the private sector more competitive by reducing the cost of transaction with the government for example in tax collection and e-procurement (MoICT, 2010b). Though for the maximum potential of e-government to be reached there is need to bridge the gap between what

is offered and what is used so as to enable getting all of the value possible out of e-government investments (Al-adawi *et al*., 2005). This study therefore sought to establish with focus on information security how to bridge that gap for the value and importance of e-government adoption to be effectively realized.

2.3 The E-Government Adoption Process

The E-Government adoption is a process that involves both implementation and adoption aspects using a variety of models. A brief outline of the implementation phases is described here before adoption models are presented.

2.3.1 The E-government Implementation Phases

The implementation of e-government involves five phases emerging, enhanced, interactive, transactional and connected (UN, 2008; Adeyemo, 2011). These e-government implementation phases are as discussed below.

Emerging: The country becomes an e-government player. Official but limited government online presence is established through a few independent government websites. These government websites are developed to provide information to citizens and the information is static.

Enhanced: Government's online presence increases (official websites) and information becomes more dynamic. There are created links to archived information that is easily accessible to citizens like reports. Interaction at this stage is still primarily unidirectional with information flowing essentially from government to the citizen.

Interactive: A platform is built for interaction between citizens and government. Government delivers online services such as downloadable forms and users can e-mail officials and interact through the web.

Transactional: At this stage there is a two-way interaction between citizens and their government. Web tools are created for facilitating transactions of government services. The users can pay for services and other transactions online.

Connected: At this stage there is integration of government systems to share resources. E-services are fully implemented across administration boundaries. This is the most sophisticated level of online e-government initiatives.

As a country progresses from emerging to the connected stage, they are faced with different challenges in terms of infrastructure development, content delivery, security and customer management (UN, 2008). A main challenge faced in the transactional phase is with regards to security in that some form of electronic authentication of the citizen's identity is required to successfully complete the exchange ((UN, 2010). These challenges impact on the rate of advancement from one phase to the next.

2.3.2 The E-government Adoption Process

E-government adoption in any country involves active participation and contribution of a number of stakeholders (Alsaghier *et al*., 2009). United Nations (2008) identified the basic roles played by actors in e-government systems as four including those responsible for enacting/legislating a law, implementing these processes for realizing a law, those defining the processes for realizing a law. Also included are end-users who use e-government services with politicians supplying the e-government system and end-users as its customers. Engaging citizens in e-government as actors however, necessitates that there be transparency, confidence in the systems plus services provided (Tassabehji, 2005). There should therefore be security controls as well as establishments in place and incorporation into the e-government system as a country's constituents actively participate in the system, a situation that necessitates information security integration in e-government adoption.

The importance of e-government lies in its great potential in developing countries, to help people develop their full potential and lead productive and creative lives in accordance with their needs and interests (Gant, 2008). Although the reasons for e-government adoption vary, they include better access to and service delivery to citizens, improved interaction with citizens and business and finally empowerment of citizens through access to information resulting into a more effective and efficient government in general placing citizens at the forefront (UN, 2008).

E-Government is adopted where there is perceived benefit to making a change (Conklin, 2007). Adoption of e-government is therefore utilizing e-government services. Löfstedt (2005) noted

that delivery of faster and cheaper services and information to citizens, business partners, employees, other agencies and government agencies is e-government's important goal. Acceptance of e-government is important for improved service delivery. However several factors fail attainment of this goal of improved service delivery such as trust which affects trust in the internet and government. Trust in government also impacts negatively on perceived risk, these affect the intention to use e-government (Belanger & Carter, 2008). These along with other factors affect e-government adoption rates. To reach the e-government adoption goal efficiently there is need to address e-government adoption from all its categories. E-Government categories based on relationship with government include government-to-citizen (G2C), government-to-employee (G2E), government-to-government (G2G) and government-to-business (G2B) all of which provide government services using internet technology (Siau & Long, 2005; Gant, 2008; Adeyemo, 2011). These as well, are customers of e-government. E-Government definition is incomplete unless all of its customers are identified and considered (Alsaghier *et al*., 2009).

For successful assessment of a country in terms of global trends in e-government development there should be solid evidence of an approach to e-government development placing citizens at the centre (citizen-centric practice). The basis of this measurement is on four factors of provision of basic services online, use of multimedia technology, promotion of two-way exchanges with citizens (transactional level), internet usage to deliver public services and soliciting occasional input on matters of public interest. Development in this context refers to how far governments have actually advanced in the e-government field instead of how ready or able they might be to do so as described in e-government readiness, which is in as regards to e-government development index (UN, 2010).

2.3.3 Theoretical Models for the E-Government Adoption Process

E-government services are built superimposed on information technology infrastructure. Addressing e-government adoption thus necessitates a discussion of the different information technology acceptance models. Several e-government models in literature that address the security construct, information security inclusive are also presented here.

The Technology Acceptance Model (Davis, 1989)

The technology Acceptance Model – TAM (Davis, 1989) is as an extension of Fishbein & Ajzen's 1975 Theory of Reasoned Action model developed to explain user acceptance of information systems.

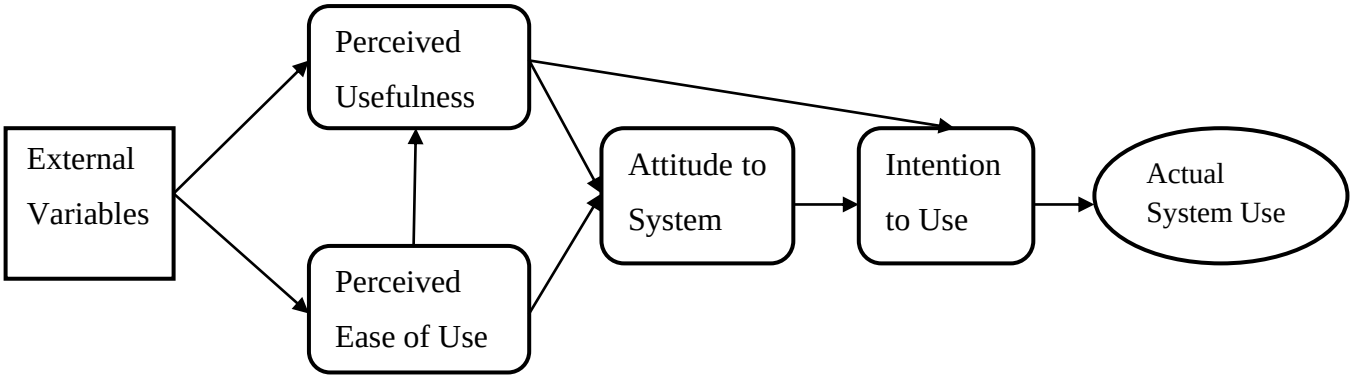

Figure 2. 1: The Technology Acceptance Model (Abbad *et al*., 2009)

This intention-based model represents how users can accept and use technology or reject it based on beliefs which influence attitudes leading to intention to use the system which then generate the behavior to use. Two factors according to this model, Perceived Usefulness (PU) "the degree to which a person believes that using a particular system would enhance his or her job performance" and Perceived ease -of -use (PEOU) "the degree to which a person believes that using a particular system would be free from effort" are crucial in influencing IT acceptance behaviors in the sense that they are products of different number of variables and they cause direct and indirect effects towards attitude of the user and in turn effects towards the adoption of new technology (Abbad *et al*., 2009). TAM as a model has been used by many researchers in reviewing acceptance of technology (Bwalya, 2009). It is a leading model in explaining and predicting system use. However this model has its set back in that it focuses on the individual user and ignores the social processes of information systems development and implementation as well as social consequences of information systems use (Bagozzi, 2007).

Unified Theory of Acceptance and Use of Technology Model (Venkatesh et al. 2003)

The Unified Theory of Acceptance and Use of Technology Model– UTAUT (Venkatesh *et al*., 2003) is as an extension of Davis's 1989 Technology Acceptance Model developed in an attempt to integrate the main competing user acceptance models.

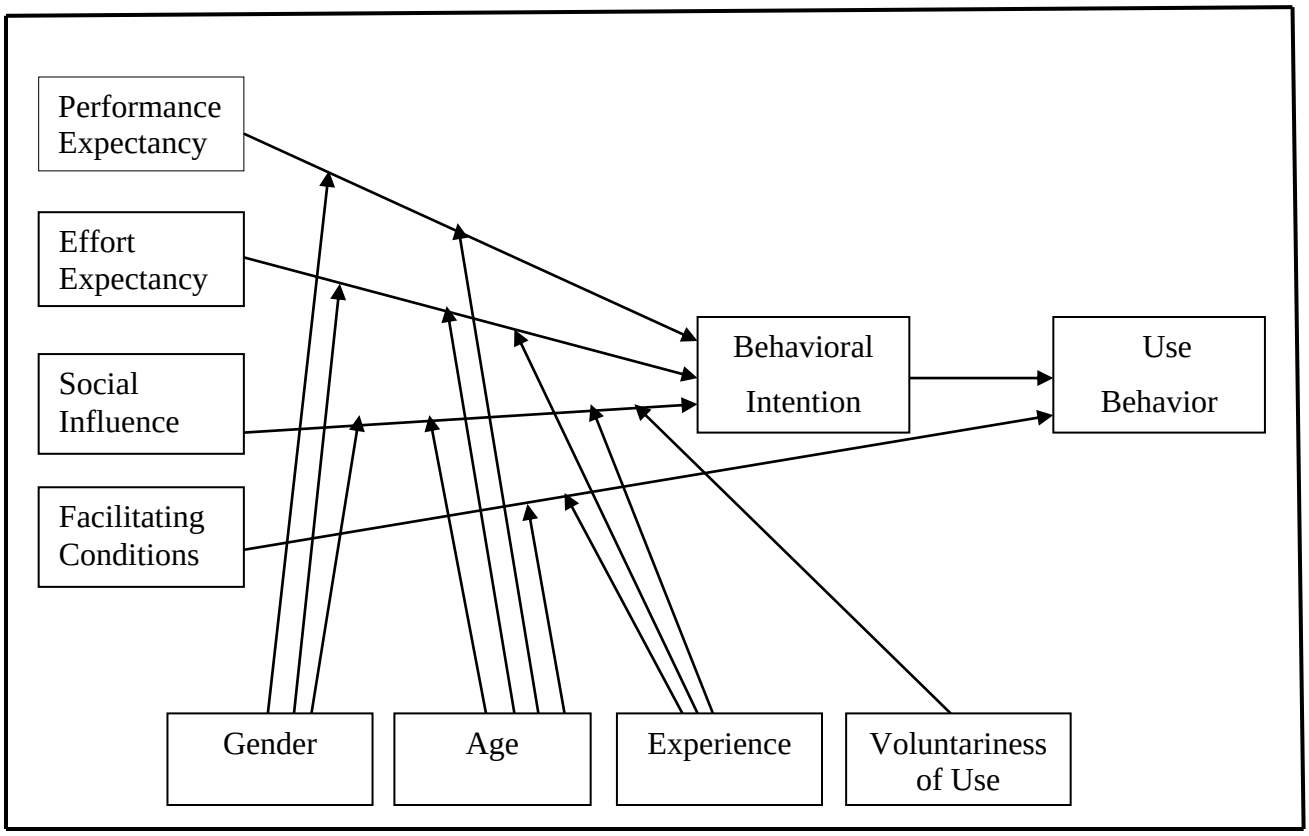

Figure 2. 2: Unified Theory of Acceptance and Use of Technology (Venkatesh *et al*., 2003)

UTAUT as a theory addresses the short come of TAM the social aspect, which is addressed under the social influence factor. The UTAUT theory helps managers assess the likelihood of success for new technologies as well as understand the drivers of technology acceptance (Bwalya, 2009).

Four constructs play a significant role as direct determinants of user acceptance and usage behavior according to this theory, performance expectancy "the degree to which an individual believes that using the system helps him or her to attain gains in job performance", effort expectancy "the degree of ease associated with the use of the system", social influence "the degree to which an individual perceives that it is important others believe he or she should use the new system" and facilitating conditions "the degree to which an individual believes that an organizational and technical infrastructure exists to support use of the system", (Venkatesh *et al*., 2003). The limitation of UTAUT theory is in the scales used to measure the core constructs which affects content validity (choosing the highest-loading items which resulted in items from some of the models not being represented in some of the core constructs). Suggested therefore is the need to view the measures of UTAUT as preliminary and for future research to develop appropriate scales for each of the constructs that address the issue of content validity.

Tassabehji's (2005) Model

The model for managing e-government security to promote inclusion, provided a deeper understanding of the interplay between e-government, security and trust by identifying the internal and external entities needed to ensure e-government security.

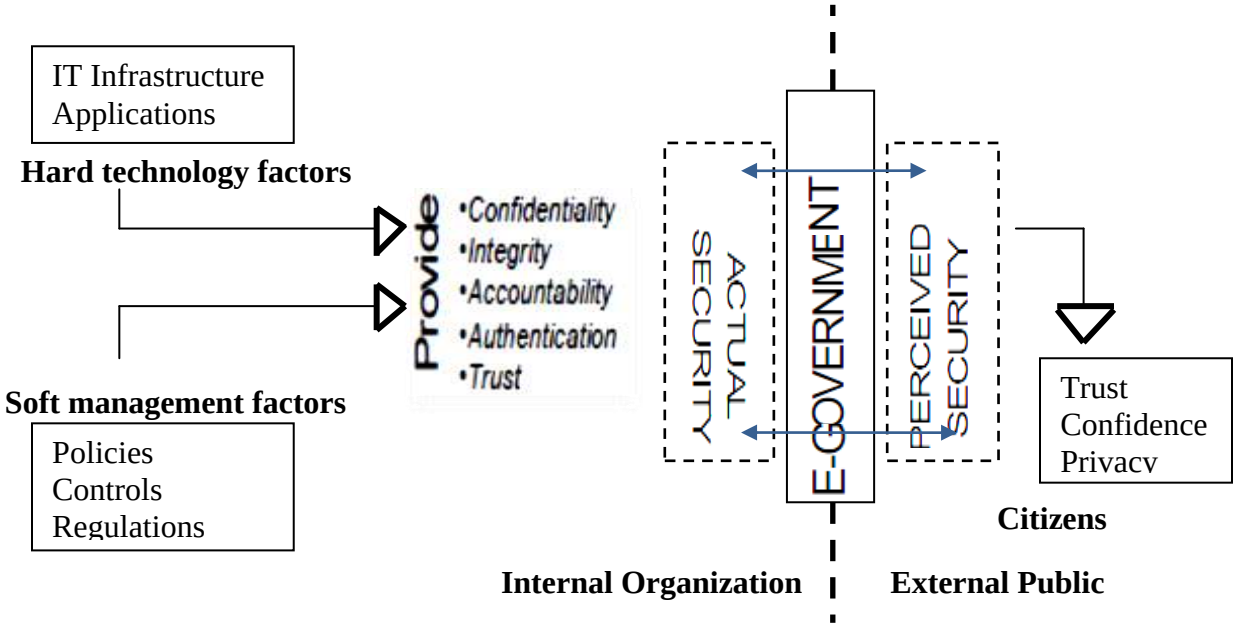

Figure 2. 3: E-government Security Management Model (Tassabehji, 2005)

On the internal side are the hard technological factors and the soft management factors. On the external side are the citizenry, the perception of security implemented in e-government has to be disseminated to. According to this model, the underlying criteria for evaluation of security in e-government are based on common security principles of confidentiality, integrity, accountability, authentication and trust. Further stated is that there should be transparency and confidence in the e-government systems in use in as regards to delivering services advertized with integrity, authentication, confidentiality, trust and accountability (the five major criteria for e-government service evaluation), in order to engage citizens in the process.

Focus of Tassabehji's model is on management of e-government security to promote inclusion. However this is a complex method to manage which becomes even more complex as successful management of security in e-government is broad to include user requirements, organizational change, government regulations and politics as factors affecting implementation and use of e-government services yet these are not addressed in this study but only proposed as areas where further research is needed. Also general e-security and not information security is addressed. To

effectively address this complexity and the above factors it is important to address e-government security from the perspective of information security to which this study seeks to do. Also proposed for further research in Tassabehji's model is the need to understand how to bridge the gap between types of security measures being implemented and the way they are perceived by citizens for instance the type of trust built by the security measures and the type of trust required to develop long term relationships between citizens and government. This can best be addressed in the study context.

Conklin's Model (2007)

Presents information security as an example of technology management in e-government and the failures associated with information security in e-government as general management failures associated with technology implementation.

In this model the moderating factors act as barriers to adoption. These include senior leadership, constituent desires, and bureaucratic rules. These factors vary based on the type of technological innovation being attempted. According to this study using information security as a domain to apply research, has several advantages to include provision of meaningful information usable for making adjustments to the change process thereby enhancing chances of successfully deploying information security controls in an e-government setting.

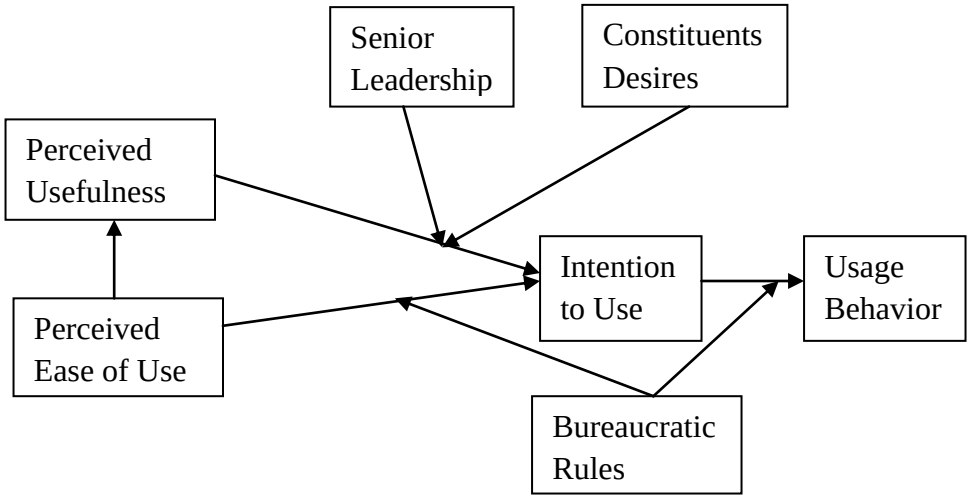

Figure 2. 4: TAM with Moderating Effects (Conklin, 2007)

Alfawaz et al.'s (2008) Model

Presents a framework addressing the management issues involved in improving e-government security in technologically developing countries. This framework is based on Ives et al. (1980) model a well established model used by researchers to tackle different information system issues.

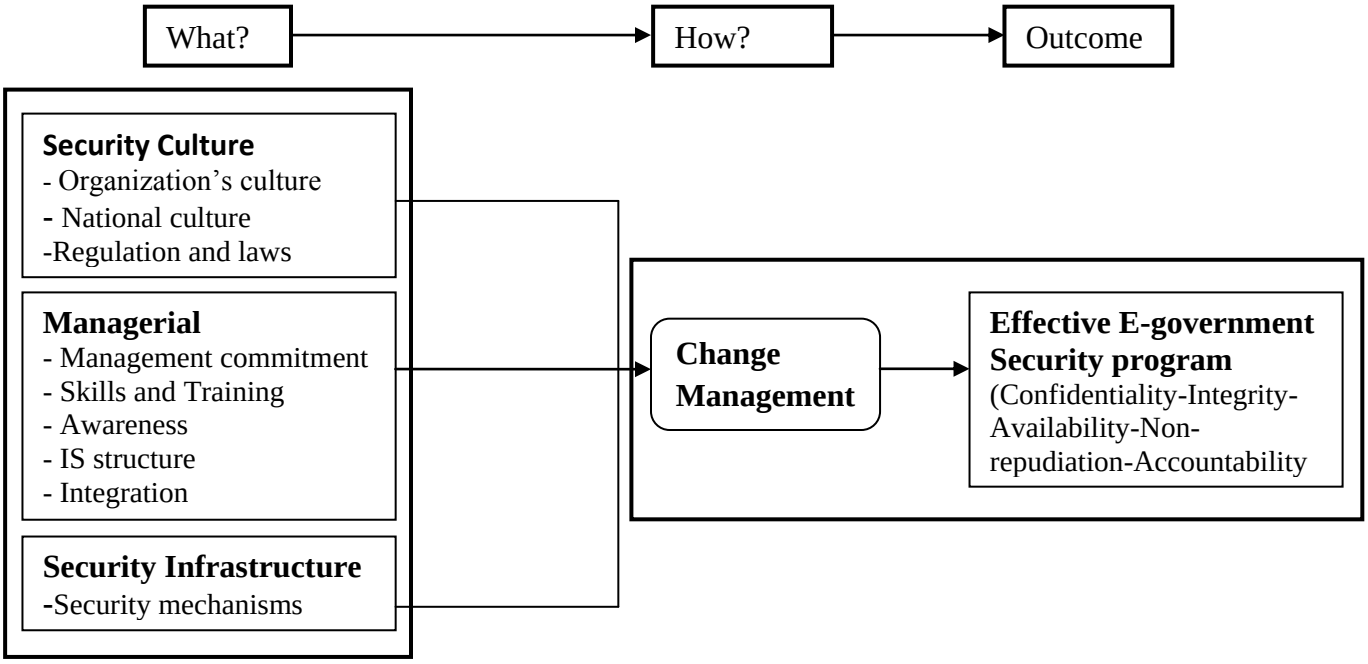

Figure 2. 5: Framework of Information Security Management Factors (Alfawaz *et al*., 2008)

This considers information security management as a main factor of information management systems with security culture, managerial, information security infrastructures and change management identified as the four major components widely believed in open literature to have potential to significantly impact on the protection of organizations' information assets.

According to this model each country has its unique setting and constraints such as political, environmental and economic ones, which impose different issues relevant to e-government security management. Emphasis of this study however, is on e-government security management with InfoSec management as just a component. Further suggested is the fact that e-government security management for countries still developing technologically has added issues mostly to do with environmental factors, which differentiates them from implicit assumptions of leading countries yet these factors impact on the resulting degrees of success of e-government implementations. Therefore a well-developed adoption strategy that enables alignment of ICTs

with the adopting country environment is needed for success (Srivastava & Teo, 2007). To address this gap this study uses a model for e-government adoption that incorporates factors impacting on e-government adoption in the Ugandan context. Proposed in Alfawaz *et al*., (2008)'s study is the need for further testing of the framework for its thorough empirical validation.

Wangwe *et al*.'s (2012) Model

The Technical, Operational and Governance Framework- TOG (Wangwe et al., 2012, p.101-102) is an information security framework for government to government transactions in the East African Community. The framework is based on the identified factors resource constraints, legal and regulatory and national constraints that need to be addressed in the East African Community information security framework (*Ibid*). These were grouped into five perspectives Technical (like hardware or software), operational (like risk assessment, business continuity plans within organizational units of an MDA), governance (policy level within MDAs, across national and regional government like legislation), process (that is a series of steps that MDAs can follow to implement a framework like resource constraints) and maturity, ensuring that the information security framework allows for continual improvement in information security practices within MDAs, across national and regional governments (Wangwe et al., 2012, p.101-102).

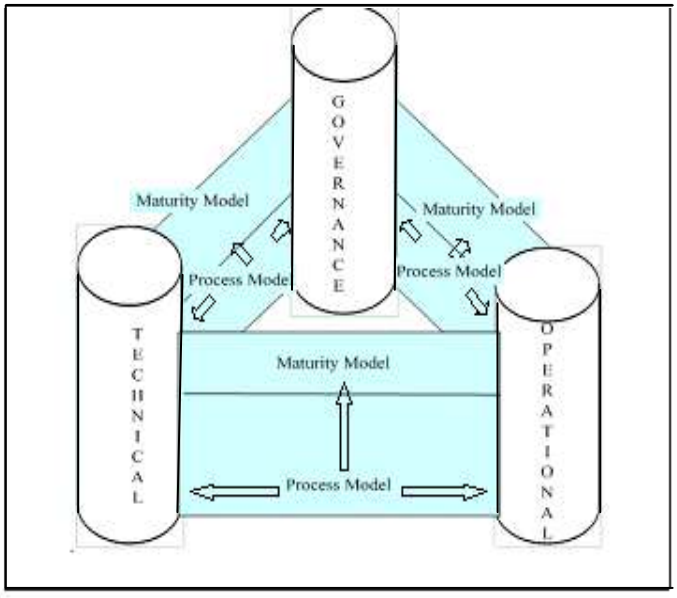

Figure 2. 6: TOG Framework (Wangwe *et al*., 2012)

According to this framework five models address information security for government to government transactions in the East African Community to include Technical (governance and attribute based access control-GABAC, government to government ontologies, service oriented architecture and PKI), operational (organizational plans and programs, certificate authority agreements and common terminology for government to government transactions), governance (international standards, national and regional laws and regulations and organizational policies), process (comprises of two layers government to government transaction between two MDAs and second layer represents any two actors within an MDA or country who are putting in place mechanisms to meet information security) and maturity having level 0, level1, level2 and level 3 maturity levels (Wangwe et al., 2012, p.106-123). Three of the models technical, operational and governance are pillars and can be applied independently to meet information security requirements for government to government transactions when resources are available or when legislation is put in place while the remaining two process and maturity models are mapping mechanisms across those pillars. This framework addresses information security requirements in a manner that recognizes that the contextual issues (resources, lack of legislation and culture in the EAC may not permit a structured approach to implementing of an information security framework. Although this framework addresses the information security gap identified in the above models, the framework has its set back in that it focuses on information security in government to government transactions and ignores other e-government categories (G2C, G2E and G2B). It also addresses the entire East African Community and not the country context yet issues such as culture vary with regard to country context (*Ibid*).

Olupot & Mayoka's 2013

Present a framework for the adoption of electronic customer relationship management (e-CRM) information systems in Uganda. This framework addressed the country context aspect. The framework is based on Thong (1999) Technology organizational environmental management (TOEM) model that identified four main categories of factors that influence technological adoption as technological, organizational, management and environmental (Olupot & Mayoka, 2013).

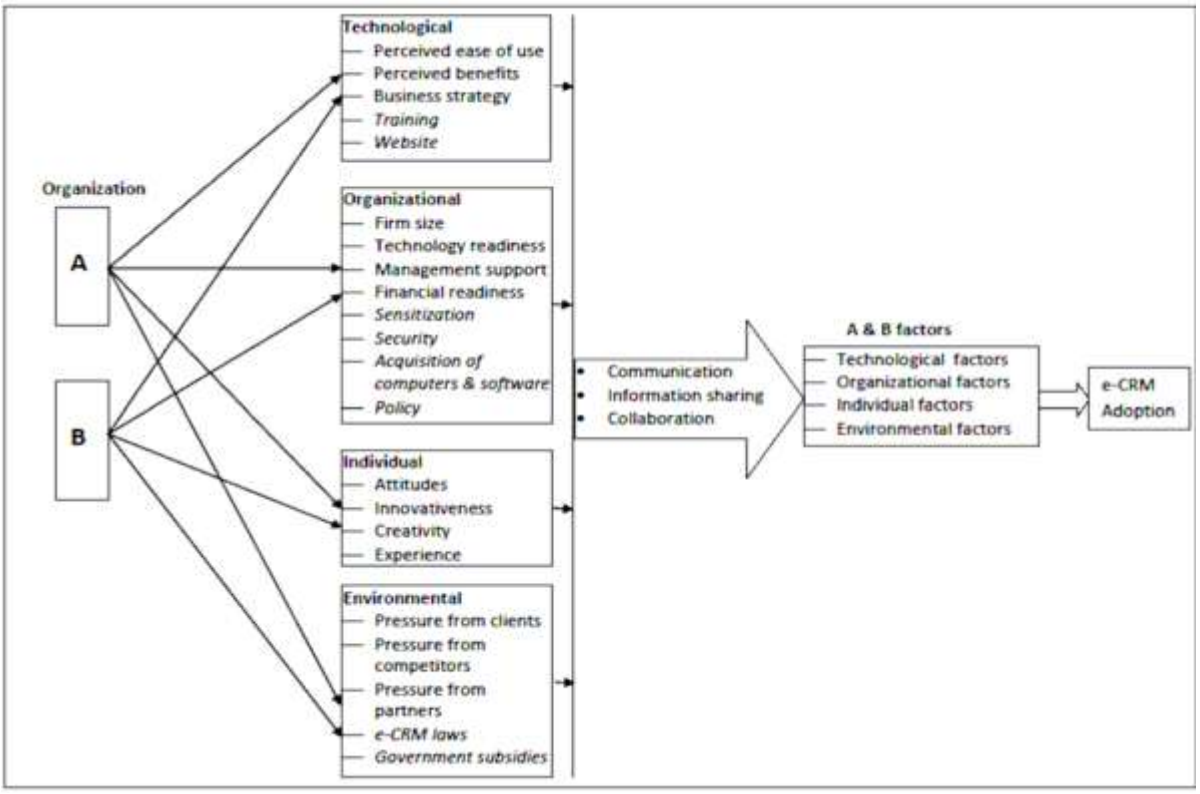

Figure 2. 7: Framework for e-CRM Adoption (Olupot & Mayoka, 2013)

Four main factors according to the e-CRM adoption framework influence electronic customer relationship management (e-CRM) information systems adoption in Uganda, technological factors (perceived ease of use, perceived benefits, business strategy, training and website), organizational (firm size, technology readiness, management support, financial readiness, sensitization, information security, acquisition of computers and software and e-CRM policy), individual (attitudes, innovativeness, creativity and experience) and environmental factors to include pressure from clients, pressure from competitors, pressure from partners, e-CRM laws and government subsidies (Olupot & Mayoka, 2013). This framework however has a setback in that its focus is on electronic customer relationship management (e-CRM) information systems adoption and not e-government adoption. The model does not also addresses information security as a main factor but as only a variable under the major construct of organizational factors (Olupot & Mayoka, 2013).

Bwalya & Healy's (2010) Model

The model of citizen's adoption of e-government in the SADC region is the model for promotion of e-government growth in the SADC region. This model suitably addressed e-government adoption from the perspective of factors inhibiting e-government growth thereby providing understanding on the influences that affect the success or failure of e-government projects. The basis of Bwalya & Healy's (2010) model is on Davis (1989) Technology Acceptance Model (TAM) which was extended so that the local conditions of the adopting country are taken into consideration. The model also uses some constructs from Wangpipatwong *et al*. (2008) that discussed continuance use of e-government besides adoption.

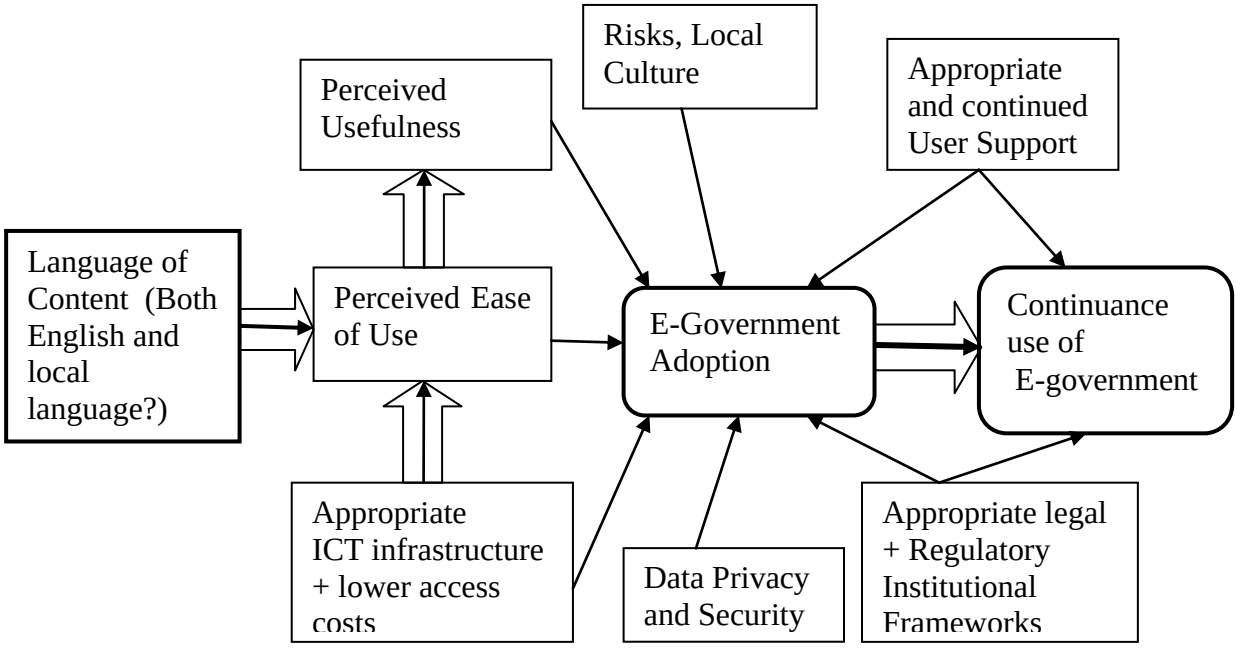

Figure 2. 8: Model of Citizen's Adoption of E-government in SADC (Bwalya & Healy, 2010)

According to Bwalya & Healy's (2010) model, the factors for harnessing e-government adoption in the SADC region include perceived usefulness, perceived ease of use, infrastructure plus lower access costs, both English and local language content, risks and local culture, data privacy and security, appropriate and continued user support, appropriate legal, regulatory plus institutional frameworks and continuance use of e-government. Bwalya & Healy (2010) suggested that data privacy and security if not controlled, may negatively affect the adoption of e-government websites and applications.

Bwalya & Healy's (2010) model extended TAM and incorporated additional factors addressing the local context and multi-dimensionality of e-government aspects. Although the extension makes the model a stronger model proper for any given environment, the model faulted in that it addressed security and privacy in the context of e-government websites and applications. Data privacy and security only addresses aspects of confidentiality and accessibility and not information security across the entire e-government infrastructure for success of the adoption process. Security in e-government services adoption is broad to include factors of confidentiality, integrity, availability, accountability and trust which strengthen user services such as authentication, authorization and reliability (Alfawaz *et al*., 2008). The study's focus is on the Southern African Development Community bloc countries. The model has also not been formally empirically validated to verify its appropriateness to SADC countries and suggested further in the study is the need to examine the dissimilar antecedents of each construct for a clarified understanding of the model (Bwalya & Healy, 2010).

Though Bwalya & Healy's (2010) model did not sufficiently address important factors of information security and trust which when left out may impact on the penetration of e-government in an African context, it was considered the most appropriate model to guide the study. This is because the model is an extension of TAM, an empirically tested model and the model also incorporated factors such as appropriate ICT infrastructure + lower access costs, appropriate legal + regulatory institutional frameworks, continued user support and continuance use of e-government that have been identified among the vital factors affecting e-government services adoption in Uganda. For this reason, information security and trust factors were identified from other studies and the field survey and incorporated into Bwalya & Healy's (2010) model as additional requirements for e-government adoption. This enabled addressing of the shortcomings of the above earlier models, domestication of the model to the Ugandan context as well as its evaluation and the development of the information security e-government adoption model for Uganda.

There is need to analyze e-government adoption in a country so as to understand the current state and the issues in e-government adoption process that need to be addressed to effectively improve e-government adoption. Examining e-government adoption necessitates looking at the different e-government adoption measures.

2.3.4 Measures of the E-Government Adoption Process

Suggested as the common aspects for use as basis in measuring the United Nations e-government development index or advancement of countries in the e-government field are the country's economic strength, technological development and aggregate level of education with technology and education combined with a direct assessment of the state of national online services (UN, 2010). Accurate measurement of the impact of e-government on society should be one based on citizen usage, further than onetime surfing of the website for information seeking purpose with usage measured in terms of a simple decision of using or not using online services, how frequently services are actually used, scope of usage and preference of a government website to other websites (Kumar *et al*., 2007).

Perceived Usefulness and Perceived Ease of Use are the main beliefs influencing attitudes of users of technology (Davis, 1989; Venkatesh *et al*., 2003; Bwalya & Healy, 2010; Olupot & Mayoka, 2013). These determine the intention to use thereby generating the behavior to use technology that is whether users accept and use technology or reject it (*Ibid*). Privacy and security are critical in influencing citizens' willingness and users' intension to adopt as well as use e-government services offered (Löfstedt, 2005; Bwalya & Healy, 2010). Assurance of security of information in e-government systems influences users' trust of the e-government systems. This affects user acceptance and use of these e-systems and services (Conklin, 2007; Alfawaz *et al*., 2008; Olupot & Mayoka, 2013). There is thus a relationship between trust, confidence, familiarity and citizens' increased usage of e-government services (Tassabehji, 2005). Ensuring security in e-systems is an ongoing process hence trust and confidence need to be built over the long term. Increased use of e-government services results in users developing positive views about e-government effectiveness at solving their problems. This results in users' trust and confidence in e-government services (Tassabehji, 2005).

E-government adoption as a process is continuous with different stages emerging, enhanced, interactive, transactional and connected. The actual online transactions take place at the transactional level (Tassabehji, 2005; UN, 2008). Attaining this stage of the two way interaction requires the factor of information security. Information security is an essential component of transaction based systems (Conklin, 2007; Wangwe *et al*., 2012). In broader sense information security involves both the technical and social aspect (Alfawaz *et al*., 2008). Social factors need

also be addressed to enable appropriate e-government security management in the context of the adopting country (Löfstedt, 2005; Alfawaz *et al*., 2008). Continuous management commitment is a requirement for success in e-government adoption (Bwalya & Healy, 2010; Olupot & Mayoka, 2013). Change management is an important aspect for successful e-government adoption (Conklin, 2007). The following table 2.1 presents a summary of the above e-government adoption measures.

Table 2. 1: A Summary of Measures for the E-Government Adoption Process

Measures (Factors)	**Models**								
	TAM Davis (1989)	**UTAUT Venkatesh et al (2003)**	**Tassabehji (2005)**	**Löfstedt (2005)**	**Conklin (2007)**	**Alfawaz et al. (2008)**	**Bwalya & Healy (2010)**	**Wangwe et al. (2012)**	**Olupot & Mayoka (2013)**
Perceived Usefulness	**Yes**	**Yes**	**No**	**Yes**	**Yes**	**No**	**Yes**	**No**	**Yes**
Perceived Ease of Use	**Yes**	**Yes**	**No**	**Yes**	**Yes**	**No**	**Yes**	**No**	**Yes**
Intention to use	**Yes**	**Yes**	**No**	**Yes**	**Yes**	**No**	**Yes**	**No**	**No**
Privacy and Security	**No**	**No**	**Yes**	**Yes**	**No**	**No**	**Yes**	**No**	**No**
Willingness to adopt	**No**	**No**	**No**	**Yes**	**No**	**No**	**No**	**No**	**No**
InfoSec	**No**	**No**	**No**	**Yes**	**Yes**	**Yes**	**No**	**Yes**	**Yes**
Social influence	**No**	**Yes**	**No**	**Yes**	**No**	**Yes**	**Yes**	**No**	**No**
Mg't	**No**	**No**	**No**	**No**	**Yes**	**Yes**	**Yes**	**No**	**Yes**
Change mg't	**No**	**No**	**No**	**No**	**Yes**	**Yes**	**No**	**No**	**No**

Perceived Usefulness is in terms of the extent to which employees believe using the e-government system would enhance their job performance. Using the e-government services should enable employees improve their job performance, productivity and make doing their job easier. Perceived Ease of Use is the degree to the employees believe using the e-government system, would be free of effort. The provided e-government services should be easy for the employees to interact with and use in their work. Intention to use is employees' aim to use the e-government services influenced by the positive or negative feelings they have towards using the

e-government system. Employees' aim should be to accept and use the e-government services and not reject them.

Privacy and security refer to systems as well as information security and employees' privacy. Government should have privacy and security measures in place to ensure the entire e-government platform is secured. With regard to willingness to adopt, the employees should be eager to adopt e-government services offered. Information security includes securing systems, media and facilities processing and maintaining information vital to e-government operations. Government must satisfy fundamental security properties of confidentiality, integrity, and availability in the e-government system to strengthen user services such as authentication, authorization, accountability and reliability. Social influence refers to employees' perception that most people who are important to them think that they should use the e-government services. Social factors such as local language, proportion of coworkers using the e-system, need also be addressed for success in e-government adoption. Management is the party making decisions and promoting e-government adoption. Management need to be committed with regard to several issues such as government support and funding of the e-system, senior management support and help to employees in the use of e-government services. Change management is managing change in e-government context for success in InfoSec management and e-government adoption.

The literature review investigated whether the adoption process and existing adoption models have addressed the above e-government adoption measures. Table 1 shows that though information security is a necessary component for transaction based e-systems most of the models don't address this construct. Five (Conklin, 2007; Alfawaz *et al*., 2008; Wangwe *et al*., 2012; Olupot & Mayoka, 2013) out of the nine models looked at, attempted to address information security but only as a factor but not a main construct. Besides the existing models are tailored for developed countries and are not applicable to Uganda. It is therefore imperative that the information security factor and the most important ingredients creating value for the adoption of e-government applications, perceived usefulness and ease of use be incorporated into the e-government adoption model (Bwalya & Healy, 2010). This is because these determine the adopters trust, acceptance, willingness and intension to use e-government services provided. Information security should thus be addressed to enable effective understanding of the relationship between information security and e-government adoption.

2.4 Information Security

Information security (InfoSec) is the process, by which an organization protects and secures its systems, media and facilities that maintain information vital to its operations with security, as an ongoing procedure and not a state at a point in time (FFIEC, 2006). This process of information security includes management of information security, network security, computer and data security (Bhatnagar & Sharma, 2012).

Information security is important as it plays a key role in the successful adoption of new technologies including e-government systems. It determines trust and security assurance for the new technology by the intended adopters and implementers (Conklin, 2007). Security is an important problem in the spread of computer network technology (Zhou & Hu, 2008). Ensuring information security enables the security problem to be addressed. This is through implementation and meeting the information properties of confidentiality, integrity, and availability in e-government. Guaranteeing the above information properties strengthens user services such as authentication, authorization, accountability and reliability (Alfawaz *et al*., 2008). Information security therefore is vital in the achievement of information, network, computer and data security and in turn the success of e-government adoption.

To measure information security the factors of trust, confidentiality, integrity, availability, accountability, information security policy, security, privacy and perceived risk should be evaluated. Gauging information security existing in a country is essential in understanding a country's performance and state of InfoSec (MoICT, 2011). This assessment also provides the pointers needed to improve information security so as to attain success in its management.

2.4.1 The Measures of Information Security

Trust is a key factor in determination of acceptance and adoption of IT systems and information security controls in e-government (Conklin, 2007; Belanger and Carter, 2008). When users trust their interaction and information exchange over the e-system, they adopt the e-services. Confidentiality, integrity, availability and accountability have been identified as the main principles of information security that have to be considered in measuring existence of information security in e-government systems (Alfawaz *et al*., 2008). Existence of an information security policy in an agency can be used as a measure of how prepared the agency is in adopting

e-government (Belanger and Carter, 2008; Wangwe *et al*., 2009). The policy provides guidance and dictates users' behavior as they interact with the e-system (*Ibid*). The level of security and privacy existent in an e-government system affects its adoption (Conklin, 2007; Alfawaz *et al*., 2008; Bwalya & Healy, 2010).

Trust, security and privacy are main actors in e-government adoption. They lead to security assurance thereby influencing adoption of the new technology (Tassabehji, 2005). Managing security in e-government also includes non technical issues (Alfawaz *et al*., 2008). These issues affect the general attitudes towards information security and its management (Ibid). Perceived risk has been identified as a measure of information security in e-government as it leads to security assurance in e-government which impacts on the intended adopters' trust and adoption of e-government systems (Conklin, 2007; Wangwe *et al*., 2009; Bwalya & Healy, 2010). A high perceived risk associated with the e-system, reduces the rate of e-services adoption (Belanger & Carter, 2008). The following Table 2.2 compares the above information security measures as applied to the various models.

Table 2. 2: Summary of the Measures of Information Security

Authors (Models)	Measures (factors)					
	Trust	Confidentiality, Integrity, Availability and Accountability	Information Security Policy	Security and Privacy	Non Technical Issues	Perceived Risk
Tassabehji (2005)	**Yes**	**Yes**	**No**	**Yes**	**Yes**	**No**
Löfstedt (2005)	**Yes**	**Yes**	**No**	**Yes**	**No**	**No**
Conklin (2007)	**Yes**	**No**	**No**	**Yes**	**No**	**Yes**
Alfawaz et al. (2008)	**No**	**Yes**	**Yes**	**Yes**	**Yes**	**No**
Belanger & Carter (2008)	**Yes**	**No**	**Yes**	**No**	**No**	**Yes**
Wangwe et al. (2009)	**Yes**	**Yes**	**Yes**	**Yes**	**No**	**Yes**
Bwalya & Healy (2010)	**No**	**No**	**No**	**Yes**	**No**	**Yes**

As observed in table 2.2 above, the information security measures to include i) Trust ii) Confidentiality, integrity, availability and accountability iii) Information security policy iv) Security and privacy v) Non technical issues and vi) Perceived risk need to be addressed for success to be reached in the e-government adoption process in Uganda. The main information security measure with regard to the study context is security and privacy, according to six (Tassabehji, 2005; Löfstedt, 2005; Conklin, 2007; Alfawaz *et al*., 2008; Wangwe *et al*., 2009; Bwalya & Healy, 2010) of the seven models looked at.

2.4.2 E-Government Security

Accompanied with e-government progress are increased e-government services which require a higher level of e-government security. As e-government implementation progresses, the number of e-government services introduced to the users increase. Accompanied with this progress is change in the way of interaction between government and citizens from just single interaction to a two way exchange which leads to increased security risk (Zhou & Hu, 2008). This makes it necessary to electronically authenticate the citizen's identity to successfully complete the

exchange (UN, 2010). E-government security hence is considered one of the crucial factors for achieving an advanced stage of e-government (Alfawaz *et al*., 2008).

E-Government security therefore is an aspect that needs to be understood in as regard to describing an e-government adoption model. E-Government includes dependency on online service delivery and technologies used connected over open data networks, which is accompanied by a wide range of information threats (Srivastava and Teo, 2007). The identified security risks in using e-government as a kind of governmental administration include information intercepting, information tampering, services denial, system resources stealing and information faking (Zhou and Hu, 2008). The factors to consider as regards to management of e-government security include security culture, the prevailing attitude towards approaches to a secure organizational environment, management to include awareness, rules to be adhered to as well as responsibilities to be assigned and information security infrastructures, the systems protecting information assets from harm or misuse like the public-key infrastructures (Alfawaz *et al*., 2008).

To achieve security in an e-government system there is need to ensure security for all aspects of e-government services for the government and the users to trust the system and feel confident in using it (Löfstedt, 2005). Such a situation calls for development of a strategy that integrates all themes of e-government security for success in achieving security of an e-government system thereby enabling success in its adoption in Uganda. These themes include e-government systems, information management in the public sector, information systems management and the country context where the phenomenon is to be deployed to operate such as a country's level of e-government readiness (Alfawaz *et al*., 2008).

Zhou and Hu (2008) stated that solving the security problem of e-government system includes addressing it from an angle of security risk management. This management is done by addressing the three aspects of risk identification, risk analysis and risk control. This is the effective way to guarantee the security of an e-government system (Zhou & Hu, 2008). The existing information security infrastructures have to be identified and classified using a published scheme first so as to enumerate and classify the assets that need to be protected by determining which infrastructure is critical for the e-government functions, the security risks they face and which risks need which measures to be effectively addressed. The existence of a security culture linked to the use of IT in public and private sectors enables a lot of users to become aware of the risks arising from

using the information security infrastructures and the existing solutions for avoiding potential threats. Once the risks are identified and analyzed their management can be achieved by setting up rules to be adhered to for risks control, assigning responsibilities for the management of the security risks as well as creating awareness and training so as to build an information security knowledgeable culture across government, private sector and the public at large (MoICT, 2011). This improves trust and reception of e-government systems leading to improved adoption rates.

2.5 E-government in Uganda

The government of Uganda has taken up electronic government with the purpose of efficiently using ICT in public administration to improve public service delivery and democratic processes (MoICT, 2010b). This is to as well enhance attainment of the millennium development goals and other international obligations (*Ibid*). In a bid to implement and adopt electronic government, the government of Uganda has set up several initiatives. The telecommunication sector was liberalized leading to nationwide availability of telecommunications services. In addition a national data and e-government backbone infrastructure is being installed by the government. The e-government infrastructure is to connect all government ministries and departments. 27 ministries have already been connected to the e-government network (MoICT, 2010b).

Applications and services have been implemented as well to include development of websites for district local governments in the country under the Rural Communication Development Program, building of a national data centre to facilitate government wide data storage, usage, sharing and security. Under implementation currently is the government of Uganda web portal to act as a gateway to give government services linkages with the business sector. Different government ministries have also taken on computerization projects such as Integrated Financial Management System (IFMS) by Ministry of Finance Planning and Economic Development and Local Government Information and Communication System (LoGICS) by Ministry of Local Government (MoICT, 2010b). A legal and regulatory framework relevant to the e-government process is being setup in Uganda. This includes drafted policies like the Information Technology Policy for Uganda 2010 and ICT related laws like the Electronic Transactions Bill that are in parliament awaiting passing. The bill was developed by Ministry of ICT and the Uganda Law Reform Commission.

The e-government institutional framework in Uganda is headed by Ministry of ICT. This ministry is spearheading the e-government program in Uganda. It is in charge of creating the necessary policy coordination and harmonization. Below it is the National Information Technology Authority-Uganda that initiates and leads development of the national e-government strategies and implementation plans. Ministry of Public Service is charge of public services process review, computerization and business process reengineering activities for efficient service delivery and finally are the government Ministries, Agencies and Local governments to implement respective institutional ICT strategies and action plans in harmony with the overall national ICT Policy and government Master Plan.

2.5.1 Issues of E-Government Adoption in Uganda

Worldwide challenges to e-government adoption to mention but a few include view of technology in a deterministic fashion, lack of sufficient levels of critical resources for e-Government service provision, the digital divide barrier and information security in itself (Gant, 2008). Identified are two challenges to citizens, their willingness to adopt and use the online service and ability of the government to implement e-Government to match the needs of the citizen with the technical challenge as the ability to combine computer-based technologies with human-based administrative processes to create new ways of serving citizens (Gant, 2008).

Uganda has 3,200,000 of Africa's 110,931,700 internet users (Internet World Stats, 2010). However this is not representative of those using it for e-government. Not everyone using Internet uses it to access government services (Al-adawi *et al*., 2005). Uganda's e-government development index as of 2010 was at 0.2812 which is still not so good a performance with Uganda's position at 142 (UN, 2010). As a developing country, Uganda has a per capita gross national product less than USD$ 2,000 (Ball, 1990; Alfawaz *et al*., 2008). Online government services adoption as well as usage is of a special significance for developing countries which have a problem of shortage of resources because online services increase accessibility and bring time and cost savings to citizens. They also provide transparency built in the online channel alleviating corruption, a serious problem in a number of developing countries (Kumar *et al*., 2007). Usage of online government services by countries depends on those with a high per capita gross domestic product, more competitive, less restricted ICT environment, those spending more money on ICT and having better access to Internet (Al-adawi *et al*., 2005).

To facilitate e-government, Uganda formulated the e-government strategy in 2004 and set up numerous ICT projects in various sectors of Ugandan society with the help of donor agencies (UNESCO, 2005; Rwangoga & Baryayetunga, 2007). E-government platform is being deployed with projected benefits of increased transparency of government activities and enabling of government departments to share public data and enhance interdepartmental coordination thereby reducing costs and generally improving work efficiency (Huawei, 2010). This e-government platform deployment is however already facing challenges such as minimal use with application of most ICT investments still basic like computers being used as word processors (MoICT, 2010b). Therefore needed is a thorough understanding of these challenges and the different issues they impose as regards to e-government adoption for them to be effectively addressed with measures suitable for the study area.

There is need to understand the environment of Uganda as a country and to gain insight of its cultural dimension encompassing both the national and organizational culture in order to appreciate addressing e-government adoption from the information security perspective (Alfawaz *et al*., 2008). Implementation and adoption of e-government in a country requires an environment that is conducive to realize its potential for development (UNESCO, 2005). This is assessed through a country's e-readiness and how well prepared a country is for adoption of e-government. Uganda was ranked at position 143 with an e-government development index of 0.3185 with the East African region having a sub-regional average e-government development index of 0.3011 and the overall world average at 0.4882 (UN, 2012). Alfawaz *et al*. (2008) stated that the key aspect in e-government adoption process in a country's context, is where the phenomenon is to be deployed and where it is to operate. There is therefore need for a detailed understanding of the problems in e-government adoption for them to be effectively addressed for its success.

The problems hindering successful e-government adoption in Uganda include inadequacy in the supporting legal framework both international and national, persistent poor information security awareness and security culture, difficulty in attracting, recruiting as well as retaining skilled staff and inadequacy in the review of business processes for efficient application of electronic government processes as well as applications to mention but a few (Rwangoga & Baryayetunga, 2007; MoICT, 2011). These problems have been worsened by the continued creation of new

districts which increases administrative units yet already existing resources are limited, with the new created districts having to depend on the mother districts for effective operation.

A major problem in e-government adoption in Uganda just like elsewhere globally is information security. According to a nationwide survey of local e-government conducted by the International City/County Management Association (ICMA), USA in 2004 on the barriers to e-government adoption, the rating of security issues was at 37%, privacy issues at 29% as reported by between a quarter and a third of respondents (Coursey & Norris, 2008). With the increased reliance on open data networks for e-government adoption, information security has become one of the most crucial success factors to consider for both public and private organizations (Alfawaz *et al*., 2008).

Along with increased use and reliance on ICTs by government comes increased risk of cyber attacks, other IT security threats and the need to ensure security of information during e-government transactions. Although there is increasing awareness and consciousness of this security problem in Uganda, little is still known about the actual issues involved in securing networks, information and electronic assets with many people considering anti-virus software for defending against viruses as the cure of all varieties of information security threats (MoICT, 2011). Despite the efforts by government to implement information security management, this has not yielded much benefit with these efforts frustrated by existence of weaknesses like inadequate standards and maturity models adopted in the area of information security, inadequate budgetary allocations, roll out of ICT infrastructure not being standard across government, lack of a cyber security specialist center and PKI infrastructure (MoICT, 2011). Yet the danger of cyber crime is of far greater consequence for example theft of sensitive information through online access, erasing of backup files which can affect the operations of an entire organization. Addressing this information security problem requires a national information security strategy in order to safeguard and ensure business continuity management in ICT use and application in service delivery (MoICT, 2011).

While ICTs in Uganda have been identified as a major tool for achieving socio-economic development, the success and benefits of the ICT initiatives in the governments' implementation of long-term national development programs is dependent on the availability of timely, relevant information at all levels of implementation (Rwangoga & Baryayetunga, 2007). Uganda is still

performing poorly in as regards to the e-government transactional stage which involves a two way communication and deals directly with information exchange. In as regards to this transactional e-government service provision level, performance is at 0% (UN, 2010). In a bid to improve this situation to meet the need for exchange and communication of Information and to lay a solid foundation for future service evolution, Uganda government through Huawei is implementing the Uganda e-government project (Huawei, 2010). This is to enable timely, relevant information availability at all levels.

However for users to trust the e-government system, information quality in terms of its currency, accuracy, relevance and validity becomes a crucial factor to consider (Tassabehji, 2005). This necessitates addressing the issue of security of this information. Applying information security principles in an e-government environment is a complex, multidimensional issue involving people, processes and technology and the underlying problem of information security and e-government is deeper than specifics of individual data losses (Conklin, 2007). Therefore critical analysis as well as evaluation of e-government adoption problems in Uganda provided the information needed to answer the question of which conceptual model to develop that solves the above problems and is best suited for advancing e-government adoption in Uganda from an information security perspective. The following Table 2.3 shows the above issues that are general and specific to e-government adoption in Uganda

Table 2. 3: Summary of Issues for the E-Government Adoption Process in Uganda

	General Issues	**Issues Specific to Uganda**
Issues of e-government adoption in Uganda	Lack of critical resources for e-government services provision	Country's context and environment where e-government is to be deployed and operate.
	Digital divide barrier	Inadequacy in supporting legal framework both international and national
	View of technology in a non deterministic fashion.	Persistent poor information security awareness
	Information security	Poor security culture
	Users willingness to adopt and use the online services	Difficulty in recruiting and training skilled staff
	Government's ability to implement e-government that matches needs of users	Increasing district units yet existing resources are already limited.
	Inadequacy in review of business processes hence mismatch during implementation	Inadequate budgetary allocation to information security management
	Increased risk of cyber attacks	Inadequacy of existing information security model
	Security issues	Lack of a cyber security specialist center and PKI infrastructure
	Privacy issues	Rollout of ICT infrastructure is not standard across government

As seen in table 2.3 above for success to be attained in e-government adoption, the following issues of e-government adoption in Uganda need to be addressed. The general issues to include i) Lack of critical resources for e-government services provision ii) Digital divide barrier iii) View of technology in a non deterministic fashion iv) Information security v) Users willingness to adopt and use the online services vi) Government's ability to implement e-government that matches needs of users vii) Inadequacy in review of business processes hence mismatch during implementation viii) Increased risk of cyber attacks ix) Security issues x) Privacy issues

The challenges specific to e-government adoption in Uganda should also be addressed to include i) Country's context and environment where e-government is to be deployed and operate ii) Inadequacy in supporting legal framework both international and national iii) Persistent poor information security awareness iv) Poor security culture v) Difficulty in recruiting and training skilled staff vi) Increasing district units yet existing resources are already limited vii) Inadequate budgetary allocation to information security management viii) Inadequacy of existing information security model ix) Lack of a cyber security specialist center and PKI infrastructure x) Rollout of ICT infrastructure is not standard across government.

There has been little effort to address the issue of information security despite the fact that it is vital for e-government adoption (Tassabehji, 2005; MoICT, 2011). Even existing adoption models don't wholly address the aspect of information security (Löfstedt, 2005; Alfawaz *et al*., 2008). In Uganda, there is lack of an appropriate information security e-government adoption model to guide in successful e-government adoption and even existing models are more suited to developed countries. Information security when incorporated into e-government adoption has the potential to influence users' privacy, trust, confidence and security which impact on their willingness to adopt the e-government system (Tassabehji, 2005). This can however only be achieved if information security is incorporated into an e-government adoption model described, suitable to guide the adoption process in Uganda.

2.6 A Conceptual Model for the E-Government Adoption Process

The conceptual model selected for use adopts from Bwalya & Healy's (2010) model as an important theoretical base to address the issue of information security in the e-government adoption process for Uganda. Bwalya & Healy's (2010) model is based on Davis' TAM (1989) that has Perceived Ease of Use and Perceived Usefulness as the main constructs influencing the attitude of a user toward a system. Bwalya & Healy's (2010) model suggested that ICT infrastructure plus lower access costs, local and English language, risks, local culture, data privacy and security, and continued user support and legal, regulatory plus institutional frameworks together with the main constructs of TAM influence e-government adoption process and the continuance use of e-government. Information security, security culture and trust also

explain the relationship between information security and the e-government adoption process in the study context. The following is an outline of the conceptual model used.

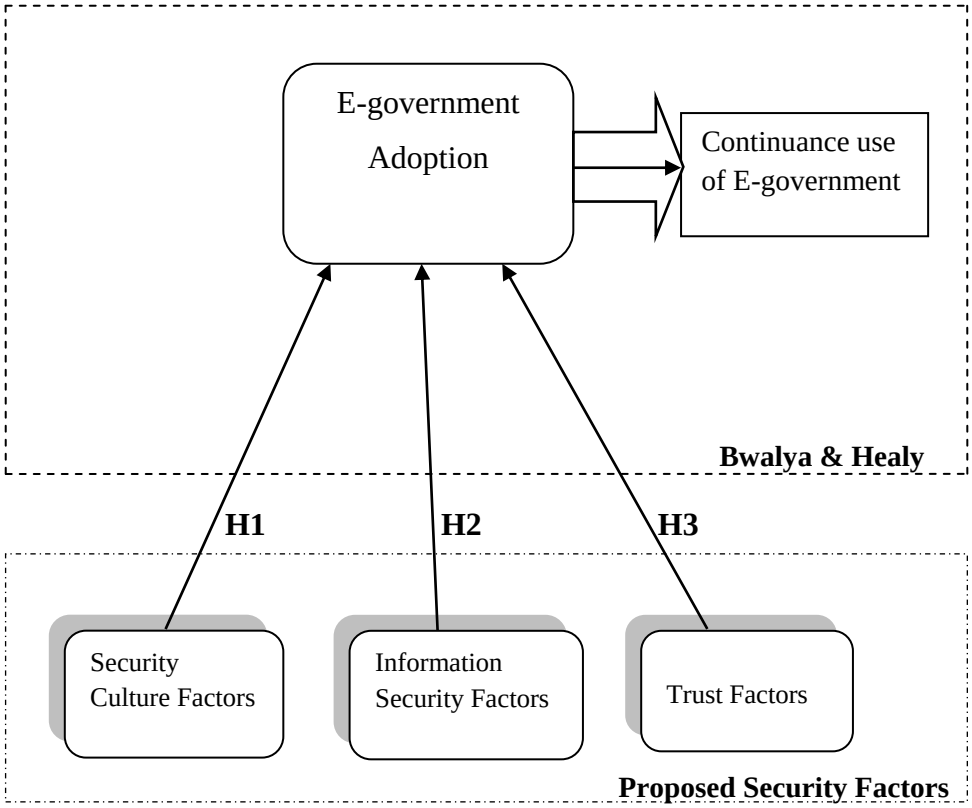

Figure 2. 9: The Conceptual Information Security E-government Adoption Process Model

This section now provides the description of the constructs, the relationships and the theoretical explanation for their inclusion in the conceptual model above. The constructs described in the model are security culture factors, information security factors, trust factors, e-government adoption and continuance use of e-government.

Security Culture Factors

Security culture is a new construct that was added. This represents the prevailing attitude towards approaches to a secure e-environment and they contain the variables: organization's culture, national culture and regulations and laws (Alfawaz *et al*., 2008). (Ibid) incorporated the security culture construct identifying the national culture, organizational culture and the security practices in the organizational culture (Vroom, 2004; Chang and Ho, 2006 Chaula, 2006; Chang, 2007; Ruighaver *et al*., 2007) into security culture factors. According to their study, these factors may

tend to reinforce resistance to technology such as e-government and contribute to lack of compliance to the measures and controls in place to safeguard the information assets and ensure information security. In this study security culture factors are measured by the security practices in e-government in terms of information security awareness campaigns, supporting legislation, suitable security & privacy policies and Skills Training (Tassabehji, 2005; Alfawaz *et al*., 2008; MoICT, 2011).

Information Security

Information security is another new integrated factor. This is the process, by which the government protects and secures its systems, media and facilities that maintain information vital to its operations with security, as an ongoing procedure and not a state at a point in time (FFIEC, 2006). The information security process is made up of management of information security, network security, computer and data security. Several studies suggest that information security is an important factor for e-government and is a management responsibility (Löfstedt, 2005; Conklin, 2007; Alfawaz *et al*., 2008). Löfstedt (2005) identified the properties that make up information security as availability, confidentiality, integrity, information assurance and accountability. In this study information security is measured in terms of the ability to satisfy the properties of confidentiality/ privacy, integrity, accountability and trust in e-government systems (Tassabehji, 2005).

Trust

Trust is also a new factor identified in the study. Trust is defined as the expectation that the promise of an individual or group can be relied upon and contains two variables: trust of the internet and trust of the government Rotter's study (as cited in Belanger & Carter, 2008). Tassabehji (2005) incorporated the construct of trust identifying privacy of information and citizens, security of online interactions, confidence in e-government services, freedom from unwanted government intrusion information as trust factors (Plexico 2000; Shetty 2002; Anon 2003; Clark; 2003). In this study trust is measured in terms of security of the e-government system. Assuring e-government users that their privacy and security concerns have been addressed to enable information accuracy, reliability, relevancy, and the systems provided are easy to use ensures information security. This causes them to have confidence and trust in the provided e-services which in turn affect their participation and adoption of provided e-

government services. Trust was found to positively influence intention to use an e-government service (Belanger & Carter, 2008).

E-Government Adoption

E-government Adoption is the intention to use e-government services Belanger and Carters' study (as cited in Anthopoulose *et al*., 2010). Colesca & Dobrica (2008) identify three factors that make up e-government adoption: willingness to use, intent to use and frequency of use. According to this study, understanding the factors that cause e-government adoption and acceptance would be of great value for the successful deployment of e-government services. Kumar *et al*. (2007) included the construct of e-government adoption identifying willingness to use and intent to use (Gilbert and Balestrini, 2004; Carter and Bélanger, 2005) into the factor of e-government adoption. These studies address e-government adoption in terms of adoption to innovation and behavioral aspect. Bwalya & Healy (2010) claim that appropriate e-government adoption framework will positively impact on continuance use of e-government. To have an appropriate adoption framework it is necessary that all the factors affecting the adoption process be integrated. The current study addresses e-government adoption in terms of information security that is the relationship between information security and intent to use e-government services such as e-tax, e-health, e-mail, e-voting, e-banking as well as the continuance use of these services.

Continuance Use of E-government

This is the continued use of the provided e-government system. Appropriateness of the e-government adoption framework will affect continuance use of e-government. As users engage in, participate and adopt the e-government system, a long term trust relationship is developed between government and the users of the provided e-services. Based on the trust relationship, employees will adopt and continue using e-government services provided. The study thus suggests that an appropriate e-government adoption framework will positively impact on continuance use of e-government (Bwalya & Healy, 2010).

The Relationships in the Model

Information security determines the trust of users for the provided e-government systems, how they are to perceive the e-government services and what their intentions are with regard to

accepting and using all aspects of e-government services and operations provided. From the conceptual model in figure 2.7, to address e-government adoption process in Uganda requires answering questions about the following: What are the information security factors that affect adoption of e-government in Uganda? How can security of e-government services be improved to increase public trust hence adoption of e-government? Addressing these questions helps to: i) determine the information security factors affecting the e-government adoption process in Uganda, ii) develop a model for e-government adoption relating the information security factors to the adoption process in the Ugandan context iii) explain the importance of the factors to the adoption process.

In the conceptual model these questions are tested for using the following assumed relationships H1, H2, and H3.

1) **H1:** Security culture factors are related to the adoption of e-government services and systems in Uganda.

2) **H2:** Information security factors have a relationship with the adoption of e-government services and systems in Uganda.

3) **H3:** Trust factors are related to and help to predict the e-government adoption process in Uganda.

Testing these relationships as suggested enables the development of a model suitable for predicting the successful adoption of e-government services from an information security perspective in the Ugandan context.

CHAPTER THREE

Methodology

3.1 Introduction

The previous chapter reviewed literature related to the problem of study on e-government adoption and information security. This chapter now presents the research strategy, design, methods and techniques that were used during the study in order to answer the research questions. Included in this chapter is also an explanation of how the selection of the methods and techniques used for data collection and analysis was achieved. A research design in this study is what was used to structure the research, how all main parts of the research project worked together to try and address the central research questions (Trochim, 2006). A field survey was used in this study to collect data about the requirements for e-government adoption from an information security perspective in Uganda in order to develop the model. This chapter also includes the methods that were used to develop the model as well as its evaluation.

3.2 Methods of Research

The types of methods of inquiry to research design and data collection used in carrying out research operations are many with the common approaches including quantitative, qualitative and mixed methods as explained below (Myers, 1997; Williams, 2007). In this section quantitative and qualitative research methods as well as their strengths and weaknesses are explained in order to show how the mixed method was selected for use in the study.

3.2.1 Quantitative Research Methods

This refers to inquiry based in the assumption that features of the social environment constitute an objective reality that is relatively constant across time and settings. To describe and explain features of this reality the main method used was to collect numerical data on observable behaviors of samples by subjecting these data to statistical analysis Gall *et al*.,'s study (as cited in Hart *et al*., 2009). The broad classifications of the quantitative research methods include descriptive research, experimental, quasi-experimental and finally causal comparative (Williams,

2007: Hart *et al*., 2009). Data collection techniques for quantitative research methods include survey, observation and questionnaires. Quantitative research methods have strengths and weaknesses (Johnson & Onwuegbuzie, 2004). These include:

Strengths

- Tests and validates already constructed theories about how and why phenomena occur
- Tests hypotheses that are constructed before the data are collected
- Can generalize research findings when the data are based on random samples of sufficient size
- Can generalize a research finding when it has been replicated on many different populations and subpopulations
- Is useful for obtaining data that allow quantitative predictions to be made
- One may construct a situation that eliminates the confusing influence of many variables, allowing to establish one or more credible cause-and-effect relationships
- Data collection using some quantitative methods is relatively quick (e.g. interviews)
- Provide precise, quantitative numerical data
- Data analysis is relatively less time consuming (using statistical software)
- The results are relatively independent of the researcher (e.g. statistical significance)
- May have higher credibility with many people in power (e.g. administrators)
- Is useful for studying larger numbers of people

Weaknesses

- The categories used might not reflect local constituencies' understandings
- The theories used might not reflect local constituencies' understandings
- The researcher might miss out on phenomena occurring because of focus on theory or hypothesis testing rather than on theory or hypothesis generation (confirmation bias)
- Knowledge produced might be too abstract and general for direct application to specific local situations, contexts and individuals

3.2.2 Qualitative Research Methods

This refers to investigation based in the assumption that individuals make social reality in the form of meanings plus interpretations and that these creations tend to be temporary and situational, so to discover these meanings as well as the interpretations this method was conducted by studying cases intensively in natural settings and subjecting the resulting data to analytical induction Gall *et al.*,'s study (as cited in Hart *et al.*, 2009; Joubish *et al.*, 2011). Qualitative research methods include case, ethnography, grounded theory, phenomenological studies and content analysis (Williams, 2007; Joubish *et al.*, 2011). Examples of qualitative research data collection techniques include interviews, observations and document analysis. Qualitative research methods have strengths and weaknesses (Johnson & Onwuegbuzie, 2004). These include:

Strengths

- Data is based on the participants' own categories of meaning
- Is useful for studying a limited number of cases in depth
- Is useful for describing complex phenomena
- Provides understanding and description of people's personal experiences of phenomena (i.e. insider's viewpoint)
- Can describe in rich detail phenomena as they are situated and embedded in local contexts
- The researcher almost always identifies contextual and setting factors as they relate to the phenomenon of interest
- The researcher can study dynamic processes (i.e. change)
- The researcher can use the primarily qualitative method of grounded theory to inductively generate a tentative but explanatory theory about a phenomenon
- Can determine how participants interpret constructs (e.g. self-esteem)
- Data are usually collected in naturalistic settings in qualitative research
- Qualitative approaches are especially responsive to local situations, conditions and stakeholders' needs
- Qualitative researchers are especially responsive to changes that occur during the conduct of a study and may shift the focus of their studies as a result

- Qualitative data in the words and categories of participants lend themselves to exploring how and why phenomena occur
- Can use an important case to vividly demonstrate a phenomenon to the readers of a report
- Determines idiographic causation (i.e. determination of causes of a particular event)

Weaknesses

- Knowledge produced might not generalize to other people or other settings (i.e. findings might be unique to the relatively few people included in the research study)
- It is difficult to make quantitative predictions
- It is more difficult to test hypotheses and theories with large participant pools
- It might have lower credibility with some administrators and commissioners of programs
- It generally takes more time to collect data when compared to quantitative research
- Data analysis is often time consuming
- The results are more easily influenced by the researcher's personal biases and idiosyncrasies

3.2.3 Mixed Research Methods

These are methods where both quantitative and qualitative data were collected concurrently or sequentially and given priority in a single study and it involved integration of the data at one or more stages in the process of research Creswell *et al*.,'s study (as cited in Hanson *et al*., 2005; Hayes *et al*., 2013). Hanson *et al*. (2005) states that mixed methods research, is viewed as a method allowing researchers to use any number of theoretical foundations for its justification and use. Therefore the best paradigm for use in the research study was determined by the researcher and the research problem and not by the method. Based on the use of explicit theoretical lens, approach of implementation, priority given to qualitative and quantitative data, stage of data analysis and integration and procedural information, there are two major mixed methods research design classifications, time order that is concurrent versus sequential and paradigm emphasis to include equal status versus dominant status (Johnson & Onwuegbuzie, 2004; Hanson *et al*., 2005; Hayes *et al*., 2013). Mixed methods research has strengths and weaknesses (Johnson & Onwuegbuzie, 2004). These include:

Strengths

- Words, pictures and narratives can be used to add meaning to numbers
- Numbers can be used to add precision to words, pictures and narrative.
- Can provide quantitative and qualitative research strengths
- The researcher can generate and test a grounded theory
- Can answer a broader and more complete range of research questions because the researcher is not confined to a single method or approach
- Specific mixed research designs have specific strengths and weaknesses that should be considered for example the phase one results can be used to develop and inform the purpose and design of the phase two component
- The strengths of an additional method can be used to overcome the weaknesses in another method by using both in a research study (Complementarity)
- Can provide stronger evidence for a conclusion through convergence and corroboration of findings (triangulation)
- Can add insights and understanding that might be missed when only a single method is used
- Can be used to increase the generalizing of the results
- Qualitative and quantitative research used together produces more complete knowledge necessary to inform theory and practice.

Weaknesses

- It can be difficult for a single researcher to carry out both qualitative and quantitative research, especially if two or more approaches are expected to be done concurrently.
- The researcher has to learn about multiple methods and approaches and understand how to approximately mix them
- Methodological purists contend that one should always work within either a qualitative or a quantitative paradigm
- Is more expensive and time consuming
- Some of the details of mixed research remain to be fully worked out by research methodologists (e.g. how to interpret conflicting results)

Due to quantitative research methods weaknesses to include (focus on theory testing rather than generation and knowledge produced being abstract and general for direct application) and qualitative research methods weaknesses (difficulty to make quantitative predictions, difficulty to test hypotheses with large participants and data analysis is often time consuming), mixed methods research was used in the study. This is because use of mixed methods research combined strengths of both qualitative and quantitative methods and reduced on their weaknesses to include (using both methods in the research study which enabled complementary understanding of the research problem(Complementarity), using both words and numbers which enabled meaning and precision to be added to numbers, words, pictures and narrative, it enabled adequate answering of the different research questions, increased generalizing of results and produced more complete knowledge necessary to inform theory and practice.)

Therefore based on the research problem and the research questions, the mixed methods approach was used where the field survey quantitative and the case study qualitative methods were used concurrently. Questionnaires, observation, interview and document analysis techniques were used for data collection to elicit the requirements needed for model development with inductive logic used for reasoning the obtained data. First research questions were used to collect requirements for developing the information security e-government adoption model, followed by the pattern stage where the collected requirements were analyzed using SPSS software package to obtain the information security factors for use to develop the model in the provisional hypothesis stage and then the developed model was evaluated using correlation and regression analyses so as to resolve the research problem under study appropriately (Burney and Mahmood, 2006; Williams, 2007). The mixed method research process has nine (9) steps in its implementation which were followed during the study. The order of steps is not static as can vary from study to study depending on needs and concerns arising during the study. Data interpretation and validation are done throughout the data collection process (Wilkins and Woodgate, 2008). These steps were used for the study in order to obtain information on information security and e-government adoption in Uganda as follows:

Step1. Define the research problem and appropriateness of mixed methods research for the problem: The research problem the lack of an appropriate information security e-government adoption model to guide the government in successful e-government adoption in Uganda was

derived from literature review in information security, e-government adoption and implementation (Conklin, 2007; Mivule & Turner, 2011; MoICT, 2011; Wangwe *et al*., 2012; Olupot & Mayoka, 2013). This is because existing models do not emphasis the aspect of information security in e-government adoption and are not suited for developing countries like Uganda. Of these studies, Conklin (2007) identified information security as an area for further research. Olupot & Mayoka (2013) identify improvement of information security as a requirement for e-government adoption in Uganda. Mivule & Turner (2011) stated that there is no national technological framework on data privacy. Wangwe *et al*. (2012, p.11) state that there is no national information security framework that has been adopted in the East African countries, Uganda inclusive. In Uganda information security maturity growth is determined based on the methodology ISM^3 (Information Security Management Maturity Model) and according to this methodology Uganda's rating is at level 1 with security not acknowledged as a desirable property of the organization (MoICT, 2011).The research problem (the lack of an appropriate information security e-government adoption model to guide the government in successful e-government adoption in Uganda) was thus defined and used to formulate the research questions what information security factors and how to improve security of e-government services for e-government adoption. Based on the nature of the problem mixed methods research was used since use of a single method was insufficient to determine the requirements (information security factors) and their relationship to e-government so as to develop an information security e-government adoption model for Uganda. These questions guided the study and enabled attainment of the study objective.

Step2. Determine the rationale for conducting mixed methods research: There are five rationales for conducting mixed methods research to include triangulation which corroborates results from different methods and designs studying the same phenomenon, Complementarity which seeks to elaborate on results from one method with results from the other method, development which uses findings from one method to help inform the other method, expansion which extends the breadth and range of research by using different methods for different inquiry components and initiation which recasts results from one method to questions or results from the other method (Hanson *et al*., 2005; Onwuegbuzie *et al*., 2012). Complementarity rationale was used for the study which enabled results from one method quantitative data (requirements) to complement on results from another qualitative data (document analysis of reports like National electronic

government framework, National information security strategy for Uganda, observation and interviews and to be incorporated into the model as requirements). Use of Complementarity perspective helped clarify, ehance and explain on the results Bryman's study (as cited in Wilkins & Wood gate, 2008).

Step3. Select a mixed methods research design: There are two major mixed methods research designs. Sequential designs where quantitative data are collected and analyzed followed by qualitative data with priority usually unequal and the concurrent designs where quantitative and qualitative data are collected and analyzed at the same time with priority usually equal (Hanson *et al*., 2005). In this research concurrent research design was used where quantitative and qualitative data were collected and analyzed at the same time and the data transformed during data analysis. The concurrent design was used because it enabled better addressing of the study aim, research questions and gaining a broader perspective of the study topic (Hanson *et al*., 2005).

Step4. Select the Sample: The sampling process included purposive selection of the units of 2 districts (Mbale and Sironko) and 2 government ministries (ICT and Local government ministries) with the government employees working in these units identified as the target group. These employees were selected because they are at the forefront of using the adopted e-government services in Uganda. The population was then stratified into 2 (departmental heads and staff) to participate in the study. The total number of employees working in these four units was established followed by a selection of items from each stratum. Based on precision rate (0.05) and confidence level (95%), the sample size was drawn. The study used both purposive and stratified sampling techniques because of the concurrent design used and the relative advantage inherent in this method of sampling (Creswell, 2007). Therefore the sample size representative of the study population that was used for the study was determined.

Step5. Collect the data: Data collection procedures depend on the type of mixed methods research design used Creswell's study (as cited in Wilkins & Wood gate, 2008). Based on the concurrent design used, quantitative and quantitative data were collected simultaneously. Quantitative data was collected through semi-structured close ended questionnaires and a likert rating scale with scores 1-5 assigned to each of the statements in the questionnaire qualitatively describing information security factors for e-government services adoption. Qualitative data was collected through gathering documentary materials and statistical figures relating to the study areas and

their e-government setup to include the National Information Security Strategy for Uganda (2011), United Nations E-government Survey (2012), National Electronic government framework for Uganda (2010) and observation of participants as well as their interaction with the e-government system in the district sites. The questionnaire was tested using a pilot survey and the experience gained was used to make the final questionnaire that was used for data collection during the field survey Kroll *et al's*., study (as cited in Wilkins & Wood gate, 2008). Using the above methods (both quantitative and qualitative) data was thus collected and used in the study so as to develop the information security model.

Step6. Analyze the data: Responses from the completed questionnaire were analyzed using the mixed methods data analysis techniques. This was achieved by incorporating into the mixed methods process the mixed methods data analysis process that involves seven steps data reduction, data display, data transformation, data correlation, data consolidation, data comparison and data integration (Onwuegbuzie & Leech, 2006). The responses from the questionnaire were coded (content driven coding) with each response per question labeled with a code that suggested how the associated response informs the research objectives and these represented the identified themes Q1. Total number of respondents per sector Q2. Mode of e-government services used Q3. Frequency of using electronic government services Q4. Security factors for e-government systems (A. confidentiality in e-government services B. Integrity in e-government services C. Accountability for e-government systems D. Trust in e-government services E. Security culture in e-government services) and Q5 Responses were arranged according to the above categories. These categories were used for further analysis.

i Data reduction involved reducing the dimensionality of the quantitative and qualitative data. Quantitative data was analyzed using Statistical Package for Social Scientists software (SPSS)13.0 using factor analysis, descriptive statistics and Microsoft excel for the grouped data categories above. Qualitative data was analyzed using exploratory thematic analysis and inductive logic so as to collect and analyze requirements so as to be able to develop the model and evaluate it. This also included identifying and comparing codes co-occurance, relationship then identifying and describing data using the above themes (Wilkins & Wood gate, 2008).

ii Data display was achieved by use of graphs, Venn diagram for qualitative data and tables, graphs for quantitative data.

iii Data transformation involved transforming quantitative data into the above identified themes (narrative data) and this was achieved by converting quantitative data into qualitative data.

iv Data correlation was done by (Pearson's correlation coefficient and multiple regression analysis computed using SPSS 13.0) and this enabled correlating of the quantitative transformed data into the themes and qualitative data.

v Data consolidation was carried out by combining both quantitative and qualitative data to attain the consolidated variables (requirements).

vi Data comparison was done by comparing quantitative data, requirements from questionnaire (QI, Q2, Q3, Q4 compared with the qualitative from Q5) as well as qualitative data sources such as (documents, previous studies and statistical figures relating to the study areas and observation done during the field survey).

vii Data integration the final stage was achieved by integrating the quantitative data from the field survey (QI, Q2, Q3, Q4) and qualitative data Q5 and data from (documents, reports, statistical figures like results from correlation and regression analyses and observation), into final requirements (information security factors) which were incorporated into the model to develop the information security e-government adoption model for Uganda.

For QI, Q2, Q3, Q4 data reduction was done using SPSS 13.0, descriptive statistics and Microsoft excel as per the themes (number of respondents per sector, mode of e-government services used, frequency of using electronic government services, security factors for e-government systems (A. confidentiality in e-government services B. Integrity in e-government services C. Accountability for e-government systems D. Trust in e-government services E. Security culture in e-government services) respectively and Q5 exploratory thematic analysis as per the themes. The data was displayed using percentages for Q1, Q2 graph, Q3 Venn diagram Q4 and Q5 tables and graphs. Data from QI, Q2, Q3, Q4 was transformed correlated and compared with the qualitative data and data from Q5. The quantitative data (QI, Q2, Q3, Q4) and qualitative data plus data from Q5 were integrated into the final requirements (qualitative data of information security factors) and

incorporated into the model thereby enabling development of the information security e-government adoption model.

Step7. Interpret the data: Data interpretation began at the data collection stage and continued throughout the study Creswell's study (as cited in Wilkins & Wood gate, 2008). To achieve this integration and comparison of the quantitative and qualitative findings was done. Convergence of the findings strengthened the conclusions (Wilkins & Wood gate, 2008). Meaningful inferences were then made from the combined quantitative (requirements) and qualitative findings (incorporated into the model). Interpretation of the data analysis done was that quantitative and qualitative data supported the finding that information security factors affect the e-government adoption process in Uganda.

Step8. Validate the data: Data validation involved assessing trustworthiness of the data and the developed model Creswell's study (as cited in Wilkins & Wood gate, 2008; Venkatesh *et al*., 2012-2013). Validity of data and the instrument was done using Cronbach's alpha for instrument reliability, pilot study for content validity and SPSS 13.0 using factor analysis for construct validity (Al-Shafi & Weerakkody, 2010). Evaluation of the model was done using correlation and regression analyses and this confirmed the suggested relationships between variables in the model. Validation enabled confidence to be attained in the findings and the model to be authenticated.

Step9. Report the findings: The report writing step started at the beginning of the research process. To report the findings of the study the dissertation was written with the findings presented in form of five chapters with chapter 1 as introduction to the study, chapter 2 literature review on the main concepts of information security and e-government adoption, chapter 3 the methodology used to investigate the study problem so as to answer the research questions and achieve the study objectives, chapter 4 data analysis and results description and chapter 5 discussion of results and conclusions.

3.3 Research Strategy

The research strategy discussed here in detail shows how the method of reasoning used in addressing this research study in order to answer the research questions was selected. Research strategy refers to approaches to research or the plan to be used in resolving the research study.

There are two broad methods or logic employed in reasoning research in order to resolve the research, study, deductive and inductive approaches (Burney and Mahmood, 2006).

3.3.1 Deductive Research Strategy

This is reasoning that works from the more general to the more specific observations and theories (Burney & Mahmood, 2006; Trochim, 2006). This logic aims at hypothesis testing as it begins with the idea and uses the data to confirm or negate the idea. It is a knowledge driven reasoning (Skinner, 2005). Deductive reasoning is a top down approach in form of a waterfall and there is a general use of arguments based on laws, rules and accepted principles in this logic (Burney and Mahmood, 2006). This logic is narrower in nature. In this approach, the first step is to think up a theory that needs to be tested, the next step is data collection, followed by testing the hypothesis and finally confirmation or modification of the theory (Trochim, 2006).

3.3.2 Inductive Research Strategy

This is a research approach that works moving from specific observations to broader generalizations and theories (Burney & Mahmood, 2006; Trochim, 2006). This logic aims at hypothesis generating as it uses the data to generate ideas. This reasoning is feature detecting (Skinner, 2005). Also referred to as a bottom up approach, inductive reasoning is a hill climbing approach. This logic is used in qualitative data and exploratory open ended questions. Inductive research strategy works the other way round to deductive research, moving from specific observations to broader generalizations and theories.

To integrate information security into an e-government adoption model, inductive logic was used. This was done following the four steps of inductive reasoning observation, pattern, tentative hypothesis and theory. The first step included use of observation and questions to collect data to generate requirements for developing the information security e-government adoption model, this stage was followed by the pattern stage where quantitative data was transformed and integrated into qualitative data during analysis and the collected requirements were analyzed using SPSS software to obtain the information security factors for use to develop the information security model in the provisional hypothesis stage and then finally the developed model was evaluated using correlation and regression analyses (Trochim, 2006). Use of inductive reasoning provided

the researcher with new ideas and enabled expansion of the researcher's knowledge about the study area in a way that is impossible for deductive reasoning to achieve.

3.3.3 Retroductive Research Strategy

This is the logic of conclusion adopted by critical realism and as a research strategy this can provide the basis upon which different insights upon the same occurrence can be sensibly combined thus having the potential to unite aspects of different traditions of economic and social thought (Downward and Mearman, 2007). This is a hypothesis formulation strategy and it occurs in the context of theoretical assumptions. This strategy involves making hypothesis that appear to explain what has been observed, in that the occurrence is observed and then a claim is made of what it was that gave rise to the occurrence. This strategy differs from inductive in that whereas inductive strategy concludes from one set of facts to another set of facts, retroductive strategy concludes from facts of one kind to facts of another. Although theoretical concerns and kind of research question being asked usually determine the dissimilar research approach to be used, in practice however both approaches are involved in research in a circular sort of way where theory leads to observations which in turn lead to identification of new patterns and this leads to development of new theories (Skinner, 2005).

3.4 The Research Design for the Study

Quantitative methods were used to determine the information security factors affecting the adoption process and this was done during the field survey. Quantitative data collected using the questionnaire was transformed and integrated into qualitative data during data analysis to obtain requirements for developing the model (Hanson *et al*., 2005).

Qualitative methods were used to incorporate information security into the e-government model and this was done by using the collected data from the field survey about the requirements. The textural (narrative) data collected was described, explained and interpreted with inductive reasoning used in order to solve the research questions (Williams, 2007). Inductive reasoning was used because it enabled understanding the study context and for the researcher to be part of the study process thereby enabling adequate answering of the research questions.

Under this section is the whole structure of how the research was carried out so as to address the research questions. The research approach selected for use is usually determined by the kind of research question that is asked and theoretical concerns (Skinner, 2005). The research questions in particular provided a framework for conducting this study as they give rise to the type of data that was eventually collected (Onwuegbuzie and Leech, 2006). The research questions of the study are restated below.

i. What are the information security factors that affect adoption of e-government in Uganda?
ii. How can security of e-government services be improved to increase public trust hence adoption of e-government?

Research question (i) was answered using the field survey with questionnaires used to determine the requirements (InfoSec factors).

Research question (ii) was answered qualitatively using requirements from (i) to develop a model for e-government adoption relating the information security factors to the adoption process by extending an existing one.

The research problem is the lack of an appropriate information security e-government adoption model to guide the government in successful e-government adoption in Uganda. This is because the existing models do not incorporate information security and are more suited to developed countries than developing countries like Uganda. Basing on the nature of the research problem and questions, a mixed methods research approach combining both qualitative and quantitative methods was used. The selected design was QUAN + QUAL equal status concurrent design (quantitative and qualitative data collected at the same time) to answer the research questions to the study in order to attain the stated objectives requiring both numerical and textural or narrative data (words). Mixed research methods, was the selected approach because it provided several advantages over use of only quantitative or qualitative research methods to include:

Mixed methods provided the researcher with the ability to design a single study that answers the research questions about both the complex nature of information security and e-government adoption from the researcher's view point and the relationship between the measurable variables of information security and e-government (William, 2007).

Use of mixed methods helped the researcher to draw from the strengths and minimize the weaknesses of the quantitative and qualitative research approaches (Johnson & Onwuegbuzie, 2004; Hayes *et al*., 2013). Mixed methods helped the investigator to research the study problem from all sides (requiring quantitative and qualitative results). This enabled the results from one type of research quantitative (requirements) to be complemented with another qualitative (incorporated into the model) thereby providing a better understanding of the research problem.

For quantitative research methods the field survey was used with questionnaires as the main data collection method for use in the field. Quantitative data collected was transformed and integrated into qualitative data during data analysis to determine requirements (InfoSec factors). Use of quantitative methods enabled requirements to be obtained so as to develop the needed e-government model.

The qualitative case study method was used with observation and interview as the main data collection methods in the field. Inductive logic was used to explain the qualitative data obtained. Qualitative research methods and inductive reasoning were chosen for use because these enabled the attained requirements from the quantitative data and the qualitative data obtained to be used in the development of the e-government adoption model thereby integrating information security into an e-government adoption model for Uganda.

In all, the study followed the mixed methods nine (9) steps research process using both quantitative and qualitative methods as well as inductive reasoning (Wilkins and Woodgate, 2008). The order of steps is not static as it can vary from study to study depending on needs and concerns arising during the study. Data interpretation and validation were done throughout the data collection process (Wilkins and Woodgate, 2008). The mixed method research process steps were adopted and implemented in this research as follows: A research problem was derived from literature review and from this problem, research questions were formulated under step 1(define the research problem and appropriateness of mixed methods research for the problem). This research approach selected for use at stage 2(determine the rationale for conducting mixed methods research) was based on these research questions and theoretical concerns (Skinner, 2005). This determined the mixed method design at step 3(select a mixed methods research design) and the selected sample at step 4(select the sample) chosen for use in this study.

The central research questions were addressed through the specific objectives. These objectives were in turn addressed as shown in the following figure 3.1. it shows the major activities conducted during this study namely: i) literature review for theoretical model building, ii) Field study for requirements determination and iii) the outline of an information security (InfoSec) based e-government adoption model and iv) regression analysis.

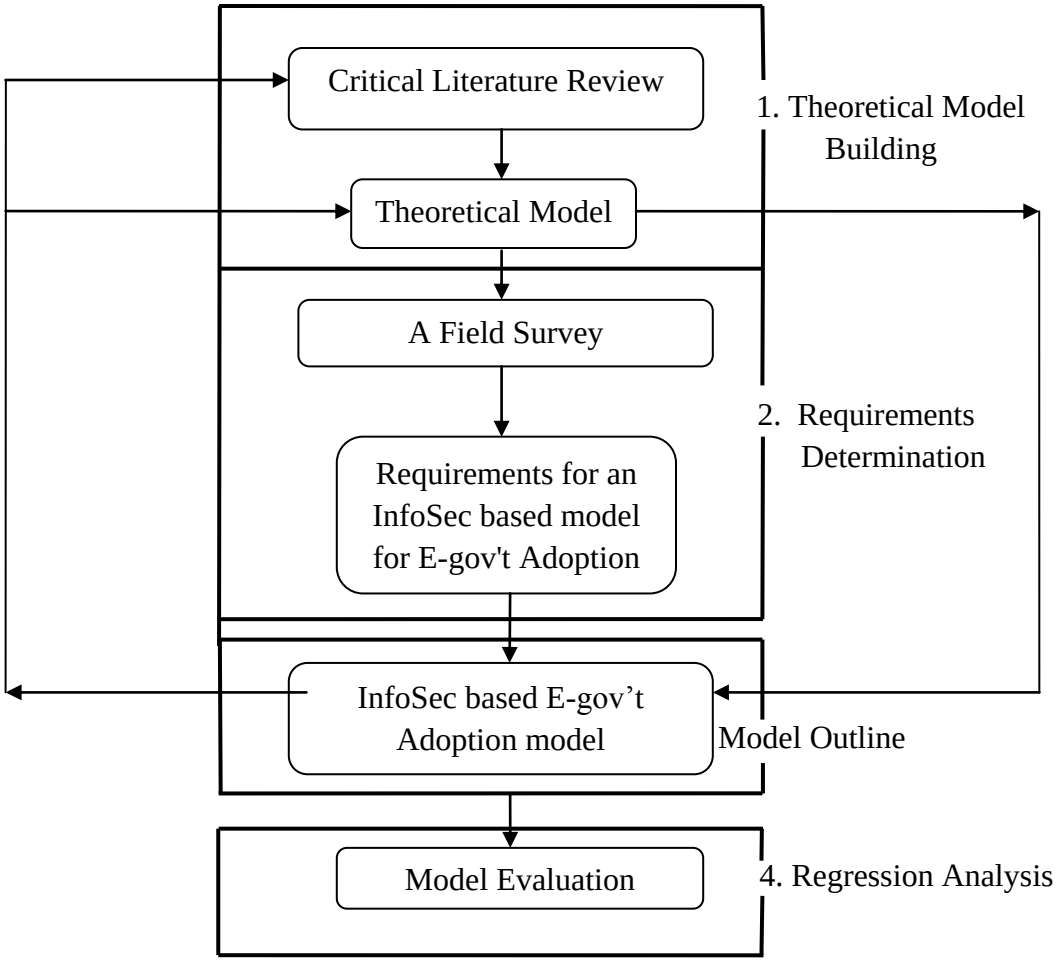

Figure 3. 1: Activities of the Research Process (Creswell, 2003)

A detailed description of the above activities that were conducted during the study is in the subsections below.

3.4.1 Literature Review

Relevant literature on e-government adoption and information security was critically reviewed in order to build the theoretical model. This was done by critically reviewing related literature in information technology, information security and existing technology adoption models. Documents reviewed included the National electronic government framework for Uganda (2010) and the National information security strategy for Uganda (2011). The national e-Government framework (2010) identified one of the challenges and threats to e-government implementation in Uganda as cyber crime and cyber terrorism and the information security strategy (2011) states that Uganda's information security maturity growth based on ISM^3 (Information Security

Management Maturity Model) is at level 1 with security not acknowledged as a desirable property of the organization. Related studies were also reviewed to include (Mivule & Turner, 2011; Wangwe *et al*., 2012; Olupot & Mayoka, 2013). Mivule & Turner (2011) state in their study that there is no national technological framework on data privacy in Uganda which entities could employ. Olupot & Mayoka (2013) identify improvement of information security as a requirement for e-government adoption in Uganda. Wangwe *et al*. (2012, p.11) state that there is no national information security framework that has been adopted in the East African countries to include Uganda. The review enabled information security factors to be obtained and ideas to be borrowed from known e-government adoption models such as (Davis, 1989; Conklin; 2007; Alfawaz *et al*., 2008; Bwalya & Healy; 2010) which were used to build the theoretical information security based e-government adoption model.

3.4.2 The Field Study

A descriptive field survey was conducted in the study area to determine requirements (InfoSec factors) for a successful e-government adoption process in Uganda. The procedure followed during data collection, analysis, validation and interpretation is discussed in the subsection below. The field study enabled the obtaining of requirements which were used for development of the information security e-government adoption model for the Ugandan context, thereby addressing the first objective to this study.

Data Collection Methods

The survey method was used with the main instrument for data collection as the questionnaire to determine requirements for successful e-government adoption in Uganda. Use of the survey method enabled the gathering of data from the large study sample which enabled inferences about the population to be made. Observations and secondary data were also used. Semi-structured close ended questionnaires were administered to the employees of the selected districts of Mbale, Sironko and government ministries of ICT and Local government in order to collect data. The questionnaire was the chosen instrument for use because it enabled the collecting of accurate primary data. A likert rating scale with scores ranging from 1-5 was assigned to each of the responses used to measure a set of variables (statements) in the questionnaire qualitatively describing information security factors for e-government systems adoption. The pilot survey was conducted to test the questionnaires and the corrections plus the experience gained were applied

to improve and make the final questionnaire which was used during the field study to collect requirements (info sec factors) that were used to develop the information security model.

Sample Selection

Sampling is the process of examining a representative set of items (people) out of the whole population in order to gain an understanding about some attribute of this population (Lucey, 2002). The sample drawn was truly representative of the study population characteristics without any bias so that it results in valid and reliable conclusions (Kothari, 2004). To obtain a sample of the study population, the sampling design included selection of some sampling units such as districts (Mbale and Sironko) and government headquarter ministries ICT and Local government Kampala from which inferences about the population were made. The number of employees working in each of these districts and ministries to include departmental heads and staff were then identified. Basing on representation basis, purposive sampling (respondents who are more knowledgeable in the area of study) was then used to draw a sample from these employees. This technique was adopted because of the relative advantage of time and money inherent in this method of sampling and the size of this research.

Target Population

Population is the total of items about which information was desired (Kothari, 2004).The aggregate of elementary units from which the sample was drawn for example population of the district. In this research, the target population included government employees working in district and ministry units of Mbale, Sironko, ICT and Local government ministry headquarters as departmental managers and staff.

Sampling Method

To obtain a sample truly representative of the study population, there is need to select a method which for a given sample size and cost has a smaller sampling error. With regards to representation basis the main methods of sampling include probability sampling based on the concept of random selection and non-probability sampling which is non-random sampling (Kothari, 2004). In this research, non probability sampling method was used. This is a procedure where each element of the population did not have a known probability of being included in the sample (Kothari, 2004). This involved the purposive selection of particular units Mbale, Sironko

districts and ICT, Local government ministry headquarters, Kampala) to constitute the study sample on the basis that these were representative of the entire universe. Non-probability sampling includes convenience, quota, snowballing and purposive sampling methods.

Purposive sampling was chosen for use in this research. Purposive sampling is a method where there was deliberate selection of particular units of the universe by the researcher for constituting the sample which represented the universe (Kothari, 2004). It is a process where research participants are selected on the basis of their ability to provide information central to the purpose of the research study Speziale & Carpenters' study (as cited in Wilkins and Woodgate, 2008). Under this the researcher specified characteristics of the population of interest and then located individuals who matched those characteristics like only important items that had experience or knowledge in the selected area of study. This method was chosen therefore so as to capture respondents who were more knowledgeable in the area of study of e-government adoption, the challenges and the requirements needed for its successful adoption in Uganda. It is with this that the units of 2 districts (Mbale and Sironko) and 2 government ministry headquarters (ICT and Local government ministries) were deliberately chosen by the researcher as representative of the entire study population with the target respondents including the employees working in these units. These employees were selected because they are at the fore front of using the adopted and implemented e-government services in Uganda like e-mails, e-tax, e-banking, and e-commerce in executing their work and are therefore more knowledgeable in the area of study. The population of employees was then stratified into 2 (departmental heads and staff) to participate in the study. The total number of employees working in these four units was established followed by a selection of items from each stratum. Based on precision rate (0.05) and confidence level (95%), the sample size was drawn. These departmental heads and staff were then given questionnaires to fill to determine the information security factors affecting e-government adoption in Uganda as well as to establish how and the requirements for incorporating information security into e-government process to enable its successful adoption in all government administrative units to include the districts and government ministries. The study used both purposive and stratified sampling techniques because of the concurrent design used (Creswell, 2007). Use of these methods enabled the sample size representative of the study population to be determined which was used for the study.

Sample Size

This refers to the number of people who were selected from the study population to constitute a sample (Kothari, 2004). An effective approach of selecting the number of items to represent the selected units, were sought with the nature of these units, population size, and budgetary constraints taken into consideration.

The sample size was determined from the overall population of departmental heads and staff working in the selected units of Mbale, Sironko districts as well as ICT and Local government ministry headquarters Kampala. The total number of employees working in these four units was established as below in order to determine the sample size.

Table 3. 1: Employees in the Different Selected Administrative Units

Name of the Unit	**No of departmental heads**	**No of staff**
Mbale	10	72
Sironko	10	64
Ministry of Local government	18	138
Ministry of ICT	16	118
Total	**54**	**392**

To obtain an optimum sample needed so as to make generalizations about the whole population in the above table, the size of the sample was determined based on the specification of three criteria to include level of precision or sampling error (the range within which the true value of the population varied and was still acceptable), confidence or risk level that is the likelihood that the answer fell within that range and degree of variability which is the distribution of attributes in the population (Israel, 1992; Kothari, 2004). Use of these criteria enabled determination of an appropriate sample size. The size of the sample was also influenced by budgetary and time constraints. The sample size was determined based on the precision rate approach so as to control the sampling error which may arise and this was done by specifying the precision 'e' expressed as (Kothari, 2004).

$$e = Z \cdot \sqrt{\frac{p\,q}{n}} \qquad \text{(Equation 3.1)}$$

Therefore size of sample 'n' is

$$n = \frac{Z^2 \cdot p \cdot q}{e^2} \qquad \text{(Equation 3.2)}$$

Therefore the above formula for calculating a sample for proportions was used to obtain a representative sample for proportions from a large population (Israel, 1992: Kothari, 2004). It was deemed best for use since there was a likelihood of the sample size varying widely from one attribute to another with each attribute having a different variance. However for a finite population which was the case in the study, the above formula in equation 3.2 was changed (Kothari, 2004).

Using the finite population multiplier $\sqrt{(N-n) / (N-1)}$, the formula for determining sample size for this study was changed as under:

$$n = \frac{Z^2 \cdot p \cdot q \cdot N}{e^2 (N-1) + Z^2 \cdot p \cdot q} \qquad \text{(Equation 3.3)}$$

Where

Z = (value of standard variate at given confidence level), e = (acceptable error), N = (size of population), P = (sample proportion, q = 1- p).

Assumptions used

±5% or 0.05 was the desired precision. In a normal distribution, confidence level is 95%. Standard variate 'Z' for given confidence level 95% (as per normal curve area table) was 1.96. Large population with an unknown variability in proportion 'p' was 0.5 (maximum variability). 'q' was (1-0.5 maximum possible proportion to yield maximum possible sample size).

Using the equation 3.3 above, the sample size based on the population of 54 (fifty four) departmental heads and 392 (three hundred ninety two) staff was as follows:

Departmental heads (sample size)

$$n = \frac{(1.96)^2 (0.5) (1-0.5) (54)}{(0.05)^2 (54-1) + (1.96)^2 (0.5) (1-0.5)} = \frac{51.8616}{1.0929} = 47.45 \sim 47 \quad \text{(Equation 3.4)}$$

Staff (Sample size)

$$n = \frac{(1.96)^2 (0.5) (1-0.5) (392)}{(0.05)^2 (392-1) + (1.96)^2 (0.5) (1-0.5)} = \frac{376.4768}{1.9379} = 194.27 \sim 194 \quad \text{(Equation 3.5)}$$

The survey therefore required and used the sample size of 47 departmental heads and 194 staff as respondents.

3.4.3 Data Analysis and Interpretation

After data collection, responses from the completed questionnaires were processed and analyzed using both qualitative and quantitative techniques. This was achieved by incorporating into the mixed methods process the mixed methods data analysis techniques that included the seven steps of data reduction, data display, data transformation, data correlation, data consolidation, data comparison and data integration (Onwuegbuzie & Leech, 2006). Responses from the questionnaire were coded (content driven coding) with each response per question labeled with a code that suggested how the associated response informed the research objectives and these represented the identified themes Q1. Total number of respondents per sector Q2. Mode of e-government services used Q3. Frequency of using electronic government services Q4. Security factors for e-government systems (A. confidentiality in e-government services B. Integrity in e-government services C. Accountability for e-government systems D. Trust in e-government services E. Security culture in e-government services) and Q5 Responses were arranged according to the above categories. The mixed methods data analysis 7 techniques suggested by (Onwuegbuzie & Leech, 2006) were used as follows:

1. Data reduction involved reducing the dimensionality of the quantitative and qualitative data. For QI, Q2, Q3, Q4 data reduction for quantitative data was done using SPSS 13.0, descriptive statistics and Microsoft excel for grouped data categories as per the themes (number of respondents per sector, mode of e-government services used, frequency of using electronic government services, security factors for e-government systems (A. confidentiality in e-government services B. Integrity in e-government services C. Accountability for e-government systems D. Trust in e-government services E. Security culture in e-government services) respectively and Q5 using exploratory thematic analysis and describing of data as per the above themes. Qualitative data was analyzed using exploratory thematic analysis and inductive reasoning.
2. Data display was done using involved use of graphs, venn diagrams, tables and graphs. The data was displayed using percentages for Q1, Q2 graph, Q3 Venn diagram Q4 and Q5 tables and graphs.
3. Data transformation was done by transforming quantitative data obtained in QI, Q2, Q3, Q4 into qualitative data during data analysis as per the above identified themes (narrative data).
4. Data correlation was achieved by using (Pearson's correlation coefficient and multiple regression analysis computed using SPSS 13.0) and this enabled correlating of the quantitative transformed data into themes with the qualitative data.
5. Data consolidation was done by combining both quantitative and qualitative data to attain the consolidated results (requirements for the model).
6. Data comparison involved comparing quantitative data, requirements from questionnaire (QI, Q2, Q3, Q4 compared with the qualitative from Q5) as well as qualitative data sources such as (documents, previous studies and statistical figures relating to the study areas and observation done during the field survey).
7. Data integration the final stage was carried out by integrating the quantitative data from the field survey (QI, Q2, Q3, Q4) and qualitative data Q5 and data from (documents, reports, statistical figures like results from correlation and regression analyses and observation), into final requirements (information security factors) which were

incorporated into the model to develop the information security e-government adoption model for Uganda.

Data interpretation was done right from the stage of data collection stage throughout the study Creswell's study (as cited in Wilkins & Wood gate, 2008). Integration, comparison and convergence of the study findings were done. This strengthened the conclusions, meaningful inferences made (Wilkins & Wood gate, 2008). Interpretation of the data analysis done was that quantitative and qualitative data obtained supported the finding that information security factors affect the e-government adoption process in Uganda.

3.4.4 Scales Reliability Test

Reliability is the extent to which the questionnaire provided consistent results (Kothari, 2004; Ayodele, 2012). That is the stability and dependability of the questionnaire to obtain true information. Test of reliability among others include stability of items (Internal-consistency) and stability of the instrument over time (Test-retest reliability).

To test questionnaire reliability (whether the different subsections of the questionnaire to include section A on Confidentiality, section B on Integrity, section C on Accountability, section D on Trust and section E on Security culture yielded consistent results) Cronbach's Alpha was used. This enabled the test for internal consistency.

3.4.5 Validity Tests

This is the degree to which the instrument measured what it was supposed to measure (Kothari, 2004). That is the level to which the test measured what it was intended to measure or it's utility. This test mainly comprises of Content validity the extent to which the research instrument provided adequate coverage of the topic under study (enough items), Construct validity the degree to which scores on the test were accounted for by the explanatory constructs of a sound theory (relevant items), Convergent and Discriminant validity were performed for assessment of construct validity with convergent as the extent to which variables within a single factor were greatly interrelated and discriminant validity as the extent to which factors were distinct and unrelated. And finally Criterion-related validity the extent to which scores on an instrument are

related to an independent criterion (measure's relevance, reliability and its' being free from bias) (Kothari, 2004; Ayodele, 2012).

Content validity in this study, was achieved through interviews (pilot study) as pre-data collection validity (Al-Shafi & Weerakkody, 2010). Construct validity was done using factor analysis which was conducted using Principal Component Analysis with the varimax rotation method (Rokhman, 2011). This was done as post data collection validity (data collected through the questionnaire). And finally convergent and discriminant validities were statistically computed using SPSS 13.0. This was done using factor analysis with the extraction method as principal component analysis.

3.4.6 Model Outline

The requirements that were attained from the field survey were used together with variables from existing e-government adoption models and the relationships (regression model) to develop an information security e-government adoption model to guide successful e-government systems adoption in Uganda. The attained requirements were used to extend an existing e-government adoption model by Bwalya & Healy (2010) so as to develop an information security model suitable for the Ugandan context. The model was developed in the following steps: 1) Adopting the theoretical contribution from the model of Bwalya and Healy (2010). The model's main constructs in addition to perceived usefulness and perceived ease of use (Davis, 1989) were used to include e-government adoption and continuance use of e-government, the added factors of ICT infrastructure plus lower access costs, both English and local language content, risks and local culture, data privacy and security, appropriate and continued user support and finally appropriate legal, regulatory plus institutional frameworks (Bwalya & Healy, 2010). 2) Incorporating requirements from the field study data analysis. These requirements to include the factors important for information security such as security culture factors (information security awareness campaigns, supporting legislation, suitable security and privacy policies and skills training), information security factors (confidentiality, integrity and accountability) and trust factors (information accuracy, information reliability, information relevancy and easy to use systems) were added as new constructs in addition to the factors already existing in Bwalya & Healy's (2010) model. 3) Relationships in the model suggested between the new factors and e-

government adoption were also used to include security culture factors are positively related to the adoption of e-government services and system, information security factors have a significant positive relationship with the adoption of e-government services and system and trust factors are significantly correlated with e-government adoption and correspondingly continued use of e-government. These relationships were tested using correlation and regression analyses. 4) Correlation and regression analyses results of the factors of confidentiality, integrity, accountability, trust, security culture and e-government adoption were also used. The results from the analyses such as the variables with significant relationship with e-government adoption to include confidentiality, accountability and trust factors were then used to extend an existing model by Bwalya & Healy (2010) in order to develop the information security based e-government adoption model for Uganda.

3.4.7 Regression Analysis

For this to be achieved, correlation and regression analyses were performed. This was by analyzing the relationships suggested between the information security factors and e-government adoption. Correlation analysis was used to measure the degree of relationship between variables (Kothari, 2004). Pearson's coefficient of correlation was conducted and this enabled measurement of the strength of the relationship between the variables security culture, information security, trust factors and e-government adoption (services).

Regression analysis is a statistical technique that was used for studying the linear relationships (Kothari, 2004). Multiple regression analysis as used enabled determination of the relationship concerning the dependent variable (e-government services adoption) and the independent variables (security culture, information security and trust factors). The obtained information helped in identifying the factors that are the best starting point to be addressed for improvement of e-government adoption from the information security perspective in Uganda.

Overall, the Regression and correlation analyses of the model provided understanding and confirmation of the suggested relationship between the information security factors presented in the conceptual model and e-government adoption process. This enabled evaluation of the developed model.

CHAPTER FOUR

Data Analysis and Results Description

4.1 Introduction

The previous chapter described the methodology used to conduct this study. This chapter presents the findings of that field study conducted to collect data from the study area so as to obtain requirements for an information security based e-government adoption model for Uganda. The results of the descriptive field survey were then used to obtain requirements (information security factors) for a model for the successful e-government adoption process in Uganda. The outcome from this chapter therefore answers the research question as well as meets a specific objective of this study of determining requirements needed for an information security e-government adoption model for the Ugandan context. The results are presented in detail in the following sections.

4.2 Data Analysis

The results from the analysis of the data collected during the survey are presented in this section. The main data collection instrument used was the questionnaire issued to government employees working as departmental managers and staff in district and ministry units of Mbale, Sironko, and Local government ministry headquarters. A total of two hundred and forty one (241) questionnaires were distributed. Two hundred and twenty five respondents (225) returned correctly filled questionnaires. Out of these, 62.2% were respondents from government ministries and 37.8% from districts. The data collected was classified into usable categories, coded and arranged in themes appropriate to the research problem and objectives of the study. These themes were frequency of using electronic government services, mode of e-government services, confidentiality for e-government adoption, integrity in e-government systems, and accountability for the security of information in e-government, e-government trust to ensure information security and security culture amongst government employees. The classified data was then tabulated and the instrument reliability as well as validity analysis conducted. The findings from the analyzed data are as presented in the following sections.

4.2.1 Scales Reliability Test

Reliability is the extent to which a measuring instrument (questionnaire) provides consistent results (Kothari, 2004; Ayodele, 2012). That is the stability and dependability of a tool or it being free from error and therefore obtaining true information. Test of reliability among others include stability of items (Internal-consistency) and stability of the instrument over time (Test-retest reliability). In this case questionnaire reliability tested whether the different subsections of the questionnaire to include section A on Confidentiality, section B on Integrity, section C on Accountability, section D on Trust and section E on Security culture yield consistent results. Cronbach's coefficient alpha value was used to determine internal consistency with the recommended level of Cronbach's Alpha as more than 0.60 (Kumar *et al*., 2012).

To ensure instrument reliability and have confidence in the findings, the factors of confidentiality, integrity, accountability, trust and security culture were examined using Cronbach's alpha value to test the internal consistency of these factors measuring e-government adoption (services) from an information security view. Kumar *et al*. (2012) suggest that Cronbach's alpha more than 0.60 is a fair and acceptable reliability, more than 0.70 is good reliability and between 0.80 to 0.95 is very good reliability to correct accurate answers. Reliability values between 0.65 and 0.92 are acceptable reliability level for research (Hair *et al*.,'s study as cited in Rokhman, 2011). Reliability values for each construct are shown in table 4.1. A high value means all constructs are internally consistent and measure the same content of the construct (e-government adoption from an information security view).

Table 4. 1: Summary of Cronbach's Alpha Results for Constructs

Constructs	Alpha Value (Reliability)
E-government adoption (services)	.652
Confidentiality	.654
Integrity	.926
Accountability	.895
Trust	.668
Security culture	.881

Based on reliability results as summarized in table 4.1 most constructs were above 0.70 (integrity, accountability, security culture) while trust and confidentiality were close to 0.70, which is a good reliability result. The findings thus show that the questionnaire used in the study was reliable and the results of the questionnaire can be relied on as the alpha values were above or close to 0.70.

4.2.2 Validity Test

Content and construct validity were used in this study for validation of research constructs. Validity is the extent to which an instrument measures what it is supposed to measure (Kothari, 2004; Ayodele, 2012). To ensure validity of the constructs, the following approaches were used. Content validity in this study was done using interviews (pilot study) as pre-data collection validity (Al-Shafi & Weerakkody, 2010). This confirmed that there were enough items and questions in instrument covering the study topic.

Construct validity in the study was evaluated using factor analysis which was conducted utilizing Principal Component Analysis with the varimax rotation method, for post data collection validity (data collected through the questionnaire) (Rokhman, 2011). Factor analysis is a method used to statistically determine the correlation or relationship among variables in a dataset. This method was used because it gives a structure to group variables based on strong associations and aids the detection of misfit variables. SPSS 13.0 was used to perform this analysis and the analysis confirmed that construct discriminant validity (items are loaded properly in the construct) and convergent validity (presence of correlation) were achieved for this study. Convergent validity is the extent to which variables within a single factor are highly interrelated where as discriminant validity is the extent to which factors are distinct and unrelated. The communality of items or the level to which an item correlates with all other items were also determined with variables having values that are low (0.0-0.4) identified as items to be extracted after examining the pattern matrix. This is because such variables struggle to load significantly on any factor.

Validity on Confidentiality for E-Government Adoption

Convergent and discriminant validities were statistically computed on the factor of confidentiality rated against e-government adoption (services) using the Statistical Package for Social Sciences (SPSS). In factor analysis, convergent validity is considered satisfactory when items load high on

their respective factors as per the rule that is a loading higher than 0.50 and an Eigen value above one (> 1.0). Discriminant validity was assessed by examining whether each item loaded higher on the construct it measured than on any other constructs. Table 4.2 below presents the results for discriminant validity on confidentiality rated against e-government adoption services (e-tax, e-mail, e-health, e-commerce, e-banking and e-voting).

Table 4. 2: Component Factor Loading on Confidentiality for E-Government Adoption

	Rotated Component Matrix(a)		
	Constructs on Confidentiality	Component	
		1	2
1	Access to information in e-government systems should be accessible to allowed e-government users only	.580	
2	I can use the e-mail service if the system and my personal information are accessible to allowed e-government users	.721	
3	Personal information should be kept private in the e-health system		.835
4	I am more likely to use the e-commerce system if the transactions are to be kept confidential		.791
5	E-banking information should be accessible to allowed e-government users only	.773	
6	Personal information in the e-voting system should be kept confidential	.469	.491*

Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization. Rotation converged in 3 iterations.

Based on the results presented in table 4.2 above of discriminant validity, five items loaded above (0.50) the minimum recommended value. Most factors loaded highly on their own factors than on other factors except factor (6) which had cross loading that was differing by more than 0.2 which according to the rule should be the case. Factor loadings below 0.40 were suppressed. In as regards to convergent validity, two factors were extracted with an Eigen value above one (>1.0) and most items extracted had loading higher than 0.50 apart from item (1 and 6) whose loadings were (0.395 and 0.461) respectively. The two extracted factors explained 55.6% of the variance as presented in appendix III. Reasonable validity was achieved for both convergent and

discriminant validities on the construct of confidentiality and thus, the results satisfied the analysis.

Validity on Integrity as a Construct for E-Government Systems

To examine validity on the construct of integrity rated against e-government adoption (services), factor analysis using principal component analysis with varimax rotation was used. Results for discriminant validity on the construct of integrity rated against e-government adoption (e-tax, e-mail, e-commerce, e-banking, e-health and e-voting) are as shown below in table 4.3.

Table 4. 3: Component Factor Loading on the Construct of Integrity

	Component Matrix(a)	
	Constructs on Integrity	Component
		1
1	E-tax data should not be tampered with during transfer	.783
2	E-mail service data should not be tampered with during transfer	.882
3	E-commerce data should not be tampered with during transfer	.864
4	E-banking data should not be tampered with during transfer	.881
5	E-health service data should not be tampered with during transfer	.871
6	E-voting data should not be tampered with during transfer	.861

Extraction Method: Principal Component Analysis. 1 component extracted, the solution could not be rotated.

As observed in the results in table 4.3 above of discriminant validity on the construct of integrity, all items loaded above (0.50) the recommended value. Thus the items loaded properly in the construct discriminate validity. Both discriminant and convergent validities results on integrity were desirable and satisfied the analysis. Only one component was extracted and so the solution could not be rotated. This component explained 73.6% of the variance. All the factors loaded higher than 0.50 on their own factors. One factor which was extracted had an Eigen value above one (>0.1) and all factors loading higher than 0.50 as presented in appendix III.

Validity on Accountability for E-government Systems

Factor analysis using principle component analysis with varimax rotation was used to evaluate construct validity for accountability. Accountability was rated against e-government adoption (services). The results for discriminant validity for the construct of accountability are as presented in table 4.4 below.

Table 4. 4: Component Factor Loading on Accountability for E-Government

	Component Matrix(a)	
	Constructs on Accountability	Component
		1
1	Recipients of data in e-tax systems should not be able to deny receiving it	.799
2	Senders of data in e-tax systems, should not be able to deny sending it	.790
3	Recipients of data in e-mail systems should not be able to deny receiving it	.799
4	Senders of data in e-mail systems should not be able to deny sending it	.811
5	Senders of data in e-commerce systems should not be able to deny sending it	.811
6	Recipients of data in e-banking systems should not be able to deny receiving it	.853

Extraction Method: Principal Component Analysis. 1 component extracted, the solution could not be rotated.

Results in table 4.4 show that all the items loaded properly in the construct discriminate validity (all items loaded above 0.40 and there was no cross loading). Assessment of convergent validity on the construct of accountability indicated that one factor with an Eigen value above 1.0 was extracted. This factor explained 65.7% of the variance. All factors after extraction were higher than 0.50. A desirable convergent validity was attained as presented in appendix III. Desirable discriminant validity was also achieved as factors loaded highly on their own factors. One component was extracted and there were no cross loadings. Discriminiant and convergent validity results on accountability as a construct for e-government was thus significant and satisfied the analysis.

Validity on Trust for E-government Adoption

Factor analysis using the principle components with varimax rotation was used to determine construct validity for the factor of trust. Trust was rated against e-government adoption (information accuracy, information reliability, easy to use e-government systems, language content and information relevancy issues). Discriminant validity results on the construct of trust are presented in table 4.5 below.

Table 4. 5: Factor Loading on Trust as a Construct for E-Government Adoption

	Rotated Component Matrix(a)		
	Constructs on Trust	Component	
		1	2
1	Information provided by e-government systems should be accurate if it is to be trusted	.905	
2	Information provided by the e-government systems should be reliable if it is to be trusted	.825	
3	E-government systems should be easy to use	.748	
4	I would prefer using e-government systems whose content is in local language		.987
5	E-government systems should provide information relevant to users	.755	

Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization. Rotation converged in 3 iterations.

Results in table 4.5 above show discriminant validity results on Trust. All the items loaded highly on their own factors than on other factors, above the value of (0.50). Four items of trust loaded at component 1, while 1item loaded at component 2. The results showed that reasonable discriminant validity was attained. Suitable convergent validity was also achieved with two factors extracted having Eigen values above one (>0.1) and all factors loading higher than 0.50. The two factors extracted explained 73.2% of the variance as presented in appendix III. Discriminant and convergent validity results for trust as a construct for e-government adoption (services) was therefore desirable and satisfied the analysis.

Validity on Security Culture for E-Government Adoption

Factor analysis using principle component analysis with varimax rotation was used to evaluate construct validity for the factor of security culture. To determine if each item loaded higher on the factor it measured than on any other factors, discriminant validity was conducted on the construct of security culture rated against e-government adoption (in issues of supporting legislation, staff training, information security awareness campaigns, suitable security and privacy policies). The analysis results are depicted below in table 4.6.

Table 4. 6: Component Factor Loading on Security Culture for E-Government Adoption

	Component Matrix(a)	
	Constructs on Security Culture	Component
		1
1	Supporting legislation is required for e-government systems	.831
2	Training is required for proper e-government systems use	.863
3	Suitable security and privacy policies are required for e-government systems	.872
4	Awareness campaigns are required to increase e-government use	.882

Extraction Method: Principal Component Analysis. 1 component extracted, the solution could not be rotated.

According to the results presented in table 4.6 above, suitable discriminant validity was attained as all items loaded well in the construct discriminate validity (highly above 0.50). The solution could not be rotated as only one component was extracted. Convergent validity as per the results presented in appendix III, indicate that all items loaded higher than 0.50 on their particular factors. One factor had an Eigen value above one (>1.0) and was extracted. This factor explained 74.3% of the variance. Therefore discriminant and convergent validity attained on security culture as a construct for e-government adoption was significant and satisfied the analysis.

4.3 The Descriptive Statistics

Different statistical methods can be used to analyze collected data sets. Two steps are usually involved in quantitative data analyses: 1) descriptive statistics to obtain a descriptive overview of

data, and statistical tests for hypothesis testing (Hair *et al*. 2007). In order to get a descriptive overview of the data, descriptive statistics is used. This statistical analysis summarizes the large set of data through a limited number of meaningful statistical indicators. Each variable is studied separately to compare average scores of variables among the different groups of respondents (Janssens *et al*., 2008). Usually, descriptive statistics contain three types of indicators: frequency distribution, central tendency measures, and dispersion measures. The use of frequency distribution indicates how the scores of individual respondents are distributed for each of the variables, and it examines the data of one variable at a time (Janssens *et al*., 2008). A frequency distribution shows the variable name and description, frequency counts for each value of the variable, and cumulative percentages for each value associated with a variable (Hair *et al*., 2007). For this study, frequency distribution was conducted as presented in the following subsections.

4.3.1 Frequency of Using Electronic Government Services

Data was collected on frequency of using e-government services by employees at work was analyzed using SPSS and compared based on respondents agree or disagree response rate. Results obtained on frequency of e-government services use were presented as percentage proportions. Results showing the proportions of frequency of e-government services' use by employees are illustrated in Figure 4.1 below.

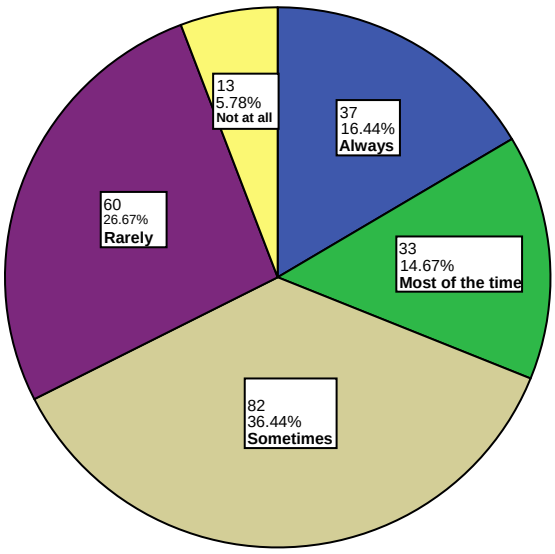

Figure 4. 1: Frequency of Using E-government Services.

Figure 4.1 shows the overall frequency of use of e-government services at 94.2% with 5.8% respondents not using the available e-services at all. Out of the 94.2% respondents, 36.4% of the government employees used electronic government services sometimes, 26.7% rarely, 14.7% most of the time and 16.4% always. Those using them sometimes were the majority because not all offices were connected to electronic government services and the employees only use e-services when there is really need to execute work related assignments. Frequency of e-services use is a main indicator of respondents' access to e-government services. As was observed those using the e-services always, most of the time and sometimes were more conversant about the different electronic government services available at work and their use. Although the percentage frequency for use in general was high 94.2%, the employees using e-services most of the time and always is still low 31.1%. There is thus need to address the factors hindering the use of e-government services' by employees so as to improve on the frequency of e-government services' use and the overall adoption process.

4.3.2 Mode of E-Government Services

Data was collected on the mode of e-government services e-mail, e-tax, e-voting, e-health, e-banking and e-commerce used by employees at their places of work. It was analyzed in SPSS and a comparison was made based on the respondents' agree or disagree rate. Data computed on respondents use of modes of e-government services was presented in appendix IV. The obtained results were presented as percentages in the following figure below.

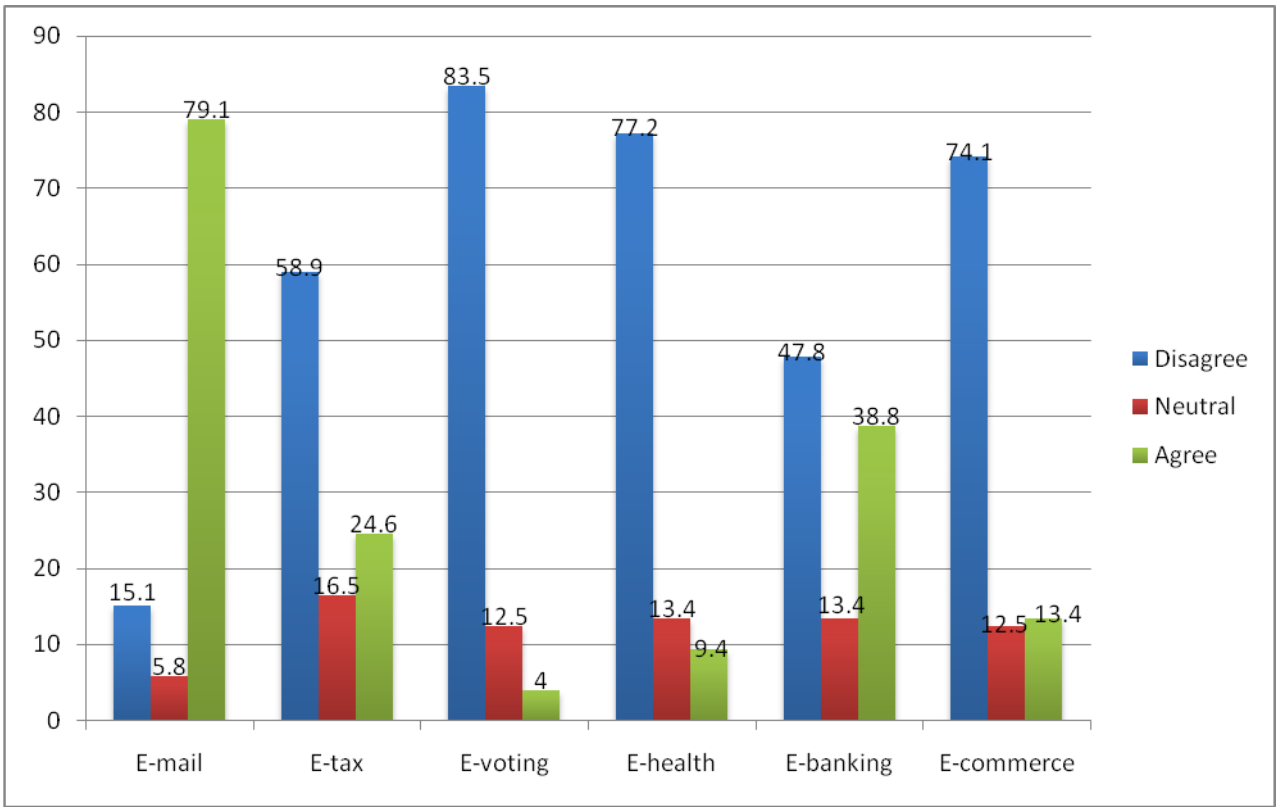

Figure 4. 2: Mode of E-government Services Used by Employees

Results in Figure 4.2 above indicate the email service as the most used as 79.1% of the respondents agreed to use of the e-mail service while 15.1% disagreed to its use at their place of work. The least used service was electronic voting which had 4% of the respondents agreeing to its use and 83.5% disagreeing to its use at work. Results indicate the most used mode of electronic service at work as e-mail which is used mainly for communication. Majority of the employees were aware of the electronic mail service and had used it. This was followed by e-banking mainly used for their salary payment and finally e-tax used for remitting taxes to Uganda Revenue Authority. Respondents' use of the e-services were computed because these respondents are more informed about the available electronic services, the challenges faced and the security requirements needed for their successful adoption at their place of work. Overall the e-mail service is used most at 79.1% with the other modes of e-services e-tax, e-health, e-banking, e-voting and e-commerce scoring poorly as regards to their use by employees at places of work. Therefore there is need to address this low use of other e-government services e-tax, e-voting, e-health, e-banking and e-commerce by employees at their work places for success to be attained in the adoption of e-government services.

4.3.3 Confidentiality in E-Government Services

The study gathered data on the information security factor of confidentiality which was rated against e-government services of e-tax information, e-mail personal information, e-health personal information, e-commerce transactions, e-banking information and e-voting personal information. Data gathered was analyzed using SPSS and compared based on respondents agree or disagree rate. The data computed on responses of employees on the need for confidentiality in the different e-government services was presented in appendix IV. The results got were presented as percentages as illustrated in the bar graph below.

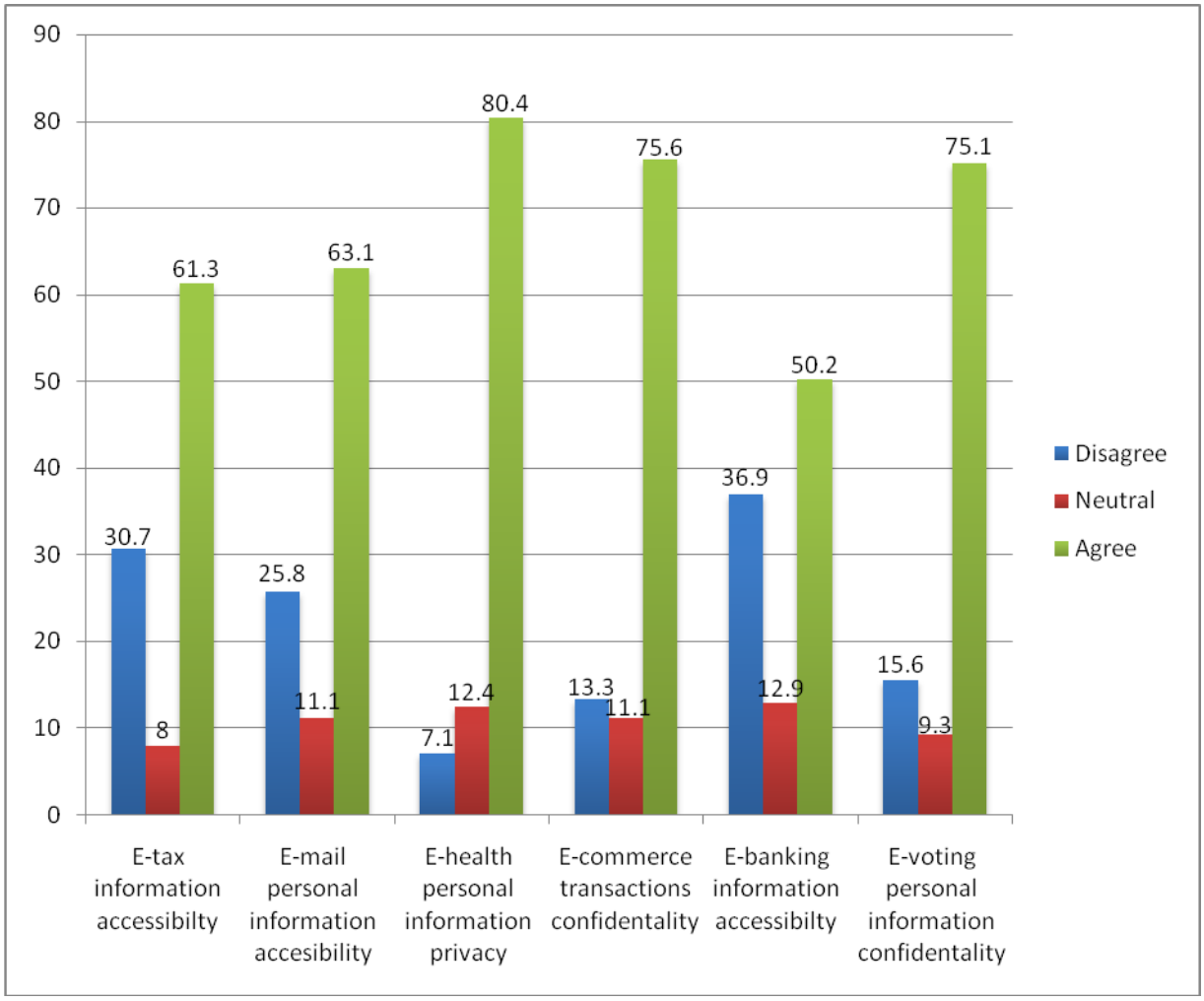

Figure 4. 3: Confidentiality for E-government Systems

Based on the results in Figure 4.3 above, 61.3% of the e-tax respondents agreed to the need to limit information access to authorized users only in e-government systems while 30.7%

disagreed, in the e-mail system 63.1% agreed while 25.8% disagreed. Only 50.2% of the respondents agreed to the need to limit information access in e-banking and 36.9% disagreed. In as regards to the need to maintain privacy of personal information in e-government, for e-health 80.4% agreed while 7.1% disagreed, e-commerce transactions 75.6% agreed while 13.3% disagreed and finally 75.1% agreed for e-voting while 15.6% disagreed. The results depict the e-health service as the main where respondents considered the need for information confidentiality for its adoption. In general all the e-government services had a high respondents agree rate of above 50% with regard to the need for information confidentiality for success to be reached in their adoption. Confidentiality is thus an important requirement needed for successful e-government adoption from an information security view.

4.3.4 Integrity of E-Government Services

Data was collected on the information security factor of integrity which was rated against e-government services of e-mail data integrity, e-tax data integrity, e-commerce data integrity, e-banking data integrity, e-health data integrity and e-voting data integrity. The collected data was analyzed using SPSS and a comparison was made based on respondents' agree or disagree rate. Data computed on the views of employees as regard to the need for integrity in different e-government services was presented in appendix IV. The results attained were presented as percentages in the bar graph below.

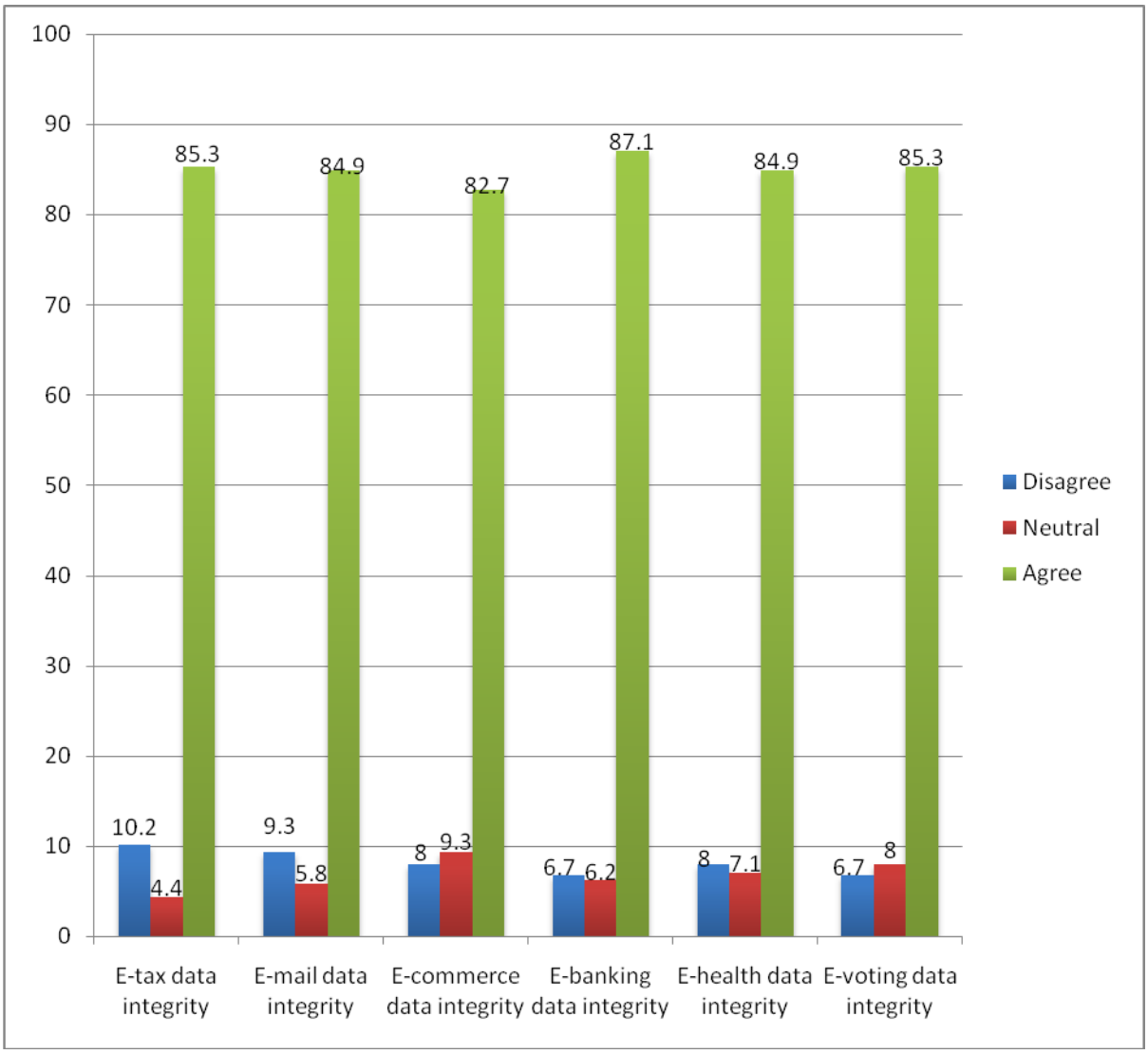

Figure 4. 4: Integrity for E-government Systems

The information in Figure 4.4 above shows that for the e-tax service 85.3% of the respondents agreed to the need for information integrity in e-government while 10.2% disagreed, 84.9% agreed for the e-mail service while 9.3% of the respondents disagreed. For e-commerce data integrity 82.7% of the respondents agreed while 8% disagreed, 87.1% agreed for e-banking data integrity while 6.7% disagreed, in e-health 84.9% agreed where as 8% disagreed, for e-voting 85.3% agreed and only 6.7% of the respondents disagreed. The results indicate that integrity of data was considered most important by respondents in the electronic banking service. Overall all the e-government services had a high respondents agree rate of above 80% with regard to the need for data integrity for success to be reached in their adoption. Therefore integrity is an important information security factor for successful e-government adoption.

4.3.5 Accountability in E-Government Services

Data was collected on the factor of accountability which was rated against the variables of liability by e-tax data recipients, liability by e-tax data senders, liability by e-mail data recipients, liability by e-mail data senders, liability by e-commerce data senders and liability by e-banking data recipients. This was so as to determine the importance of accountability for information security in e-government services. Data collected was analyzed using SPSS and compared based on respondents' level of agreement or disagreement. The data computed on employees' views as regard to the need for accountability in the different e-government services was presented in appendix IV. Results attained on the factor of accountability were presented as percentages in the bar chart below.

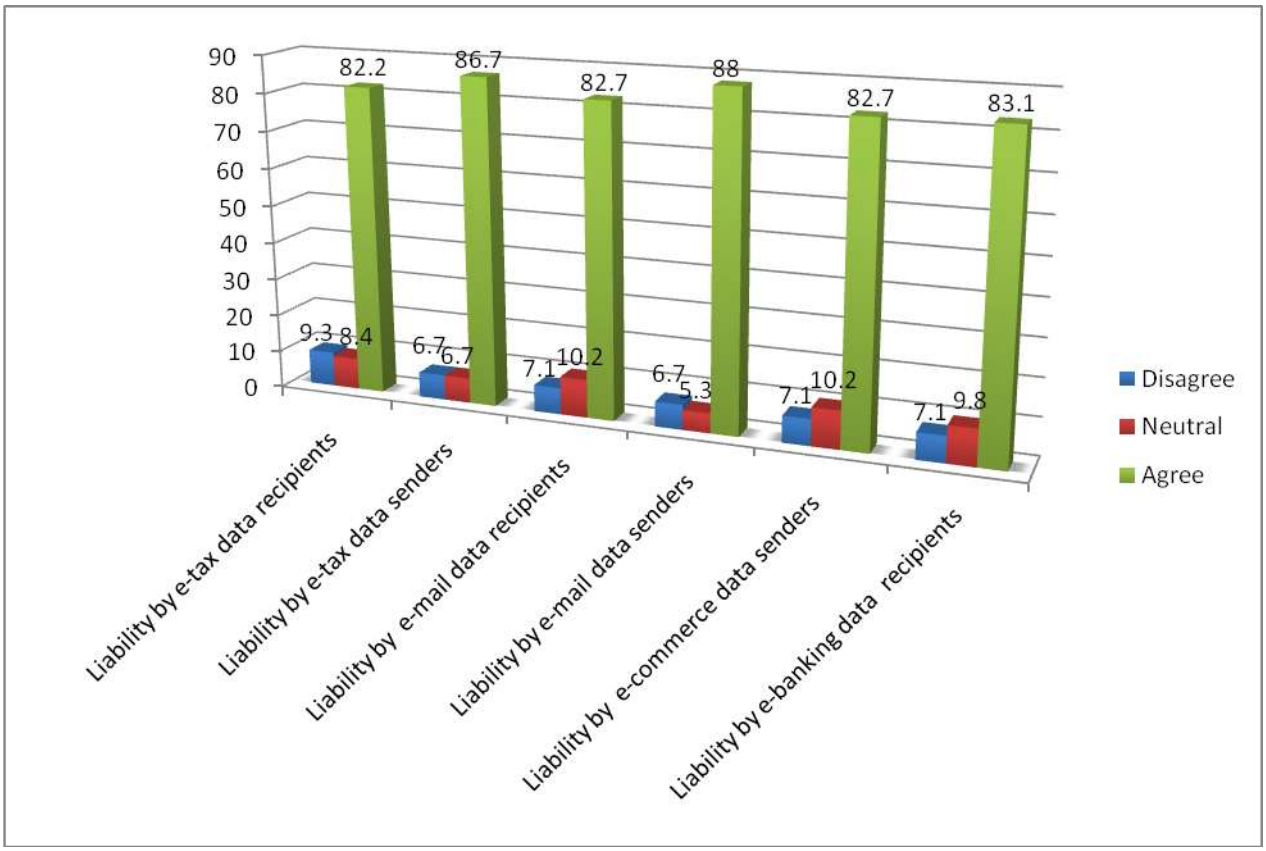

Figure 4. 5: Accountability for E-government Systems

Figure 4.5 portrays that the respondents agreed to accountability as an information security factor needed for e- government services' adoption. The need to ensure that data senders or recipients in e-government systems account for their actions was considered most important for e-mail data

senders which had 88% of the respondents in agreement and only 6.7% disagreeing. This was followed by the factor of liability by e-tax data senders that had 86.6% of the respondents in agreement while 6.7% disagreed and finally the factor of liability by e-tax data recipients with 82.2% of the respondents in agreement while 9.3% disagreed. Overall the results show that majority of the respondents agreed to the factor of accountability as vital for ensuring security of information in e-government services' adoption.

4.3.6 Trust in E-Government Services

The study collected data on the factor of trust which was rated against the variables of information accuracy, information reliability, easy to use systems, content in local language and information relevancy. This was so as to determine the importance of trust for information security in e-government adoption. Data collected was analyzed using SPSS and a comparison was made based on respondents' agree or disagree rate. The data computed on respondents' views on the need for trust in different e-government services was presented in appendix IV. Results obtained on the factor of trust were graphically presented as percentages in the following Figure 4.6.

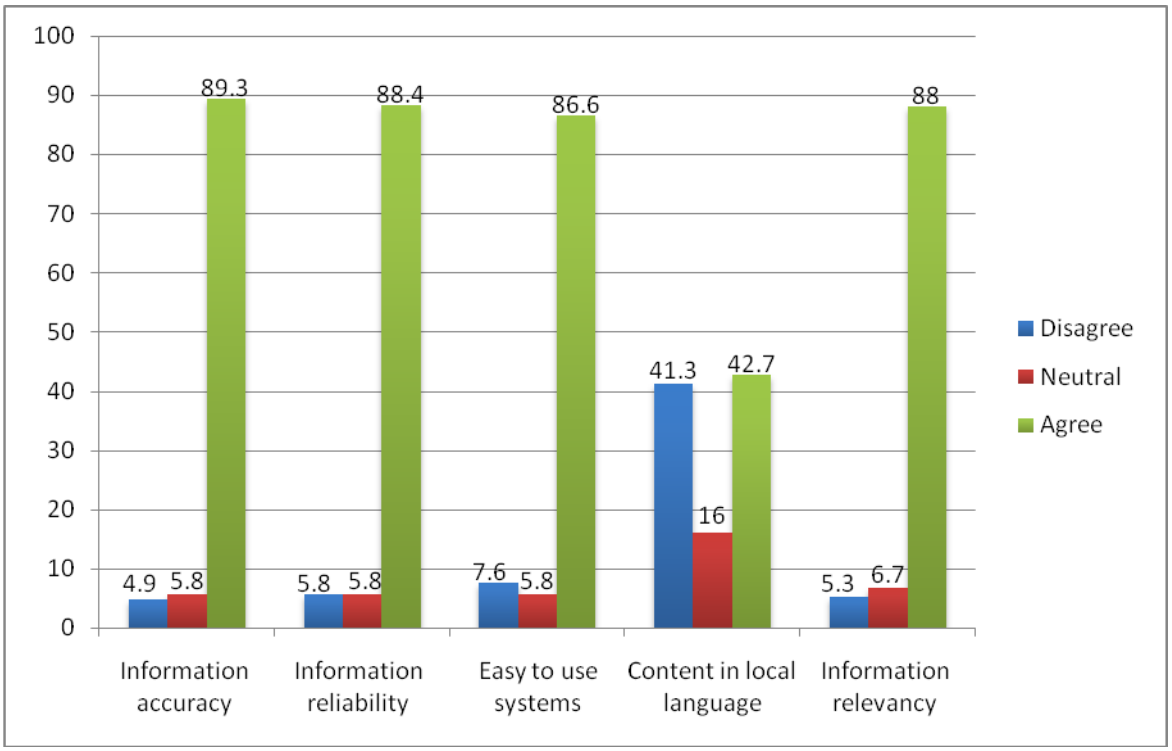

Figure 4. 6: Trust for Security in E-government Systems

As seen in Figure 4.6 above, 89.3% of the respondents agreed to the need for information accuracy to attain trust in e-government adoption while 4.9% disagreed, for information reliability 88.4% agreed and 5.8% disagreed. For the issue of ease of use of e-government systems 86.6% agreed while 7.6% disagreed, the need to have content in local language only 42.7% agreed where as 41.3% of the respondents disagreed and for the aspect of information relevancy 88% of the respondents agreed while 5.3 % disagreed. Results show that though in general respondents agreed to the importance of trust in e-government adoption, trust as an e-government security factor was considered most essential as regards to information accuracy and least important for the need to have content in the local language.

4.3.7 Security Culture in E-Government Services

Data was gathered on the factor of security culture which was rated against the variables of supporting legislation, training, awareness campaigns, suitable security and privacy policies. This was so as to determine the importance of security culture for information security in e-government services' adoption. Data gathered was analyzed using SPSS and a comparison was made based on respondents' agree or disagree rate. Data computed on employees' responses on the need to have a suitable security culture in place to ensure information security in e-government was presented in appendix IV. The summary of the obtained results on security culture were presented as percentages in Figure 4.7.

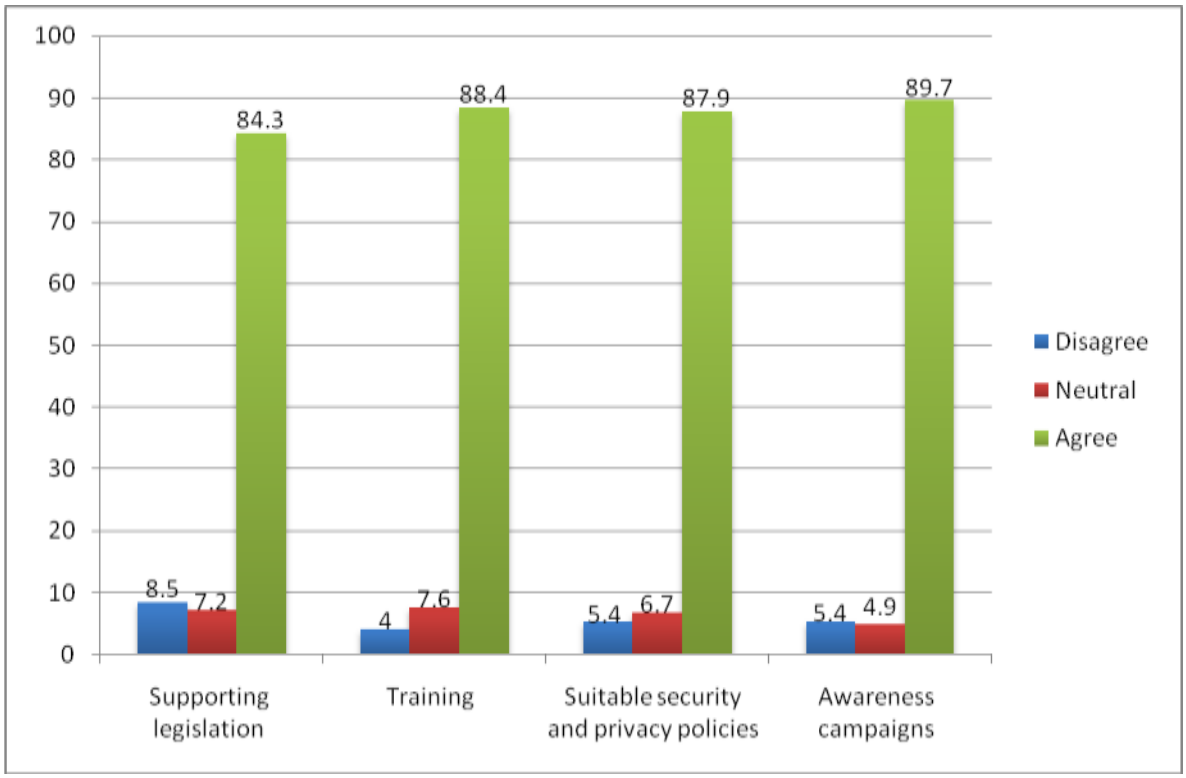

Figure 4. 7: Security Culture to Ensure E-government Adoption

Results in Figure 4.7 show that respondents agreed to security culture as a factor needed for the adoption of e- government services. The variable of awareness campaigns had the highest agree rate 89.7% and a 5.4% disagree rate, followed by training with 88.4% respondents in agreement and 4% in disagreement, then suitable security and privacy policies with 87.9% in agreement and 5.4% in disagreement and finally supporting legislation that had 84.3% of the respondents agreeing and 8.5% disagreeing. Overall the results show that majority of the respondents above 80%, agreed to the need for the factor of security culture. In all, these results highlight the importance of having a suitable security culture in place for success in the adoption of e-government services.

4.4 Summary of the Field Study Findings

In conclusion, the study aimed at obtaining the requirements needed for the development of an information security e-government adoption model for Uganda. Data was gathered on employees' views on the factors confidentiality, integrity, accountability, trust and security

culture rated against e-government adoption. The data gathered was analyzed using SPSS and the field study findings are summarized in Table below.

Table 4.7: Summary of Requirements

Requirements	**Area in E-services where requirement is needed**	**Area in E-services with Highest percentage (**where requirement is most needed)
Confidentiality	E-tax (information accessibility), E-mail (personal information accessibility), E-health (personal information privacy), E-commerce (transactions confidentiality), E-banking (information accessibility), E-voting (personal information confidentiality)	E-health personal information privacy
Integrity	E-tax (data integrity), E-mail (data integrity), E-commerce (data integrity), E-banking (data integrity), E-health (data integrity), E-voting (data integrity)	E-banking data integrity
Accountability	Accountability by e-tax data recipients, accountability by e-tax data senders, accountability by e-mail data recipients, accountability by e-mail data senders, accountability by e-commerce data senders, accountability by e-banking data recipients	Accountability by E-mail data senders
Trust	Information accuracy, information reliability, easy to use systems, information relevancy	Information accuracy
Security culture	Supporting legislation, skills training, suitable security and privacy policies, information security awareness campaigns	Information security awareness campaigns

The detailed description of the field study findings was presented in section 4.3. This section summarizes those findings and requirements. According to the field results presented in figure 4.1, the overall percentage frequency of using e-government services by employees was high. Although the percentage frequency for e-services use in general was high 94.2%, the employees using e-services most of the time and always is still low 31.1%. There is therefore need to address the factors hindering effective use of e-government services by employees so as to improve on the frequency of e-services use by employees for success to be achieved in the adoption process.

Though e-government services in place are being used by employees, it was observed that with regard to the mode of e-government services used at work places the e-mail service was the most used 79.1% while use of the other e-services is still low e-tax 24.6%, e-voting 4%, e-health 9.4%, e-banking 38.8% and e-commerce 13.4%. Therefore there is need to improve on this low use of other e-government services by employee at their work places for success to be reached in the adoption of e-government services.

Results in table 4.7 above show that all the factors confidentiality, integrity, accountability, trust and security culture had high percentages of respondents agreeing to their importance in the adoption process and were thus taken as requirements for the development of an information security e-government adoption model for Uganda. The variable of putting e-government content in local language proposed under trust was left out because it had a low percentage of agree 42.7% with disagree percentage as 41.3%.

Based on the above results, confidentiality was considered an important requirement for successful e-government adoption from an information security view especially with regard to e-health personal information privacy, integrity in e-banking data integrity, accountability in accountability by e-mail data senders, trust in information accuracy and security culture mainly in information security awareness campaigns. Therefore, requirements that need to be in place for successful e-government services adoption from an information security view are confidentiality, integrity, accountability, trust and security culture factors. These are used in the outline of an e-government adoption model in the following section.

4.5 Model Outline and Development

This section presents the development of a model for e-government adoption that incorporates the information security perspective in the Ugandan context. It uses requirements obtained from the analyzed results of the field study presented in the preceding sections. The developed model adopts and extends an existing e-government technology adoption model of Bwalya & Healy (2010). An outline of the model for e-government adoption in Uganda is here presented. The development of the new model and its evaluation helped to answer research questions and meet specific objective 2 of this study.

The information security model for e-government adoption was derived and evaluated in the following steps: 1) Adopting the theoretical contribution from the model of Bwalya and Healy (2010) and 2) incorporating requirements from the field study data analysis. The model outlined in figure 4.8 below is therefore an extension of the model for harnessing e-government adoption in the SADC region by Bwalya & Healy (2010). The model by Bwalya & Healy (2010) derives from TAM (Davis 1989). Requirements from the field study analysis are incorporated in the outlined model. In addition to the factors already existing in Bwalya & Healy's (2010) model, the new outlined model adds new constructs important for information security. These are,

1) Security culture factors that include information security awareness campaigns, supporting legislation, suitable security and privacy policies and skills training.
2) Information security factors that includes confidentiality, integrity and accountability.
3) Trust factors comprising of information accuracy, information reliability, information relevancy and easy to use systems.

The components of the model outline are presented in the following figure 4.8.

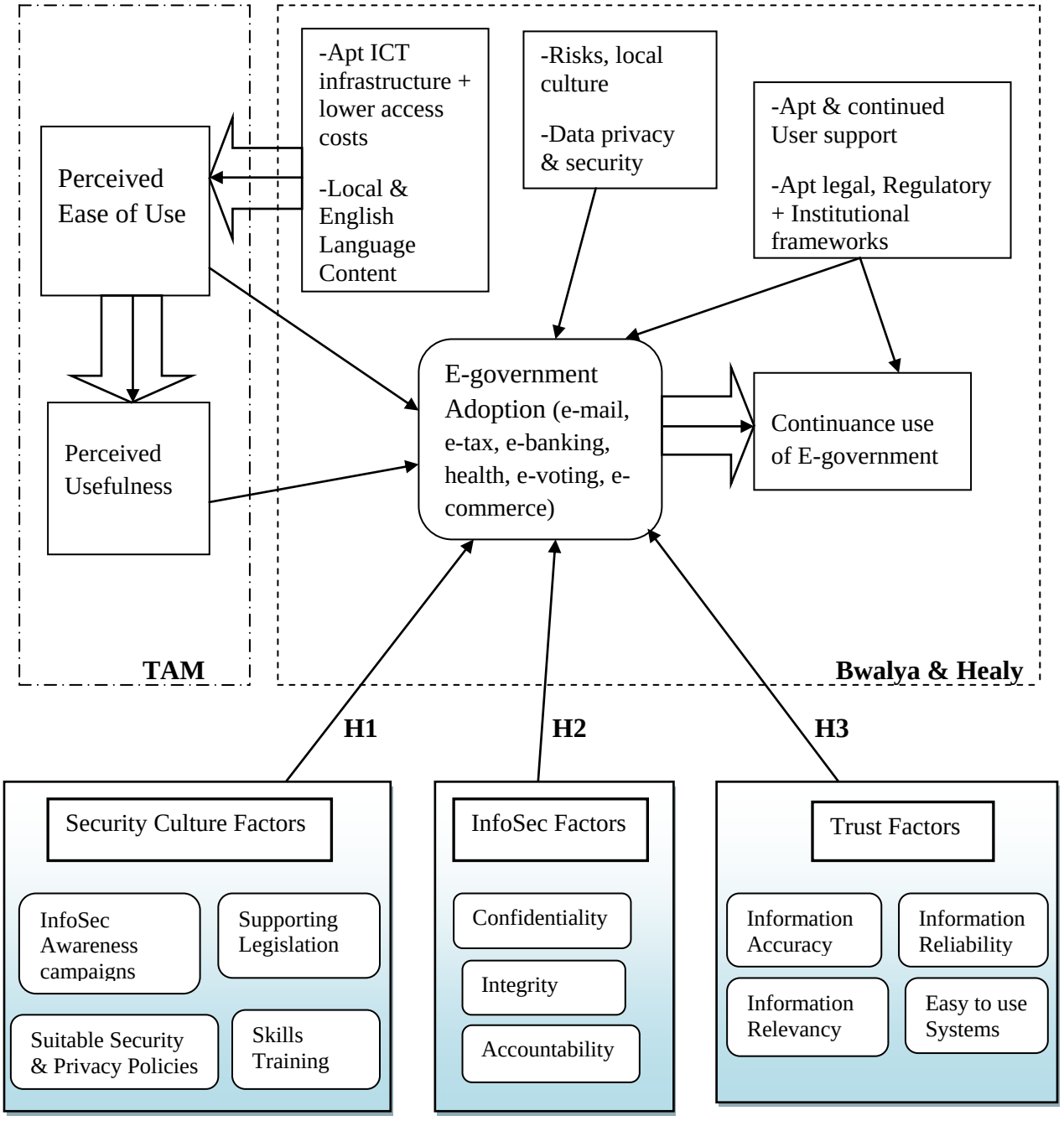

Figure 4. 8: The Information Security E-government Adoption Model

Figure 4.8 is an outline of the extended model by Bwalya & Healy (2010) for effective addressing of e-government adoption from an information security standpoint for a transitioning country such as Uganda. The model development process is presented in the following subsections.

4.5.1 Theoretical Contribution from TAM to the Model

TAM is the basis of the model of Bwalya & Healy's (2010), selected for adoption and extension in this study. This model has been empirically tested in different parts of the world and been proven as reliable and providing an explanation of individuals' intention of adopting technology (Bwalya & Healy, 2010). TAM is a leading model in explaining and predicting system use. It has as well been used in most research that deals with user acceptance of technology with perceived ease of use and perceived usefulness identified and confirmed as important in predicting a person's behavior (Chuttur, 2009). Venkatesh and Davis (2000) as cited in Bwalya & Healy (2010) stated perceived ease of use and perceived usefulness as the most important ingredients and determinants of citizen's intention to engage in a technology.

Perceived Ease of Use

Perceived ease of use is the degree to which an individual believes that using a particular system would be free of effort (Davis, 1989; Venkatesh *et al*., 2003). Kumar *et al*. (2007) identified the factors that make up perceived ease of use as easy to learn, controllable, clear and understandable, flexible and easy to become skillful with regard to system use (Davis, 1989). Perceived ease of use in this study is used with regard to information security and e-government services adoption in terms of ease of interacting with system, skill required, ease of understanding and using the system in their work (Venkatesh *et al*., 2003). When employees believe that using a particular e-government service will be free of physical and mental effort, they will adopt the e-government service. Therefore the government needs to provide e-government services that are easy to learn and use, to train employees in the use of the e-government services and to avail a technical team to assist with system difficulties and maintenance. This will impact on their intention to use and adopt the e-services leading to success in the e-government adoption process.

Perceived Usefulness

Perceived Usefulness is the degree to which an individual believes that using a particular system would enhance his or her job performance (Davis, 1989; Venkatesh *et al*., 2003). Kumar *et al*. (2007) integrated perceived usefulness to include work more quickly, job performance, increase in productivity, effectiveness and make job easier, with regard to system use (Davis, 1989). In

this study perceived usefulness is used with regard to information security and e-government services adoption in terms of improved job performance, enhanced job effectiveness, increased productivity, and accomplishing tasks at work more quickly (Venkatesh *et al*., 2003). If an employee believes that using a particular e-government service would help them perform their job better they would consider the provided e-services useful and adopt it. Thus the government needs to provide e-government services that will enhance the employees' job performance. This will impact on the employees' intention to use and adopt the e-government system resulting into successful e-government adoption.

4.5.2 Contribution from Bwalya and Healy (2010) to the Model

In order to ensure availed e-government systems are trusted and adopted, there have been different efforts by e-governments to get their security right. This has resulted into the development of different e-government adoption models. Conklin (2007) recommended using adoption of information security as a domain for research to enable constructive change in e-government adoption. Tassabehji (2005) suggested using the model for managing e-government security for the sake of promoting citizen inclusion. Alfawaz *et al*. (2008) stated the key aspect as the country's context where the phenomenon is deployed and operates as each country has its unique setting and constraints to e-government security management. There is thus a challenge as regards to getting a suitable model for use that addresses the e-government security management context of a country such as Uganda. Therefore to address this information security gap with regard to the adopting country context the study presents a model for use for e-government adoption that incorporates factors impacting on e-government adoption in the Ugandan context.

Bwalya & Healy's (2010) model that incorporated factors that may limit the penetration of e-government in an African setup such as Uganda was used in this study. This model is mainly based on TAM (Davis, 1989) with some constructs from Wangpipatwong *et al*. (2008). Moon and Kim (2001) as cited in Bwalya & Healy (2010) stipulated that the TAM has to be given extra factors or included with other IT acceptance models to provide an even stronger model that is commensurate to any given environment. Bwalya & Healy (2010) extended Davis' TAM to take into consideration local conditions so that the adoption model may be commensurate with promoting the growth of e-government in the SADC region.

The model by Bwalya & Healy (2010) that extends TAM so that local conditions and the multi-dimensionality of e-government are addressed is an essential model for use in this study for investigating and understanding e-government adoption from an information security perspective. This incorporation of local conditions makes this model generic and relevant for use in other transitioning countries such as Uganda. The model's main constructs in addition to perceived usefulness and perceived ease of use (Davis, 1989) include e-government adoption and continuance use of e-government (Wangpipatwong et al., 2008), the added factors of ICT infrastructure plus lower access costs, both English and local language content, risks and local culture, data privacy and security, appropriate and continued user support and finally appropriate legal, regulatory plus institutional frameworks (Bwalya & Healy, 2010).

Appropriate ICT Infrastructure plus Lower Access Costs

Infrastructure as used in the study includes hardware and software evaluated according to the properties of confidentiality, integrity and availability (Tassabehji, 2005). Bwalya & Healy (2010) stated that this construct can positively impact on usability and correspondingly on perceived ease of use and the overall intension to use and adopt e-government. Bwalya (2009), also states that the construct of adequate and inexpensive IT infrastructure can significantly influence e-government adoption. According to this study, if apt infrastructure evaluated according to the above properties is set up it will impact on perceived ease of use by enabling protection of the e-government system and information. This in turn impacts on employees' perceptions that the provided e-system is secure making them adopt the e-government services. ICT infrastructure appropriate for e-government should be availed in local governments, government ministries, departments and agencies at lower access costs to the employees. This will enable success in e-government adoption in Uganda.

Language of Content (Both English and Local Language)

This refers to the language of content in the e-government services (Bwalya & Healy, 2010). Bwalya (2009) integrated the local language content, cultural incorporation into the cultural awareness factor. The study suggests that cultural awareness is important for e-participation in e-government adoption. In this study, language of content is measured in terms of both English and local language content. Language of content has a significant positive impact on easing the complexity of use of e-government services and applications and therefore will impact positively

on perceived ease of use in e-government (Bwalya & Healy, 2010). E-government services in Uganda need to be provided in a language understood by all the users, both English and local language. This eases on the complexity of using these e-services and applications. This will in turn impact on perceived ease of use and the adoption of the e-government system by the users.

Risks, Local Culture

Perceived risk is the citizen's subjective expectation of suffering a loss in pursuit of a desired outcome and is composed of behavioral and environmental uncertainty (Belanger & Carter, 2008). Kumar *et al*. (2007) integrated the construct of perceived risk identifying financial, performance, psychological, social, convenience and overall risk (Pires *et al*., 2004; Ueltschy *et al*., 2004) into perceived risk. According to Alfawaz *et al*. (2008), culture has a significant impact on how technology is perceived, used and adapted. Additionally, Bwalya (2009) claim that culture awareness is important for e-participation in e-government adoption. Kumar *et al*. (2007) state that, perceived risk and website design directly influence e-government adoption. In contrast Belanger & Carter (2008) found that risk perceptions did not decrease citizen's intention to use an e-government service. In this study perceived risk and local culture are addressed in the view that perceived risk and local culture if not controlled may have a negative impact on the adoption of e-government (Bwalya & Healy, 2010). The government as the provider of the e-government system needs to incorporate the local culture aspect and reduce the risk perceived in using e-government. This will ensure success in e-participation by the users and in the adoption process.

Data Privacy and Security

Security is the protection of transactions via the e-government system and this is with regard to securing the entire e-government platform (Löfstedt, 2005). Privacy is with regard to the users (employees') privacy (Tassabehji, 2005). Löfstedt (2005) states that security is critical since it can influence the willingness to adopt the provided e-services. Tassabehji (2005) integrates security and privacy and according to this study security together with privacy and trust make up security (Tassabehji, 2003; Patton & Josang, 2004; Yousafzai *et al*., 2005) which is a main obstacle in the growth and adoption of e-commerce. Kumar *et al*. (2007) also incorporated the variable of privacy concerns and systems security concerns (Miyazaki and Fernandez, 2001) under user characteristics. In this study, user characteristics to include perceived risk and data security and privacy directly influence e-government adoption. The study thus addressed the

aspect of data privacy and security. Data privacy and security, if not controlled, may negatively impact on the adoption of e-government (Bwalya & Healy, 2010). The entire e-government platform in Uganda should be secured to enable data privacy and security. Ensuring security over the e-government system will impact on users' willingness to adopt the provided e-government services which is important for successful e-government adoption.

Appropriate and Continued User Support

This refers to support infrastructure in place to include organizational and technical infrastructure to support e-government services use. Venkatesh *et al*. (2003) integrated a similar construct identifying guidance in system selection, specialized instructions concerning system and a specific person or group available for assistance with system difficulties (Thompson *et al*., 1991) into facilitating conditions. Facilitating conditions were found to have a direct influence on usage of e-government (*Ibid*). Therefore this study addressed the factor of continued user support. A dedicated and user support mechanism may assure individual employees of appropriateness of engaging in e-government and this will positively impact on both e-government adoption and continuance use of e-government (Bwalya & Healy, 2010). Local government, government ministries, departments and agencies should ensure a dedicated and appropriate user support mechanism is in place in the e-government system. Providing this support mechanism helps overcome difficulties involved in using the e-government services. This will result into the adoption and continuance use of e-government in Uganda.

Legal, Regulatory and Institutional Frameworks

These frameworks provide the basis for ensuring an adequate level of compliance to international regulations and laws as well as giving internal direction (Alfawaz *et al*., 2008). Tassabehji (2005) included soft management factors identifying management and organizational policies, controls, regulations, legislature human resource management and training under this construct. In the study the construct of soft management factors is addressed as a management aspect to ensure actual security in e-government. Alfawaz *et al*. (2008) claim that existence of relevant regulations and laws have an impact on effectiveness of e-government security management. In this study this construct is measured with regard to legal frameworks in terms of legal, regulatory and institutional frameworks. legal, regulatory and institutional frameworks will positively impact on motivation of employees to engage, adopt and continue the use of e-government (Bwalya &

Healy, 2010). The government of Uganda should put in place appropriate legal, regulatory and institutional frameworks with regard to e-government system use. Having effective frameworks in place to ensure adequate level of compliance to the accepted use of the e-government system will enable e-government users to adopt and continue using the e-government system.

E-Government Adoption

E-government Adoption is the actual use of the e-government services (Anthopoulose *et al*., 2010). Although e-government has been implemented, its adoption still remains a challenge with the adoption rates still low. There is need to understand the factors that cause e-government acceptance and adoption. E-government is accepted where users believe its use is beneficial in making a change like better service delivery. Government ministries, departments, agencies and local governments in Uganda should incorporate the different factors affecting e-government adoption like information security to enable an appropriate e-government adoption framework to be put in place. Having such a framework will not only affect the employees and users' willingness to adopt but also their intention to use and the frequency of using the provided e-government services. This will lead to success in the overall adoption process and continuance use of e-government in Uganda.

Continuance Use of E-government

A challenge to continuance use of the e-government system is the relationship existing between the government providing e-government and the users of the e-government services. Government in Uganda needs to build a long term trust relationship between them and the users by providing an appropriate e-government system as promised to the users. The effectiveness of the e-government system makes the employees trust the e-services (Tassabehji, 2005). This will impact on the relationship built between the government providing the e-government system and the users of the e-services (*Ibid*). This relationship is very significant for the users' long term active inclusion, participation and their continuance use of e-government.

Bwalya & Healy's (2010) model extended TAM (1989) and incorporated additional factors addressing the local context and multi-dimensionality of e-government aspects. Although the extension makes the model a stronger model proper for any given environment, the model has shortcomings in that it addressed security and privacy in the context of e-government websites

and applications. Data privacy and security only addresses aspects of confidentiality and accessibility and not information security across the entire e-government infrastructure for success of the adoption process. Security in e-government services adoption is broad to include factors of confidentiality, integrity, availability, accountability and trust which strengthen user services such as authentication, authorization and reliability (Alfawaz *et al*., 2008). The study's focus is on the Southern African Development Community bloc countries. The model has also not been formally empirically validated to verify its appropriateness to SADC countries and suggested further in the study is the need to examine the dissimilar antecedents of each construct for a clarified understanding of the model (Bwalya & Healy, 2010).

Though Bwalya & Healy's (2010) model did not sufficiently address important factors of information security and trust which when left out may impact on the penetration of e-government in an African context, it was considered the most appropriate model to guide the study. This is because the model is an extension of TAM, an empirically tested model and it also incorporated factors such as appropriate ICT infrastructure + lower access costs identified among important factors affecting e-government services adoption in Uganda. For this reason, information security and trust factors were identified from other studies and the field survey and incorporated into Bwalya & Healy's (2010) model as additional requirements for e-government adoption. Results from the field survey of the needed model requirements to include the factors of security culture, information security and trust factors therefore address the main identified gap of the model which was information security and trust for the entire e-government infrastructure. This was appropriately addressed in the information security e-government adoption model.

The new extended model therefore comprises of 1) Bwalya & Healy's (2010) model constructs of perceived usefulness, perceived ease of use, infrastructure plus lower access costs, both English and local language content, risks and local culture, data privacy and security, appropriate and continued user support, appropriate legal and regulatory plus institutional frameworks and continuance use of e-government and 2) the additional factors (requirements) from the field study data analysis to include Security culture factors (information security awareness campaigns, supporting legislation, suitable security and privacy policies and skills training), information security factors (confidentiality, integrity and accountability) and trust factors (information

accuracy, information reliability, information relevancy and easy to use systems) . The new factors incorporated thus addressed the main identified gap of information security and trust for success in e-government adoption.

4.5.3 Contribution from Data Analysis

The field study results (the information security e-government adoption factors identified in chapter 4) and the reviewed literature were used to attain the requirements needed to develop the model. These requirements from the field study results were then used to develop the information security e-government adoption model for Uganda. This was achieved by classifying the obtained information security factors into the following three groups as summarized in this section:

Security Culture Factors

Security culture factors include formulation of supporting legislation for e-government systems, skills training for proper e-government systems use, formulation of suitable security and privacy policies for e-government systems and information security awareness campaigns to increase e-government use. Security culture factors impact on acceptance to technology and the compliance to information security in e-government. The summarized factors for the information security model from the above factors are supporting legislation, skills training, suitable security and privacy policies and information security awareness campaigns.

Information Security Factors

Information security factors include confidentiality / privacy (e-tax information accessibility, e-mail personal information accessibility, e-health personal information privacy, e-commerce transactions confidentiality, e-banking information accessibility and e-voting personal information confidentiality), integrity (e-tax data integrity, e-mail data integrity, e-commerce data integrity, e-banking data integrity, e-health data integrity and e-voting data integrity) and finally accountability (accountability by e-tax data recipients and senders, accountability by e-mail data recipients and senders, accountability by e-commerce data senders and accountability by e-banking data recipients). These factors are needed to ensure protection and security of the e-government system and information. The factors of confidentiality, integrity and accountability are identified from the information security factors.

Trust Factors

Trust factors are ensuring information accuracy in e-government systems, information reliability in e-government systems, provision of easy to use e-government systems and information relevancy in e-government systems. These factors are needed to ensure users confidence and trust in the e-government system. The factors summarized from trust, for the information security based model are information accuracy, information reliability, information relevancy and easy to use systems.

4.5.4 Relationships in the Model

E-government adoption in the model is dependent on all the above discussed factors as shown in figure 4.8. Relationships are suggested between the new factors and e-government adoption. Security culture factors are positively related to the adoption of e-government services and system. Information security factors have a significant positive relationship with the adoption of e-government services and system. Trust factors are significantly correlated with e-government adoption and correspondingly continued use of e-government. Each of these added components is thus related to a higher level construct success; security culture factors influence e-government services adoption, information security factors influence e-government services adoption and trust factors influence e-government services adoption. All these factors influence e-government adoption.

Relationships suggested between the incorporated information security factors and e-government adoption were assessed using regression analysis as presented in the subsequent sections. According to the relationships, success in e-government adoption in Uganda from an information security view point is dependent on confidentiality, integrity, accountability, trust and security culture factors. Correlation and regression analyses were performed to test the relationships. Correlation analysis was used to measure strength of the relationship between the variables confidentiality, integrity, accountability, trust, security culture and the variable e-government adoption. Regression analysis was used to determine how much of the variability in the dependent variable e-government adoption is explained by variability in the independent variables of confidentiality, integrity, accountability, trust and security culture. Use of regression analysis helped in identifying the independent variables having significant relationship with e-

government adoption. This enabled the development of a regression model that explains an information security based e-government adoption model for Uganda.

4.6 Regression Analysis

This section presents the results of the regression analysis of the information security e-government adoption model for Uganda discussed in the previous section 4.5. To evaluate the model, correlation and regression analyses were conducted. Correlation analysis was used to measure the strength of the relationship between the variables confidentiality, integrity, accountability, trust, security culture and the variable e-government adoption. Regression analysis was used to determine how much change in the dependent variable e-government adoption is explained by how much change in the independent variables of confidentiality, integrity, accountability, trust and security culture (Kothari, 2004). Variables having significant relationship with e-government adoption were also attained.

In testing the relationships in the model, the study objective 2 of development of a model of e-government adoption that relates the information security factors to the adoption process in Uganda was achieved. To assess the model, relationships as suggested between the information security factors and e-government adoption were tested. Regression analysis was used to test the following assumed relationships H1, H2, and H3 as proposed in figure 2.7 (Conceptual model) and described in section 4.5. The relationships are here restated as:

1) **H1:** Security culture factors are related to the adoption of e-government services and systems in Uganda.

2) **H2:** Information security factors have a relationship with the adoption of e-government services and systems in Uganda.

3) **H3:** Trust factors are related to and help to predict the e-government adoption process in Uganda.

Model testing using correlation and regression analyses enabled confirmation and understanding of the relationship between the variables (confidentiality, integrity, accountability, trust, and security culture and e-government adoption) as per the study context.

Correlation Analysis

Correlation analysis is a measure of the degree of relationship between variables using either Spearman's coefficient of correlation or Pearson's coefficient of correlation (Kothari, 2004). In this study, Pearson's coefficient of correlation was used to measure the strength of the relationship between the variables. The output of the correlation calculation is the correlation coefficient or (r). This is the product moment correlation coefficient (r) ranging between -1 and 1 (Kothari, 2004). Positive value of r indicates positive relationship between the two variables, negative r value indicates negative relationship, and zero value indicates no relationship.

Pearson's correlation coefficient was statistically computed using SPSS to measure the strength of the relationship between the variables confidentiality, integrity, accountability, trust, security culture and adoption of e-government services. a value of 1 shows perfect positive correlation (as one variable increases, the second increases in a linear form), a -1 value shows perfect negative correlation (as one variable increases, the second decreases) and zero value shows no correlation (Kothari 2004). Pearson's correlation coefficient results computed for each individual variable and the variable of e-government adoption are presented in appendix V. The correlation coefficient (r) results for each factor are illustrated below in table 4.8

Table 4. 8: Pearson's Correlation Coefficient

		E-government Adoption (services)
Confidentiality /accessibility	Pearson Correlation Sig. (2-tailed) N	.567(**) .000 225
Integrity	Pearson Correlation Sig. (2-tailed) N	.571(**) .000 225
Accountability	Pearson Correlation Sig. (2-tailed) N	.613(**) .000 225
Trust	Pearson Correlation Sig. (2-tailed) N	.576(**) .000 225
Security culture	Pearson Correlation Sig. (2-tailed) N	.503(**) .000 224
E-government Adoption (services)	Pearson Correlation N	1 225

** Correlation is significant at the 0.01 level (2-tailed)

The results in table 4.8 show the correlation coefficients that were calculated to measure the strength of the relationship between the variables. The results show that there is positive relationship between confidentiality and e-government adoption (r=.567**), between integrity and e-government adoption (r=.571**), between accountability and e-government adoption (r=.613**), between security culture and e-government adoption (r=.503**) and between trust and e-government adoption (r=.576**).

Pearson's correlation coefficient results confirmed that there is moderate relationship between the variable of confidentiality and the variable of e-government adoption (r=.567**, p< .000). The results in table 4.8 show that there is moderate relationship between the variables integrity and e-government adoption (r=.571**, p< .000). The relationship between the variable of accountability and the variable of e-government adoption (services) was also confirmed to be important (r=.613**, p< .000). The correlation coefficient results above validated that there is moderate relationship between variables of security culture and e-government adoption (r=.503**, p< .000). There is also important relationship between the variable of trust and the variable of e-government adoption (r=.576**, p< .000) according to the above results.

Therefore the correlation coefficient results confirmed that there is positive and moderate relationship between each of the variables of trust, confidentiality, security culture, integrity and the variable of e-government adoption. This correlation analysis hence provided understanding of the relationship between the above information security factors and e-government adoption as shown in the model.

4.6.1 Regression Analysis

Different statistical techniques are used for studying linear relationship between variables (Okereke, 2011). Two methods are normally used in identifying how different variables in a process are related. Simple regression that assumes that one variable is dependent upon another single independent variable and multiple regression analysis that assumes that one variable is dependent upon multiple independent variables (Kothari, 2004). Use of regression analysis enables estimating the effect of some explanatory variable on the dependent variable. This statistical method plots a line of best fit to the data using the least-squares method. A line which minimizes the total of the squared deviations of the actual observations from the calculated line is

computed (Lucey, 2002, Okereke, 2011). In order to study the linear relationship between variables, multiple regression analysis is used. This method was deemed best for use since there was one dependent variable and more than one independent variable to be analyzed.

In the study, multiple regression analysis was computed on SPSS to study the relationship between the dependent variable e-government adoption (services) and the independent variables confidentiality, integrity, trust, security culture and accountability.

A general form for the relationship is given by the equation:

Y= β_0 + β_1(Confidentiality) + β_2(Integrity) + β_3(Accountability) + β_4(Security culture) + β_5(Trust) + u

Where

Y= Dependent variable (E-government adoption) .

β_0, β_1,…β_5 parameters = The y-intercept and the slope of the relationship, respectively (Calculated by dividing change in the dependent variable by change in the independent variables).

0= (Other factors constant).

$x_1, \ldots, x_5$ = Independent variables (Confidentiality, Integrity, Accountability, Security culture and Trust factors).

u= Error (disturbance). The vertical distance between the values of observed Y and 'fitted Y'.

A multiple regression analysis was performed to examine the relationship between e-government adoption as the dependent variable and confidentiality, integrity, accountability, security culture, trust as the predictor variables. Table 4.9 below presents a summary of the multiple regression analysis results.

Table 4. 9: Regression Analysis: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.692(a)	.479	.467	.54784

a Predictors: (Constant), Security culture, Confidentiality, Trust, Accountability, Integrity

Table 4.9 presents the model summary and at the footnote to the model summary, are the predictors that are relevant for the R and R-Square. The predictors of e-government adoption from an information security perspective in the model include security culture, confidentiality, trust, integrity and accountability. R is the Pearson Product Moment Correlation Coefficient. The multiple correlation coefficient R, which is the square root of R Square shows how strongly the multiple independent factors relate to the one dependent variable. R varies from 0 to 1 and in table 4.9 above, R=0.692 which implies that there is a strong relationship between the multiple independent factors and the dependent variable. R-Square the Coefficient of determination, is the amount of variance in the dependent variable (e-government adoption) which is explained by the independent variables (confidentiality, integrity, accountability, security culture and trust). R-Square values vary from 0 to 1; 0 indicating no relationship, 1 indicating a perfect relationship. The closer the R-Square value is to 1.0, the better the model (meaning one can better predict one term from another) and the closer the R-Square value is to 0, the worse the model (meaning knowing one term does not help one know the other term at all). According to the results above, R-Square is 0. 479 and this means that 47.9% of the variance in e-government adoption (services) from an information security perspective can be predicted from the variables confidentiality, integrity, accountability, security culture and trust. Other unidentified factors account for the remaining 52.1% which is the proportion of unexplained variance in the dependent variable (1-R=0.521). Adjusted R-square is an adjustment of the R-Square that penalizes the addition of irrelevant predictors to the model. Adjusted R-Square therefore tries to yield a more honest value to estimate R-Square. Adjusted R-Square is 46.7% and the standard error of estimate (standard deviation), 0.548.

The Regression analysis, ANOVA (b) results between the predictor variables confidentiality, integrity, accountability, security culture, trust and the dependent variable e-government adoption (services) are shown in table 4.10

Table 4. 10: Regression Analysis: ANOVA (b)

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	60.047	5	12.009	40.014	.000(a)
	Residual	65.428	218	.300		
	Total	125.476	223			

a Predictors: (Constant), Security culture, Confidentiality, Trust, Accountability, Integrity

b Dependent Variable: E-government Adoption (services)

Results in table 4.10 above, show that a significant model emerged from the analysis ($F(5, 225) = 40.014$, $p<0.000$). The significance value (p-value) which shows whether the independent variables reliably predict the dependent variable associated with the F value (40.014) is very small (0.000). This p-value is small compared to the alpha level (0.05). The smaller the p-value compared to the alpha level (0.05) suggests that the independent variables show a statistically significant relationship with the dependent variable and the greater the p-value than the alpha level (0.05) means the independent variables do not show a statistically significant relationship with the dependent variable. Results in table 4.10 show that the independent variables have a significant relationship with the dependent variable because their p-value ($p=0.000$) is less than the level of significance ($p<0.05$). This means that holding other factors constant the independent variables (security culture, confidentiality, trust, accountability and integrity) reliably predict the dependent variable e-government adoption (services).

The Regression analysis Coefficients (a), in table 4.11 for the variables confidentiality, integrity, accountability, security culture, trust and e-government adoption (services) were also computed to determine what the nature of relationship between these variables is and how much change in the independent variables is associated with how much change in the dependent variable e-government adoption.

In Table 4.11, B are the un-standardized coefficients. These values of the regression equation predict e-government adoption (services) from confidentiality, integrity, accountability, security culture and trust. A positive coefficient for B indicates positive relationship and negative coefficient indicates negative relationship. These values are measured in their natural units. Std. Error, is the standard error and this measures the extent to which the prediction can be trusted. Beta values are the standardized coefficients and these values measure the strength of the relationship between each of the variables of confidentiality, integrity, accountability, security culture and trust to e-government adoption. The higher the beta value the larger the impact of the independent variable in explaining variation of the dependent variable. These coefficients are obtained when all the variables (e-government adoption, confidentiality, integrity, accountability, security culture and trust) in the regression are put on the same scale and the regression is run. Beta values are measured in standard deviation units. T values are the tolerance values and they measure the correlation between the independent variables (confidentiality, integrity, accountability, security culture and trust). Tolerance values can vary between 0 to 1 and the closer the variable value to zero, the stronger the relationship. Sig. is the significance value (p) and this explains whether confidentiality, integrity, accountability, security culture and trust variables reliably predict the variable of e-government adoption. A smaller p-value indicates that the independent variable has a significant relationship with the dependent variable. The Coefficients (a) for each variable are presented in Table 4.11 below

Table 4. 11: Regression Analysis: Coefficients (a)

Coefficients(a)						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig. (p value)
		B	Std. Error	Beta		
1	(Constant)	-0.736	0.236		-3.118	0.002
	Confidentiality	0.242	0.060	0.256	4.030	0.000
	Integrity	0.057	0.068	0.069	0.835	0.404
	Accountability	0.219	0.072	0.242	3.034	0.003
	Security culture	0.089	0.062	0.098	1.431	0.154
	Trust	0.170	0.076	0.167	2.235	0.026
A	Dependent Variable: E-government Adoption (services)					

The multiple regression analysis results in table 4.11 above show positive B coefficients which indicates that the independent variables confidentiality, integrity, accountability, security culture and trust have positive relationships with e-government adoption. From the analysis, the significant variables are confidentiality (p=0.000), accountability (p=0.003) and trust (p=0.026). This is because their p-values compared to the level of significance (0.05) are smaller. Thus the variables of confidentiality, accountability and trust have a significant relationship with e-government adoption. As seen in the results in table 4.11, confidentiality (β=0.256) has the largest impact in explaining variation of e-government adoption (services). This is followed by accountability (β=0.242) then trust (β=0.167), security culture (β=0.098) and integrity (β=0.069).

Therefore e-government adoption is dependent on the information security factors of confidentiality (β=.256, p<.000), accountability (β=.242, p<.003) and trust factors (β=.167 p<.026), that had a significant relationship with e-government adoption at the level 0f 0.05. Integrity and security culture factors were found not to be significant. This is illustrated using the regression model in the following figure 4.9 below.

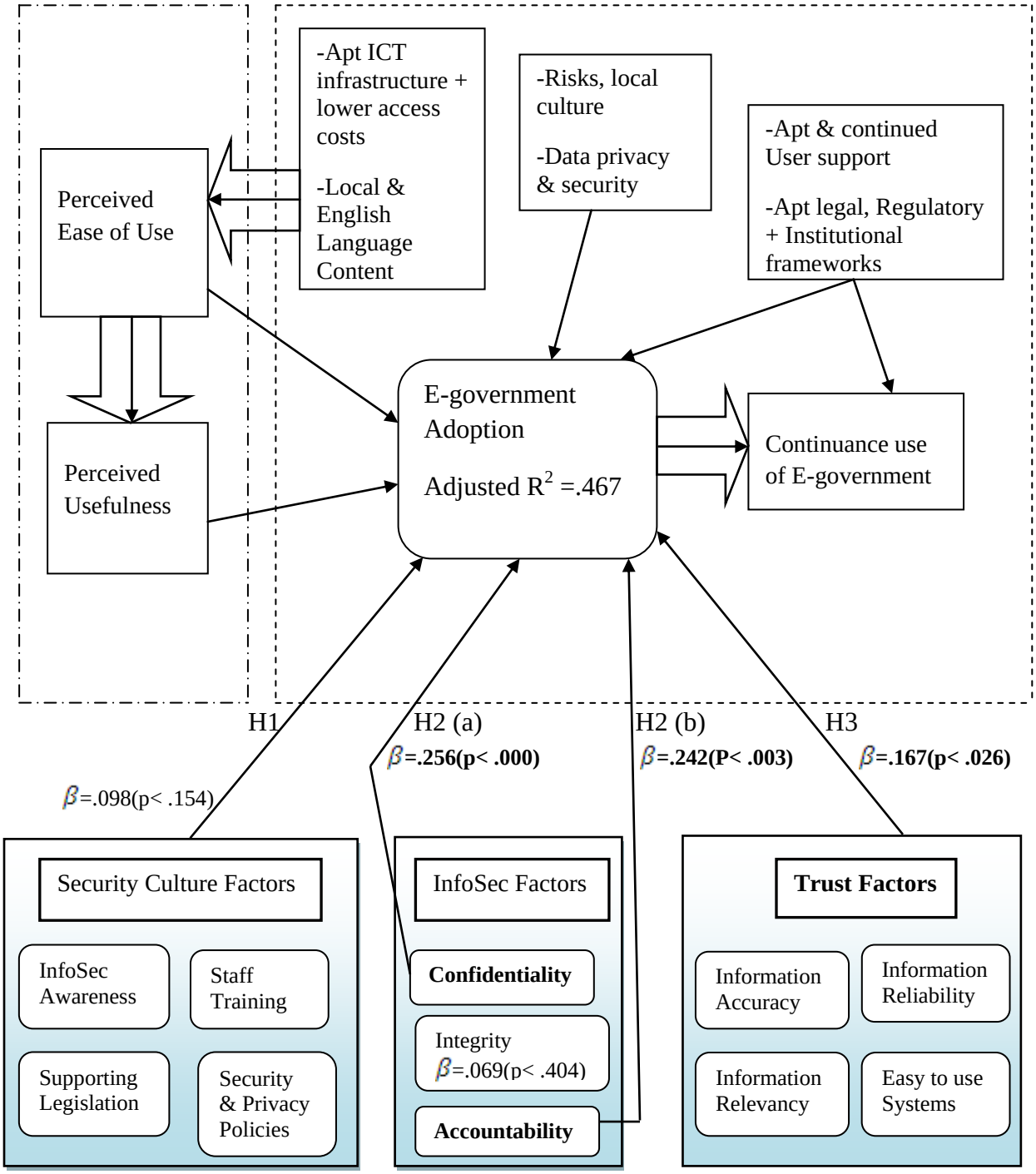

Figure 4. 9: Validated Factors for E-government Adoption from an InfoSec View (p<.05)

4.7 Summary

The regression analysis as observed in figure 4.9 shows that, all the assumed relationships H1, H2, H3 are supported as indicated by the following equations:

H1: Security culture factors (information security awareness, security and privacy policies, staff training and supporting legislation) are related to the adoption of e-government services and systems. The relationship for this assertion as illustrated in table 4.11 as given by the equation 4.1 and 4.2 is:

$$Y = \beta_0 + \beta_4(\text{Security culture}) \quad \text{(Equation 4.1)}$$

$$Y = -0.736 + 0.089\ (x_4) \quad \text{(Equation 4.2)}$$

Where:

Y= Dependent variable (E-government adoption)

β_0 = - 0.736 is the other constant factors

β_4 = 0.089 in this expression, b_4 represents the proportion of change in the levels of adoption of e-government services that is predicted by a change in the levels of security culture factors.

X_4= Security culture factors. The value of security culture (x_4) has to be assumed in order to predict the expected value of Y (e-government adoption) which is the dependent variable.

Despite the insignificant relationship ($p=0.154<.05$) in the analysis, the positive relationship assumed in the conceptual model between security culture factors and the adoption of e-government services and system was supported.

H2: Information security factors (confidentiality, integrity and accountability) have a relationship with the adoption of e-government services and system. The relationship for this assertion as illustrated in table 4.11 as given by the equation 4.3 and 4.4 is:

$$Y = \beta_0 + \beta_1(\text{Confidentiality}) + \beta_2(\text{Integrity}) + \beta_3(\text{Accountability}) \quad \text{(Equation 4.3)}$$

$$Y = -0.736 + 0.242\ (x_1) + 0.057\ (x_2) + 0.219\ (x_3) \quad \text{(Equation 4.4)}$$

Where:

Y= Dependent variable (E-government adoption).

β_0 = -0.736 is the other constant factors

β_1 = 0.242 in this expression, b_1 represents the proportion of change in the levels of adoption of e-government services that is predicted by a change in the levels of confidentiality factors.

β_2= 0.057 in this expression, b_2 represents the proportion of change in the levels of adoption of e-government services that is predicted by a change in the levels of integrity factors.

β_3= 0.219 in this expression, b_3 represents the proportion of change in the levels of adoption of e-government services that is predicted by a change in the levels of accountability factors.

$X_{1,\ 2,\ 3}$ = Information security factors. The value of confidentiality (x_1), integrity (x_2) and accountability (x_3) have to be assumed in order to predict the expected value of Y (e-government adoption) which is the dependent variable.

The coefficients of the three InfoSec factors were positive confirming the assumed relationship with the dependent variable (e-government adoption). But with regard to statistical significance, confidentiality and accountability were the only ones that had significant influence on e-government adoption with p-values indicated by 0.000 and 0.003 respectively.

H3: Trust factors (information accuracy, reliability, relevancy and easy to use systems) are related to and help to explain the e-government adoption process. The relationship for this assertion as illustrated in table 4.11 as given by the equation 4.5 and 4.6 is:

$$Y= \beta_0 + \beta_5(\text{Trust}) \qquad \text{(Equation 4.5)}$$

$$Y= -0.736+ 0.170\ (x_5) \qquad \text{(Equation 4.6)}$$

Where:

Y= Dependent variable (E-government adoption).

β_0 = -0.736 is the other constant factors

β_5 = 0.170 in this expression, b_5 represents the proportion of change in the levels of adoption of e-government services that is predicted by a change in the levels of trust factors.

X_5 = Trust factors. The value of trust (x_5) has to be assumed in order to predict the expected value of Y (e-government adoption) which is the dependent variable.

In relation to trust the results support the assumed relationship between this explanatory variable and the dependent variable as given by the positive Beta coefficient (0.170) which was also significant with p-value equal to 0.026.

For success to be attained in e-government adoption to include e-tax, e-health, e-banking, e-commerce, e-mail and e-voting services in Uganda, information security should be incorporated into the adoption process. Understanding of the information security factors for e-government adoption in Uganda is thus essential. The study therefore evaluated the extended model by Bwalya & Healy (2010) using information security factors so as to determine the strength of the relationship between the variables and the factors having significant association with e-government adoption. The results showed that there is positive correlation between the variables. Results also showed that the factors of confidentiality, accountability and trust have significant relationship with e-government adoption at significance level 0.05 while security culture and integrity factors were not significant as discussed below.

Confidentiality factors had the most significant influence on e-government adoption (services). Incorporating confidentiality factors in e-government will ensure improved adoption of e-government services as users will be assured of the privacy of their personal information and transparency of the e-government system.

In as regards to accountability factors, the results showed that accountability factors have significant relationship with e-government adoption. E-government users accounting for their actions while using e-government systems will lead to improved adoption of e-government services as users will trust and use the provided e-services.

Trust factors are also significantly related with e-government adoption (services). This means that when trust factors are incorporated in e-government, a long term trust relationship will be built

between e-government users and the government providing e-government systems resulting into improved e-government adoption as well as its continued use.

The factors of integrity and security culture did not have significant association with e-government services adoption as depicted in the multiple regression analysis results.

Therefore government ministries and local government district units should ensure confidentially, accountability and trust factors in e-government in a bid to improve e-government adoption (e-health, e-tax, e-mail, e-banking, e-commerce and e-voting services.) According to the multiple regression analysis results the extended model accounted for up to 47.9% of the variance in e-government services adoption from an information security perspective, other factors constant. Thus the extended model can be reliably used to make deductions and recommendations for government ministries and local government district units in line with incorporation of information security and e-government services adoption in Uganda.

CHAPTER FIVE

Discussion of Results and Conclusions

5.1 Introduction

The previous chapter presented the description of the model and its testing. This Chapter discusses the results from the data analysis of the survey, in relation to the literature. Also included in this chapter is a summary of the contributions of this study, the implications, limitations of the study, and recommendations for future research.

5.2 Discussion of Findings

The purpose of this study was to create an e-government adoption model that explains the relationship between information security factors and the successful adoption of e-government. Based on the study purpose, the research set out to create a model that explains the relationship between information security factors and the successful adoption of e-government in Uganda. To achieve this aim, the study set out to answer the following two specific research questions.

i. What are the information security factors that affect adoption of e-government in Uganda?
ii. How can security of e-government services be improved to increase public trust hence adoption of e-government?

These questions provided guidance for the research and they were addressed through the following specific objectives.

1. To determine the information security factors affecting the e-government adoption process in Uganda.
2. To develop a model for e-government adoption that relates the information security factors to the adoption process in the Ugandan context.

The findings from the analysis and discussion are presented in the following sections as themes corresponding to the research questions.

5.2.1 Requirements for Information Security

The following requirements security culture, information security (confidentiality, integrity, accountability) and trust factors are here discussed.

Security Culture Factors as Requirements

The results indicated that security culture factors are a requirement for e-government adoption (table 4.8). To measure security culture for this study, four variables selected from previous literature were used. These were supporting legislation, staff training, suitable security and privacy policies and information security awareness campaigns. The findings of the study indicate that there is positive relationship between security culture factors and e-government adoption (r=.503**, p< .000) with items 1, 2, 3, 4 correlated with e-government services adoption at (r=.448**, p< .000), (r=.436**, p< .000) (r=.432**, p< .000) and (r=.415**, p< .000) respectively as shown in appendix v. The moderate correlation score indicates that security culture factors contribute to successful adoption of e-government services. These findings are in agreement with that reported by Alfawaz *et al*. (2008). These authors state that security culture factors are important to technology acceptance such as e-government and they also contribute to compliance to the measures and controls in place to safeguard information assets and ensure information security in e-government. Previous studies considered security culture as vital for success in e-government security (*Ibid*).

Information Security Factors as Requirements

Information security factors are a requirement for e-government adoption according to the results (table 4.8). Three variables from previous literature were used to measure information security for this study. These include confidentiality, integrity and accountability. The study findings show that there is positive relationship between information security factors confidentiality (r=.567**, p< .000), integrity (r=.571**, p< .000), accountability (r=.613**, p< .000) and e-government adoption. Items 1, 2, 3, 4, 5, 6 for confidentiality correlated with e-government services adoption at (r=.412**, p< .000), (r=.233**, p< .000) (r=.366**, p< .000), (r=.328**, p< .000), (r=.347**, p< .000) and (r=.385**, p< .000) respectively as presented in appendix v. For integrity items 1, 2, 3, 4, 5, 6 correlated with e-government services adoption at (r=.450**, p< .000), (r=.520**, p< .000) (r=.476**, p< .000), (r=.497**, p< .000), (r=.513**, p< .000) and

(r=.481**, p< .000) while for accountability items 1, 2, 3, 4, 5, 6 correlated with e-government services adoption at (r=.519**, p< .000), (r=.442**, p< .000) (r=.502**, p< .000), (r=.482**, p< .000), (r=.516**, p< .000) and (r=.519**, p< .000) respectively as shown in appendix v. These moderate correlation scores indicate that confidentiality, integrity and accountability factors contribute to successful e-government services adoption. The findings are in conformity with earlier studies. Alfawaz *et al*. (2008) state that traditionally security is concerned with information properties of confidentiality, integrity and availability which strengthen user services such as accountability. Wangwe *et al*. (2009) suggested that for government agencies and departments to provide integrated services to citizens, information security needs to be addressed to ensure confidentiality and integrity of information transmitted over the e-government system. Earlier research also considered information security factors of confidentiality, integrity and accountability as essential for success in e-government services adoption from an information security view (Tassabehji, 2005; Wangwe *et al*., 2009).

Trust Factors as Requirements

Results from the study showed that trust factors are a requirement for the adoption of e-government (table 4.8). To gauge trust in the study context, five variables got from earlier studies were used. These were information accuracy, information reliability, easy to use e-government systems, e-government content in local language and information relevancy. The study findings indicate that there is positive relationship between trust factors and e-government adoption (r=.576**, p< .000) with items 1, 2, 3, 5 correlated with e-government services adoption at (r=.507**, p< .000), (r=.504**, p< .000) (r=.426**, p< .000) and (r=.418**, p< .000) respectively as depicted in appendix v. Item 4, e-government content in local language was later dropped because it had a weak correlation with e-government adoption (r=.207**, p< .002). The moderate correlation score indicate that trust factors contribute to successful adoption of e-government services. These findings correspond with earlier research. Tassabehji (2005) states that trust factors are very essential in determining the relationship built between government and e-users and this relationship is needed for users' active inclusion and participation in e-government services. Previous studies found that trust factors are crucial for success in e-government adoption (Belanger & Carter, 2008; Alsaghier *et al*., 2009).

Based on the correlation analysis results, the information security factors of confidentiality, integrity, accountability, security culture and trust are important requirements for e-government services adoption in the study context.

5.2.2 Relating Information Security to E-government Adoption

Security Culture and E-government Adoption

The results indicated that there is no significant relationship between security culture factors and e-government adoption though the relationship between security culture and e-government adoption is positive (table 4.11). The findings of the study show the relationship between security culture factors and e-government adoption at (p=0.154) in figure 4.9. The p-value score greater than the significance level (0.05) indicates that security culture factors do not significantly influence e-government services adoption. These findings are consistent with some previous studies. Alfawaz *et al*. (2008) state that security culture plays an essential role in ensuring e-government security and this contributes to e-government adoption. Tassabehji (2005) in their study developed measures for soft management factors and several of the variables they used to determine soft management factors are related to security culture. From their study, it was suggested that these variables are important to actual security in e-government and it is this security that ensures the adoption of e-government services.

This study did not find significant relationship between security culture and e-government adoption. This is because Uganda is one of the developing countries that recently adopted e-government with most of these security culture services such as information security awareness, the needed security policies not fully operational and available to the users. Therefore the lack of significant relationship, may well be because users of e-government services with regard to the study are not aware of the existent security culture services and have not utilized them.

Information Security and E-government Adoption

From the analysis it was found that there is significant relationship between the factors confidentiality, accountability and e-government adoption but no significant relationship between integrity and e-government adoption (table 4.11). The study findings indicate the relationship between confidentiality factors and e-government adoption at (p=.000), accountability factors and

e-government adoption at (p=.003) and integrity factors and e-government adoption at (p=.404) in figure 4.9. The p-value score for confidentiality and accountability are smaller than the significance level (0.05) while the p-value for integrity is greater than (0.05). The regression scores indicate that confidentiality and accountability factors significantly influence e-government services adoption while integrity factors do not. These findings contradict some previous studies. According to Tassabehji (2005), evaluating security in e-government is based on the principles of confidentiality, accountability as well as integrity. This is also supported by Wangwe *et al.* (2009). These authors suggest that for integrated services to be provided to citizens, information security should be addressed to ensure information confidentiality and integrity. Earlier studies stated that information security is significantly related to successful e-government adoption and security (Conklin, 2007; Alfawaz *et al*., 2008).

In the present context, significant relationship was found between confidentiality, accountability factors and e-government adoption but no significant relationship between integrity and e-government adoption. Thus the absence of significant relationship between integrity factors and e-government adoption implies that though integrity factors may be required, they are not important for e-government adoption in the study context.

Trust Factors and E-government Adoption

There is also significant relationship between trust factors and e-government adoption according to the results (4.11). The finding of the study indicate the relationship between trust factors and e-government adoption at (p=.026) in figure4.9. The p-value score smaller than the significance level (0.05) indicates that trust factors significantly influence e-government services adoption. These findings are in agreement with previous studies. Alsaghier *et al*. (2009) state that trust in e-government positively influences the intensions of citizens to engage in e-government. Belanger & Carter (2008) also found from their empirical study support for the relationship between trust and e-government services adoption.

Therefore with regard to regression analysis results confidentiality, accountability and trust variables were found to be significantly related with e-government services adoption while security culture and integrity factors were not found to be significant, for the case of Uganda.

5.2.3 Regression Analysis

To develop and test relationships in the model correlation and regression analyses methods were used. Use of Pearson's correlation coefficient provided evidence that each of the variables of security culture, confidentiality, integrity, accountability and trust have positive relationship with the variable e-government adoption. The results also showed that the variable of accountability had the highest positive relationship with e-government adoption (r=.613**, p< .000) in table 4.8.

Multiple regression analysis provided empirical support that factors of confidentiality, accountability and trust (independent variables) significantly explain e-government services adoption (dependent variable). Security culture and integrity factors were not considered significant predictors in the study. This analysis also provided evidence that the predictor variable of confidentiality contributed the highest in explaining the variation in e-government adoption (β=0.256) in table 4.11. Government (ministries, departments, agencies and local government units) thus need to consider integration of these factors in the e-government services they provide to enable successful adoption in Uganda.

Testing of the relationships in the model therefore provided understanding of the relationship between the information security factors of security culture, confidentiality, integrity, accountability and trust to the adoption of e-government services in Uganda. Assessment of this information security model also confirmed the anticipated benefits the model has to offer as well as its appropriateness to Uganda.

5.3 Summary of the Contributions

The study makes significant contribution in the areas of information technology adoption, research and practice.

5.3.1 Contributions to Knowledge

The information security factors affecting the e-government adoption process in Uganda were determined. These include the factors of confidentiality, accountability and trust. The study thus enabled better understanding of the information security factors needed for success in the e-government adoption process.

A model for e-government adoption that relates information security factors to e-government adoption process in the Ugandan context was developed. This is the main contribution of the study. The information security e-government adoption model developed thus provides understanding of the relationship between information security and e-government adoption in Uganda.

The regression analysis conducted to test the relationships in the model developed, supported the assumed relationships between information security factors and e-government adoption. The study extended knowledge in the area of e-government adoption from an information security perspective as the relationships between information security factors and e-government adoption were confirmed. The model is therefore a useful theoretical base for use in guiding successful e-government adoption from an information security view in Uganda.

Contribution to Practice

The findings of this research also suggest important practical implications for the practitioners to like government ministries and local government district units.

Ensuring information security in e-government is vital in influencing users' adoption and continued use of the provided e-government system and services. It is thus essential for practitioners like government ministries using the e-system to deliver services, to be aware of the information security factors that influence e-government adoption and continuance so that e-government information security is improved. The study findings will enable government ministries and local government district units to understand the main issues (information security factors of confidentiality, accountability and trust, challenges and requirements) influencing user's adoption and continued use of the e-government system thereby effectively addressing them. This will therefore enable success in the adoption by making possible that current users are retained and new e- government services users are attained.

The results obtained in this study provide a good insight for use as a reference point with regards to defining appropriate requirements needed in the context of information security. For example, the model helps e-government service providers understand which factor (confidentiality) is most essential in influencing adoption of e-government services within the study context. These findings when used as a basis for evaluating the operations of the e-government system will

enable identification of what changes are needed and the appropriate addressing of these changes thus affecting users' active participation and inclusion in the e-government system.

Government needs to improve the e-government system by tailoring the availed services to cater for end-user concerns. Addressing end user concerns aired out on the challenges and requirements facing the system like unreliability of the available e-services, inconsistent power supply, uneven distribution of appropriate infrastructure in all sectors, inadequacies in the documentation of e-government services and lack of a national disaster recovery plan in place will make the e-government system more user-friendly. This will attract new users to adopt e-government services and retain the actual users as well as ensure their loyalty.

To create new users, the government may use the same approach used to target the actual users of e-government services to determine the important features motivating their actual participation and inclusion in e-government to point out areas of information security that need to be improved or which appropriate information security practices and controls need to be set up to attract the non users as well.

The results indicate that out of a number of factors (security culture, confidentiality, integrity, accountability and trust) identified from existing literature and considered vital for explaining e-government adoption from an information security viewpoint in Uganda, three factors (confidentiality, accountability and trust) significantly influenced e-government services adoption in Uganda. The influence of the remaining factors (security culture and integrity) on e-government adoption in the study area was not significant. Government ministries and district units delivering e-services need to ensure confidentiality, accountability and trust factors in e-government, are adhered to improve adoption rates in Uganda.

All in all the government to include its ministries, departments, agencies and local government district units needs to take up the primary role of influencing e-users' perception of e-government services. This in turn will impact on the attitude and behavior of current and future e-service users leading to successful e-services adoption and continuance.

5.4 Limitations of the Study

Just like any other research, this study has certain limitations. The limitations to the present study are hence presented in this section to place the findings in perspective.

This study was conducted with regards to the e-government adoption process from an information security perspective. As a result, it is possible that the findings may not be applicable to general e-government adoption. There is thus need for further investigation into adoption of e-government services from other perspectives.

The research was carried out within the Ugandan context, a country still developing technologically with most of the e-services still relatively new and some of the provided services not fully operational. As a result it is possible that the findings cannot be applied to technologically leading countries which are different with regards to the functionality of the e-systems.

Finally the correlation and regression analyses were used to measure additional factors of security culture, information security and trust factors with a few already existing factors to include language content, security and privacy policies but not to test the universal set of factors in the earlier model. The added factors were also not addressed as individual but grouped factors. These affected the correlation and regression analyses of the developed information security model.

5.5 Future Research

With regards to the findings and limitations of the present study, several suggestions have been made to chart the way forward for future research.

Further research needs to be done on the side of government (ministries and districts) to determine why the adoption rate of e-government is still low generally despite the introduction of e-services in the government ministries and district offices.

Future studies should also examine the different factors of the grouped constructs to expand the explanatory power of the model.

From the literature review during the study, it was found that some other factors derived from previous studies such as change management, constituent desires, management commitment

could have an impact on the adoption of e-government services as per the study context. The factors can thus be added to the developed model and be tested on an extensive basis. The inclusion of these factors may affect the results of the study.

The model should be further tested so that it is thoroughly evaluated. This should include assessing the factors presented in the original model as well. This may enable the model to be modified making it more appropriate as per the Ugandan context and also for the model to be even extended further.

5.6 Recommendations

Based on the field findings, several suggestions are made for incorporation at both district and ministry levels to address the study problem and as such facilitate effective e-government services adoption.

The different government ministries and district offices that have introduced use of the e-government system for service delivery to the citizenry or are on the verge of introducing it need to appropriately incorporate information security in e-government to improve adoption of e-government services. Information security factors of confidentiality, accountability and trust factors need to be integrated into the e-services that are provided in order to address the information security standpoint of e-government.

There is need for government to avail the appropriate infrastructure and internet connectivity in the government ministries plus the local government district offices. These together with the equal infrastructure distribution in all government sectors and provision of consistent power supply will ensure connection of all these government units on the national data transmission backbone thereby ensuring effectiveness and realization of the full benefits of the e-government system.

The government providing the e-government system should build a long term trust relationship between government and the employees as well as other e-users so that they have confidence in the services provided. This can be achieved when the government ensures reliability of the e-services being provided, regular updating of the information on government and district websites, integrating end-user concerns in the e-service designs, sufficient funding of e-government and

information security programs, conducting massive information security sensitization of the users, training their staff in the needed information security skills and formulation of supporting legislation for enforcement of existing security policies and legislation. Developing such a relationship facilitates users' long term active participation and inclusion in the process of e-government thereby improving the adoption process in general.

It is also vital for the government as the e-government system provider to set up an adequate national disaster recovery plan and a system for timely cyber crime detection. The setting up of such a system and plan will not only ensure timely detection of cyber crime but also effective data recovery after an incident leading to continuity of e-government operations. This can as well help to improve on the trust relationship being developed as it reduces on the information security problem thus improving adoption and continuation of e-government services.

5.7 Conclusion

The literature reviewed, showed that there is lack of an appropriate information security e-government adoption model to guide the government in successful e-government adoption in Uganda. To address this problem, the research study aimed to create a model that explains the relationship between information security factors and the successful adoption of e-government in Uganda. This was done using the mixed methods research approach that uses both quantitative and qualitative methods. The field study was conducted to collect data on government employees in the selected units of Mbale, Sironko districts as well as ICT and Local government ministry headquarters, Kampala. Data collected was analyzed using SPSS, correlation and regression analyses. Information security factors affecting the e-government adoption process in Uganda were determined to include confidentiality, accountability and trust factors. The model of information security factors for successful e-government adoption in Uganda was developed and the relationships tested confirming the assumed relationships in the study between information security factors and e-government adoption. The study therefore achieved the objectives set.

REFERENCES

Abbad, M. M., Morris, D., and Nahlik, C. (2009). Looking under the Bonnet: Factors Affecting Student Adoption of E-Learning Systems in Jordan. *International Review of Research in Open and Distance Learning, 10* (2), 1-23.

Adeyemo, A. B. (2011). E-government implementation in Nigeria: An assessment of Nigeria's global e-gov ranking. *Journal of Internet and Information System, 2* (1), 11-19.

Al-adawi, Z., Yousafzai, S., & Pallister, J. (2005). Conceptual Model of Citizen Adoption of E-Government. *The Second International Conference on Innovations in Information Technology (IIT'05).* pp. 1–10.

AlAwadhi, S., & Morris, A. (2009). Factors Influencing the Adoption of E-government Services. *Journal of Software, 4* (6), 584-590.

Alfawaz, S., May, L., & Mohanak, K. (2008). E-Government security in developing countries: A managerial conceptual framework. -Track 12 - e-Government and Institutional Change- Retrieved July 5, 2010, from www.irspm2008.bus.qut.edu.au/IRSPM-2008.pdf

Almarabeh, T., & AbuAli, A. (2010). A General Framework for E-Government: Definition Maturity Challenges, Opportunities and Success. *European Journal of Scientific Research, 39* (1), 29-42.

Al-Mushayt, O. S., Haq, K., & Perwej, Y. (2009). 'Electronic-Government in Saudi Arabia: A Positive Revolution in The Peninsula' *International Transactions in Applied Sciences, 1* (1), 87-98.

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

Al-Shafi, S., & Weerakkody, V. (2010). Factors Affecting E-Government Adoption in the State of Qatar. *The European and Mediterranean Conference on Information Systems (EMCIS 2010).* pp. 1-23.

Alshomrani, S. (2012). A Comparative Study on United Nations E-Government Indicators Between Saudi Arabia and USA. *Journal of Emerging Trends in Computing and Information Sciences, 3* (3), 411-420.

Anthopoulos, L. G., Gerogiannis, V. C., & Fitsilis, P. (2010). Measuring E-government Adoption by Governments: The Greek Case. In C.G. Reddick (Ed.), *Comparative E-Government, Integrated Series in Information Systems* (pp.353-370). Springer Science + Business Media: LLC.

Aqil Burney, S. M., & Mahmood, N. (2006). "A Brief History of Mathematical Logic and Applications of Logic in CS/IT", *Karachi University Journal of Science, 34* (1), 61-75.

Asiimwe, E. N., & Lim, N. (2010). "Usability of Government Websites in Uganda" *Electronic Journal of e-Government, 8* (1), 1-12.

Ayodele, O. J. (2012). Validity and Reliability Issues in Educational Research, *Journal of Educational and Social Research, 2* (2), 391- 400.

Bagozzi, R. P. (2007). The Legacy of the Technology Acceptance Model and a Proposal for a Paradigm Shift, *Journal of the Association for Information Systems, 8* (4), 244-254.

Belanger, F., & Carter, L. (2008). Trust and risk in e-government adoption, *Journal of Strategic Information Systems, 17* (2), 165-176.

Bhatnagar, V., & Sharma, S. (2012). Data Mining: A Necessity for Information Security, *Journal of Knowledge Management Practice, 13* (1), 1-24.

Bwalya, K. J. (2009). Factors Affecting Adoption of e-Government in Zambia. *Electronic Journal of Information Systems in Developing Countries, 38* (4), 1-13.

Bwalya, K. J., & Healy, M. (2010). "Harnessing e-Government Adoption in SADC Region: a Conceptual Underpinning" *Electronic Journal of e-Government, 8* (1), 23-32.

Carter, L., & Belanger, F. (2003). The Influence of Perceived Characteristics of Innovating on e-Government Adoption. *Electronic Journal of e-Government, 2* (1), 11-20.

Chutter, M. Y. (2009). Overview of the Technology Acceptance Model: Origins, Developments and Future Directions. *Working Papers on Information Systems*, Indiana University, USA. *9* (37), 1-23.

Colesca, S. E., & Dobrica, L. (2008). Adoption and Use of E-government Services: The Case of Romania. *Journal of Applied Research and Technology, 6* (3), 204-217.

Conklin, W. A. (2007). Barriers to Adoption of e-Government. *Proceedings of the 40th Hawaii International Conference on System Sciences – 2007*. pp. 1–8.

Coursey, D., & Norris, D. F. (2008). Models of E-Government: Are They Correct? An Empirical Assessment. New Perspectives on E-Government. *Public Administration Review, 68* (3), 523-536.

Creswell, J. W. (2007). *Designing and conducting mixed methods research.* Thousand Oaks, CA: Sage Publications.

Davis, F. D., Bagozzi, R. P., & Warshaw, R. P. (1989). 'User Acceptance of Computer Technology: A Comparison of Two Theoretical Models' *Management Science, 35* (8), 982-1003.

Downward, P., & Mearman, A. (2007). Retroduction as mixed-methods triangulation in economic research: reorienting economics into social science. *Cambridge Journal of Economics, 31* (1), 77-99.

Federal Financial Institutions Examination Council (FFIEC). (2006). *Information Security (IS) July 2006. IT Examination Handbook*. US: FFIEC.

Gant, J. P. (2008). *Electronic Government for Developing Countries. ICT Applications and Cyber security Division Policies and Strategies Department, ITU Telecommunication Development Sector: Draft Report* (August 2008). Geneva, Switzerland: International Telecommunication Union.

Hair, J. F., Babin, B., Money, A. H., & Samouel, P. (2007). *Essentials of Business Research Methods.* John Wiley & Sons, Inc.

Hanson, W. E., Creswell, J. W., Plano Clark, V. L., Petska, K. S., & Creswell, D. J. (2005). Mixed Methods Research Designs in Counseling Psychology. *Journal of Counseling Psychology, 52* (2), 224-235.

Hart, L. C., Smith, S. Z., Swars, S. L., & Smith, M. E. (2009). An Examination of Research Methods in Mathematics Education (1995-2005). *Journal of Mixed Methods Research, 3* (1), 26-41.

Hayes, B., Bonner, A., & Douglas, C. (2013). An Introduction to Mixed Methods Research for Nephrology nurses. *Renal Society of Australasia Journal, 9* (1), 8-14.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly, 28* (1), 75-105.

Hevner, A. R. (2007). A Three Cycle View of Design Science Research. *Scandinavian Journal of Information Systems, 19* (2), 87-92.

Huawei. (2010). *E-government in Uganda.* Huawei Web site: Retrieved December 12, 2010, from http://www.huawei.com/publications/view.do?id=6091&acid=113928

Internet World Statistics. (2010). *World Internet Usage and Population Statistics.* Internet World Stats Web site: Retrieved September 20, 2010, from http://www.internetworldstats.com/stats1.html

Israel, G. D. (1992). *Determining Sample Size: PEOD-6. November.* Program Evaluation and Organizational Development, IFAS: University of Florida.

Janssens, W., Wijnen, K., Pelsmacker, P. D., and Kenhove, P. V. (2008). *Marketing Research with SPSS.* New Jersey: Prentice Hall.

Johnson, R. B., & Onwuegbuzie, A. J. (2004). Mixed Methods Research: A Research Paradigm Whose Time Has Come. *Educational Researcher, 33* (7), 14-26.

Joubish, M. F., Khurram, M. A., Ahmed, A., Fatima, S. T., & Kamal, H. (2011). Paradigms and Characteristics of a Good Qualitative Research. *World Applied Sciences Journal, 12* (11), 2082-2087.

Kitaw, Y. (2006). *E-Government in Africa: Prospects, Challenges and Practices: Kitaw 2006 Report.* Lausanne: MoT.

Kothari, C. R. (2004). *Research Methodology, Methods and Techniques* (2nd ed.). India: New Age International Publishers Ltd.

Kumar, R., Ramendran, C., & Yacob, P. (2012). A Study on Turnover Intention in Fast Food Industry: Employees' Fit to the Organizational Culture and the Important of their Commitment. *International Journal of Academic Research in Business and Social Sciences, 2* (5), 9-42.

Kumar, V., Mukerji, B., Butt, I., and Persaud, A. (2007). "Factors for Successful e-Government Adoption: a Conceptual Framework" *Electronic Journal of e-Government, 5* (1), 63-76.

Löfstedt, U. (2005). "E-Government- Assessment of Current Research and Some Proposals for Future Directions" *International Journal of Public Information Systems, 1* (1), 39-51.

Lowery, L. M. (2001). *Developing a Successful E-Government Strategy.* Unpan Web site: Retrieved May 28, 2010, from http://unpan1.un.org/intradoc/groups/public/documents/.../unpan000343.pdf.

Lucey, T. (2002). *Quantitative Techniques* (6th ed.). London: BookPower/ELST.

Mivule, K., & Turner, C. (2011). Applying Data Privacy Techniques on Tabular Data in Uganda. *Electronic Journal of Information Systems in Developing Countries, 38* (4), 1-13.

Moon, J. W., & Kim, Y. G. (2001) Extending The Tam For A World-Wide-Web Context. *Information & Management, 38* (4), 217-230.

Myers, M. D. (1997). "Qualitative Research in Information Systems," *MIS Quarterly, 21* (2), 241-242.

Nkwe, N. (2012). E-Government: Challenges and Opportunities in Botswana. *International Journal of Humanities and Social Science, 2* (17), 39-48.

Nunnally, J. C. (1978). *Psychometric Theory,* (2nd ed.). New York: McGraw Hill.

Okereke, O. E. (2011). Effect of Transformation on the Parameter Estimates of a Simple Linear Regression Model: A Case Study of Division of Variables by Constants. *Asian Journal of Mathematics and Statistics, 4* (4), 174-180.

Olupot, C ., & Mayoka, K. G. (2013). A Framework for the Adoption of Electronic Customer Relationship Management Information Systems in Uganda. *Electronic Journal of Information Systems in Developing Countries, 58* (3), 1-19.

Onwuegbuzie, A. J., & Leech, N. L. (2006). Linking research questions to mixed methods data analysis procedures. *The Qualitative Report, 11* (3), 474-498. Retrieved January 22, 2011, from http://www.nova.edu/ssss/QR/QR11-3/onwuegbuzie.pdf

Onwuegbuzie, A. J., Leech, N. L., & Collins, K. M. T. (2012). Qualitative Analysis Techniques for the Review of the Literature. *The Qualitative Report, 17* (56), 1-28. Retrieved April 14, 2014, from http://www.nova.edu/ssss/QR/QR17/onwuegbuzie.pdf

Onwuegbuzie, A. J., and Teddlie, C. (2003). A framework for analyzing data in mixed methods research, in *Handbook of mixed methods in social and behavioral research,* A. Tashakkori & C. Teddlie (Eds.), Thousand Oaks, CA: Sage.

Parliament of Uganda (2010). *The Computer Misuse Act*

Parliament of Uganda (2011a). *The Electronic Signatures Act*

Parliament of Uganda (2011b). *The Electronic Transactions Act*

PCIP (2002). *Roadmap for E-Government in the Developing World. 10 Questions E-Government Leaders Should Ask Themselves: Final Report*. Los Angeles: Pacific Council on International Policy.

Republic of Uganda (1995). *Constitution of the Republic of Uganda*

Republic of Uganda, Ministry of Information and Communications Technology (MoICT). (2010a). *Information Technology Policy for Uganda: Final Draft*. Uganda: MoICT.

Republic of Uganda, Ministry of Information and Communications Technology (MoICT). (2010b). *National Electronic Government (e-Government) Framework: Draft Final*. Uganda: MoICT.

Republic of Uganda, Ministry of Information and Communications Technology (MoICT). (2011). *National Information Security Strategy: NISS Final Draft*. Uganda: MoICT.

Rokhman, A. (2011). E-Government Adoption in Developing Countries; the Case of Indonesia. *Journal of Emerging Trends in Computing and Information Sciences, 2* (5), 228-236.

Rwangoga, N. T., & Baryayetunga, A. P. (2007). E-Government for Uganda: Challenges and Opportunities. *International Journal of Computing and ICT Research, 1* (1), 36-46.

Siau, K., & Long, Y. (2005). Synthesizing e-government stage models – a meta-synthesis based on meta-ethnography approach. *Industrial Management and Data Systems, 105* (4), 443-458.

Skinner, M. (2005). *Research the essential guide. Ways to categorize research and methodology.* Deductive strategy bfi-edu-resources Web site: Retrieved January 22, 2011, from http://www.bfi.org.uk/researchguide.pdf

Srivastava, S. C., & Teo, T. S. H. (2007). E-Government Payoffs: Evidence from Cross-Country Data. *Journal of Global Information Management, 15* (4), 20-40.

Tassabehji, R. (2005). Inclusion in E-Government: A Security Perspective. *eGovernment Workshop'05(eGov05),* Brunel University, UK. pp. 1-9.

Trochim, W. M. K. (2006). *"Approaches and Strategies of Social Research".* Research Methods Knowledge Base: Social Research Methods Web site: Retrieved January 23, 2011, from http://www.minyos.its.rmit.edu.au/~dwa/Methods.html

UNESCO (2005). *E-Government Toolkit for Developing Countries.* New Delhi: UNESCO.

United Nations. (2008). *United Nations e-Government Survey 2008: From e-Government to Connected Governance: ST/ESA/PAD/SER.E/*112. New York: United Nations.

United Nations. (2010). *United Nations E-Government Survey 2010: Leveraging e-government at a time of financial and economic crisis: ST/ESA/PAD/SER.E/*131. New York: UN Publishing Section.

United Nations. (2012). *United Nations E-Government Survey 2012: E-Government for the people: ST/ESA/PAS/SER.E/*150. New York: United Nations.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly, 27* (3), 425-478.

Venkatesh, V., Brown, S. A., & Bala, H. (2012-2013). Bridging the Qualitative-Quantitative Divide: Guidelines for Conducting Mixed Methods Research in Information Systems. *MIS Quarterly, x* (x), 1-xx/Forthcoming.

Verma, S., Kumari, S., Arteimi, M., Deiri, A., & Kumar, R. (2012). Challenges in Developing Citizen-Centric E-Governance in Libya. *International Arab Journal of e-Technology, 2* (3), 152-160.

Wangpipatwong, S., Chutimaskul, W., & Papasratorn, B. (2008). "Understanding Citizen's Continuance Intention to Use e-Government Website: a Composite View of Technology Acceptance Model and Computer Self-Efficacy" *The Electronic Journal of e-Government, 6* (1), 55-64.

Wangwe, C. K., Eloff, M. M., & Venter, L. M. (2009). E-Government Readiness: An Information Security Perspective from East Africa. *Proceedings of IST-Africa 2009 Conference.* pp. 1–6.

Wangwe, C. K., Eloff, M. M., & Venter, L. M. (2012). *Towards an Information Security Framework for Government to Government Transactions: A Perspective from East Africa.* PhD Thesis. University of South Africa. Retrieved May 25, 2014, from uir.unisa.ac.za/bitstream/handle/10500/.../thesis_final_edited_nov9.pdf

Wilkins, K., & Woodgate, R. (2008). Designing a Mixed Methods Study in Pediatric Oncology Nursing Research. *Journal of Pediatric Oncology Nursing, 25* (1), 24-33.

Williams, C. (2007). Research Methods. *Journal of Business and Economic Research, 5* (3), 65 72.

Zhou, Z., & Hu, C. (2008). Study on the E-government Security Risk Management. *International Journal of Computer Science and Network Security, 8* (5), 208-213.

APPENDICES

Appendix I

(Survey Questionnaire)

A Predictive Model for the E-Government Adoption Process in Uganda: An Information Security Perspective

Preamble

E-government provides benefits of improved public administration and government services delivery where it has been successfully adopted. In Uganda, e-government adoption remains low. In this study, we assert that a key obstacle for successful adoption of the electronic government systems in developing countries like Uganda remains the lack of trust for the security of Information provided by such systems among other Our thesis is therefore that Information Security factors have an important role to play in the successful adoption of E-government systems in Uganda. In this questionnaire we therefore request for your participation in putting together security factors to be used as requirements for a model for successful e-government adoption in Uganda. All responses shall remain anonymous and be used for this purpose only.

Definition of Terms as Used in the Questionnaire

a) E-government is the use of information and communication technologies (like Internet, telephone, community centers, wireless devices, local and wide area networks) to enhance access to and delivery of government services to citizens, businesses, employees and other stakeholders.

b) Information Security is the protection and securing of information vital to the organizations' operations and information systems from unauthorized access, use, disclosure, disruption, modification or destruction.

c) E-government Adoption is the intention to use e-government services by government officers, citizens, businesses and other stakeholders.

Please fill in the blank space or tick one box where applicable

1. Please state the sector where you work in / for

☐ Government Ministry ☐ District

Others specify……..

2. The following services are used in e-government adoption. Please indicate whether you use any of these services at your place of work (Use the scale which is indicated below)

	E-government Services	**1 (SD)**	**2 (D)**	**3 (N)**	**4 (A)**	**5 (SA)**
1	E-mail					
2	E-tax					
3	E-voting					
4	E-health					
5	E-banking					
6	E-commerce					
7	Others specify					

3. How frequently do you use electronic government services? (Tick one box)

☐ Always ☐ Most of the time ☐ Sometimes ☐ Rarely ☐ Not at all

4. Table 1 presents a number of statements deemed as important factors or requirements for e-government systems. Please indicate your level of agreement with each of these factors / statements as being important for e-government adoption. Complete the form below by indicating for each statement if you agree or disagree using the rating scale from "1" to "5". A rating of:

Strongly agree (SA)	**Agree(A)**	**Neutral (N)**	**Disagree (D)**	**Strongly disagree (SD)**
5	**4**	**3**	**2**	**1**

Table1

No	**Security factors for e-government systems**	**Check your response**				
		1 (SD)	**2 (D)**	**3 (N)**	**4 (A)**	**5 (SA)**
A	**On Confidentiality/ Privacy/Accessibility**					
1	Access to information in e-government systems (e.g. e-tax information) should be accessible to allowed e-government users only					
2	I can use the e-mail service if the system and my personal information are accessible to allowed e-government users					
3	Personal information should be kept private in the e-health system					
4	I am more likely to use the e-commerce system if the transactions are to be kept confidential					
5	E-banking information should be accessible to allowed e-government users only					
6	Personal information in the e-voting system should be kept confidential					

B	**On Integrity**					
1	E-tax data should not be tampered with (altered) during transfer					
2	E-mail service data should not be tampered with (altered) during transfer					
3	E-commerce data should not be tampered with (altered) during transfer					
4	E-banking data should not be tampered with (altered)during transfer					
5	E-health service data should not be tampered with during transfer					
6	E-voting data should not be tampered with (altered) during transfer					
C	**On Accountability/ Non-repudiation**					
1	Recipients of data in e-tax systems, should not be able to deny receiving it					
2	Senders of data in e-tax systems, should not be able to deny sending it					
3	Recipients of data in e-mail systems, should not be able to deny receiving it					
4	Senders of data in e-mail systems should not be able to deny sending it					
5	Senders of data in e- e-commerce systems should not be able to deny sending it					
6	Recipients of data in e-banking systems, should not be able to deny receiving it					
D	**On Trust**					
1	Information provided (on e.g. e-tax, e-banking, e-mails, e-commerce)by the e-government systems should be accurate if it is to be trusted					
2	Information provided (on e.g. e-tax, e-banking, e-mails, e-commerce)by the e-government systems should be reliable if it is to be trusted					
3	E-government systems should be easy to use					
4	I would prefer using e-government systems whose content is in local language					
5	E-government systems should provide information relevant to users					
E	**On Security Culture**					
1	Supporting legislation is required for e-government systems (e.g. e-tax, e-banking, e-mails, e-commerce systems)					
2	Training is required for proper e-government systems use (e.g. e-tax, e-banking, e-mails, e-commerce systems)					
3	Suitable Security and Privacy policies are required for e-government systems (e.g. e-tax, e-banking, e-mails, e-commerce systems)					
4	Awareness campaigns are required to increase e-government use					

5. Before we end, is there anything else you feel is relevant to this study that has not been dealt with but you would like the researcher to be aware of? (Record the answer below or on a separate sheet).....
.....

Thank you

Appendix II

(Field Introductory Letter)

MAKERERE UNIVERSITY
P.O. Box 7062 Kampala Uganda
E-mail: info@cis.mak.ac.ug
URL: http://www.cis.ac.ug
Tel: +256-41-540628/534560/1-97
Fax: +256-41-540620

COLLEGE OF COMPUTING & INFORMATION SCIENCES

8th December, 2011

Dear Sir / Madam,

RE: REQUEST FOR ASSISTANCE WITH RESEARCH DATA COLLECTION

This is to introduce to you Ms. Khanyako Eseri who is a student at the School of Computing and Informatics Technology, Makerere University. She is currently carrying out an academic research on the topic: 'An E-government Adoption Model for Uganda: an Information Security Perspective'. She is collecting data to determine requirements for the development of an e-government adoption Model that incorporates the Information Security perspective as a requirement for the award of a Master of Information Technology degree of Makerere University.

This is therefore to kindly request you to avail her with any information she will require for the successful completion of this research. A sample of questionnaires has been dispatched to your office in this regard.

I will be very grateful if the request is kindly considered.

Yours Faithfully,

Gilbert Maiga (PhD)
College of Computing and Informatics Technology

Appendix III

(Factor Analysis: Convergent Validity of Constructs)

Table 5. 1: Communalities for Confidentiality

	Constructs on Confidentiality	Initial	Extraction
1	Access to information in e-government systems should be accessible to allowed e-government users only	1.000	.395
2	I can use the e-mail service if the system and my personal information are accessible to allowed e-government users	1.000	.524
3	Personal information should be kept private in the e-health system	1.000	.704
4	I am more likely to use the e-commerce system if the transactions are to be kept confidential	1.000	.632
5	E-banking information should be accessible to allowed e-government users only	1.000	.617
6	Personal information in the e-voting system should be kept confidential	1.000	.461

Extraction Method: Principal Component Analysis.

Table 5. 2: Total Variance Explained on the construct of Confidentiality

Component	Initial Eigen values			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	2.232	37.202	37.202	2.232	37.202	37.202	1.687	28.116	28.116
2	1.101	18.358	55.560	1.101	18.358	55.560	1.647	27.445	55.560
3	.854	14.229	69.790						
4	.714	11.907	81.697						
5	.579	9.655	91.352						
6	.519	8.648	100.000						

Extraction Method: Principal Component Analysis.

Table 6. 1: Communalities for Integrity

	Constructs on Integrity	Initial	Extraction
1	E-tax data should not be tampered with during transfer	1.000	.613
2	E-mail service data should not be tampered with during transfer	1.000	.777
3	E-commerce data should not be tampered with during transfer	1.000	.747
4	E-banking data should not be tampered with during transfer	1.000	.776
5	E-health service data should not be tampered with during transfer	1.000	.759
6	E-voting data should not be tampered with during transfer	1.000	.742

Extraction Method: Principal Component Analysis.

Table 6. 2: Total Variance Explained on the construct of Integrity

Component	Initial Eigen values			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	4.414	73.570	73.570	4.414	73.570	73.570
2	.467	7.791	81.361			
3	.346	5.762	87.123			
4	.274	4.561	91.684			
5	.258	4.307	95.991			
6	.241	4.009	100.000			

Extraction Method: Principal Component Analysis.

Table 7. 1: Communalities for Accountability

	Constructs on Accountability	Initial	Extraction
1	Recipients of data in e-tax systems should not be able to deny receiving it	1.000	.638
2	Senders of data in e-tax systems, should not be able to deny sending it	1.000	.624
3	Recipients of data in e-mail systems should not be able to deny receiving it	1.000	.639
4	Senders of data in e-mail systems should not be able to deny sending it	1.000	.657
5	Senders of data in e-commerce systems should not be able to deny sending it	1.000	.657
6	Recipients of data in e-banking systems should not be able to deny receiving it	1.000	.727

Extraction Method: Principal Component Analysis.

Table 7. 2: Total Variance Explained on the construct of Accountability

Component	Initial Eigen values			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	3.942	65.707	65.707	3.942	65.707	65.707
2	.623	10.381	76.088			
3	.516	8.606	84.694			
4	.408	6.802	91.496			
5	.294	4.893	96.390			
6	.217	3.610	100.000			

Extraction Method: Principal Component Analysis.

Table 8. 1: Communalities for Trust

	Constructs on Trust	Initial	Extraction
1	Information provided by e-government systems should be accurate if it is to be trusted	1.000	.819
2	Information provided by the e-government systems should be reliable if it is to be trusted	1.000	.683
3	E-government systems should be easy to use	1.000	.559
4	I would prefer using e-government systems whose content is in local language	1.000	.976
5	E-government systems should provide information relevant to users	1.000	.625

Extraction Method: Principal Component Analysis.

Table 8. 2: Total Variance Explained on the construct of Trust

Component	Initial Eigen values			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	2.651	53.020	53.020	2.651	53.020	53.020	2.629	52.585	52.585
2	1.010	20.204	73.223	1.010	20.204	73.223	1.032	20.639	73.223
3	.603	12.051	85.274						
4	.474	9.473	94.747						
5	.263	5.253	100.000						

Extraction Method: Principal Component Analysis.

Table 9. 1: Communalities for Security Culture

	Constructs on Security Culture	Initial	Extraction
1	Supporting legislation is required for e-government systems	1.000	.690
2	Training is required for proper e-government systems use	1.000	.744
3	Suitable security and privacy policies are required for e-government systems	1.000	.761
4	Awareness campaigns are required to increase e-government use	1.000	.778

Extraction Method: Principal Component Analysis.

Table 9. 2: Total Variance Explained on the construct of Security Culture

Component	Initial Eigen values			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	2.973	74.334	74.334	2.973	74.334	74.334
2	.428	10.698	85.032			
3	.329	8.231	93.263			
4	.269	6.737	100.000			

Extraction Method: Principal Component Analysis.

Appendix IV

(Analysis: Field Study Results)

Table 10. 1: Mode of E-government Services Used at Work Place

	E-government services	Disagree %	Neutral %	Agree %
1	E-mail	15.1	5.8	79.1
2	E-tax	58.9	16.5	24.6
3	E-voting	83.5	12.5	4
4	E-health	77.2	13.4	9.4
5	E-banking	47.8	13.4	38.8
6	E-commerce	74.1	12.5	13.4

Table 10. 2: Confidentiality as a Security Factor for E-government systems

	Confidentiality / Accessibility	Disagree %	Neutral %	Agree %
1	E-tax information accessibility	30.7	8	61.3
2	E-mail personal information accessibility	25.8	11.1	63.1
3	E-health personal information privacy	7.1	12.4	80.4
4	E-commerce transactions confidentiality	13.3	11.1	75.6
5	E-banking information accessibility	36.9	12.9	50.2
6	E-voting personal information confidentiality	15.6	9.3	75.1

Table 11. 1: Integrity as a Security Factor for E-government systems

	Integrity	Disagree %	Neutral %	Agree %
1	E-tax data integrity	10.2	4.4	85.3
2	E-mail data integrity	9.3	5.8	84.9
3	E-commerce data integrity	8	9.3	82.7
4	E-banking data integrity	6.7	6.2	87.1
5	E-health data integrity	8	7.1	84.9
6	E-voting data integrity	6.7	8	85.3

Table 11.2: Accountability as a Security Factor for E-government systems

	Accountability / Non-repudiation	Disagree %	Neutral %	Agree %
1	Liability by e-tax data recipients	9.3	8.4	82.2
2	Liability by e-tax data senders	6.7	6.7	86.6
3	Liability by e-mail data recipients	7.1	10.2	82.7
4	Liability by e-mail data senders	6.7	5.3	88
5	Liability by e-commerce data senders	7.1	10.2	82.7
6	Liability by e-banking data recipients	7.1	9.8	83.1

Table 12.1: Trust as a Security Factor for E-government systems

	Trust	Disagree %	Neutral %	Agree %
1	Information accuracy	4.9	5.8	89.3
2	Information reliability	5.8	5.8	88.4
3	Easy to use systems	7.6	5.8	86.6
4	Content in local language	41.3	16	42.7
5	Information relevancy	5.3	6.7	88

Table 12.2: Security Culture as a Factor for E-government systems

	Security Culture	Disagree %	Neutral %	Agree %
1	Supporting legislation	8.5	7.2	84.3
2	Training	4	7.6	88.4
3	Suitable security and privacy policies	5.4	6.7	87.9
4	Awareness campaigns	5.4	4.9	89.7

Appendix V

(Correlation Analysis for the Variables)

Table 13. 1: Pearson's Correlation Coefficient (Security Culture Factors)

		E-government Adoption (services)
Supporting legislation	Pearson Correlation Sig. (2-tailed) N	.448(**) .000 223
Staff training	Pearson Correlation Sig. (2-tailed) N	.436(**) .000 224
Suitable security and privacy policies	Pearson Correlation Sig. (2-tailed) N	.432(**) .000 224
InfoSec awareness campaigns	Pearson Correlation Sig. (2-tailed) N	.415(**) .000 224
E-government services	Pearson Correlation N	1 225

** Correlation is significant at the 0.01 level (2-tailed).

Table 13. 1: Pearson's Correlation Coefficient (Confidentiality Factors)

		E-government Adoption (services)
Information access in e-government systems to allowed users	Pearson Correlation	.412(**)
	Sig. (2-tailed)	.000
	N	225
E-mail system and personal information confidentiality	Pearson Correlation	.233(**)
	Sig. (2-tailed)	.000
	N	225
Personal information confidentiality in e-health system	Pearson Correlation	.366(**)
	Sig. (2-tailed)	.000
	N	225
E-commerce system (transactions confidentiality)	Pearson Correlation	.328(**)
	Sig. (2-tailed)	.000
	N	225
E-banking information confidentiality	Pearson Correlation	.347(**)
	Sig. (2-tailed)	.000
	N	225
Personal information confidentiality in e-voting system	Pearson Correlation	.385(**)
	Sig. (2-tailed)	.000
	N	225
E-government services	Pearson Correlation	1
	N	225

** Correlation is significant at the 0.01 level (2-tailed).

Table 14. 1: Pearson's Correlation Coefficient (Integrity Factors)

		E-government Adoption (services)
E-tax data Integrity	Pearson Correlation	.450(**)
	Sig. (2-tailed)	.000
	N	225
E-mail service data Integrity	Pearson Correlation	.520(**)
	Sig. (2-tailed)	.000
	N	225
E-commerce data Integrity	Pearson Correlation	.476(**)
	Sig. (2-tailed)	.000
	N	225
E-banking data Integrity	Pearson Correlation	.497(**)
	Sig. (2-tailed)	.000
	N	225
E-health service data Integrity	Pearson Correlation	.513(**)
	Sig. (2-tailed)	.000
	N	225
E-voting data Integrity	Pearson Correlation	.481(**)
	Sig. (2-tailed)	.000
	N	225
E-government services	Pearson Correlation	1
	N	225

** Correlation is significant at the 0.01 level (2-tailed).

Table 14. 2: Pearson's Correlation Coefficient (Accountability Factors)

		E-government Adoption (services)
Accountability by data recipients in e-tax systems	Pearson Correlation	.519(**)
	Sig. (2-tailed)	.000
	N	225
Accountability by data senders in e-tax systems	Pearson Correlation	.442(**)
	Sig. (2-tailed)	.000
	N	225
Accountability by data recipients in e-mail systems	Pearson Correlation	.502(**)
	Sig. (2-tailed)	.000
	N	225
Accountability by data senders in e-mail systems	Pearson Correlation	.482(**)
	Sig. (2-tailed)	.000
	N	225
Accountability by data senders in e-commerce systems	Pearson Correlation	.516(**)
	Sig. (2-tailed)	.000
	N	225
Accountability by data recipients in e-banking systems	Pearson Correlation	.519(**)
	Sig. (2-tailed)	.000
	N	225
E-government services	Pearson Correlation	1
	N	225

** Correlation is significant at the 0.01 level (2-tailed).

Table 15. 1: Pearson's Correlation Coefficient (Trust Factors)

		E-government Adoption (services)
Information Accuracy	Pearson Correlation	.507(**)
	Sig. (2-tailed)	.000
	N	225
Information Reliability	Pearson Correlation	.504(**)
	Sig. (2-tailed)	.000
	N	224
Easy to use e-government systems	Pearson Correlation	.426(**)
	Sig. (2-tailed)	.000
	N	224
E-government content in local language	Pearson Correlation	.207(**)
	Sig. (2-tailed)	.002
	N	225
Information relevancy	Pearson Correlation	.418(**)
	Sig. (2-tailed)	.000
	N	225
E-government services	Pearson Correlation	1
	N	225

** Correlation is significant at the 0.01 level (2-tailed).