An Information Security Model for E-government Services Adoption in Uganda

Eseri KHANYAKO, Gilbert MAIGA
Dept. of Information Technology, School of Computing and Information Sciences, Makerere University, Kampala, Uganda
Email: khanyakoesther8.last@yahoo.com, gmaiga@cit.mak.ac.ug

Abstract: The successful adoption of e-government systems leads to efficient delivery of government services. Despite several e-government initiatives by the Uganda government, there has been limited success, with the levels of adoption and use remaining generally low. Building user trust which in itself depends on ensuring information security is identified as being a factor for the successful adoption and use of e-government systems. This paper presents the results of a study in which a trust based model for e-government services adoption for Uganda is given. The model addresses information security factors of confidentiality, accountability and trust for e-government adoption. The results 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 to other technologically developing countries.

Keywords: E-government; E-government services adoption; Information Security; Technology adoption models; Developing countries.

1. Introduction

The major driving goal for adopting e-government by any country is to improve citizen access to and delivery of all government services [14]. However, achievement of this goal is dependent on the e-government system acceptance and actual use by citizens, a situation highly determined by their level of trust in the e-services. To gain user trust necessitates ensuring security of information exchanged during these transactions [10]. Information security (IS) is an essential factor for the successful adoption of new technologies including e-government systems, as it determines trust and security assurance for the new technology by the intended adopters and implementers [10] [21]. Assuring information security for e-government services is therefore vital for its successful adoption.

Uganda has embraced e-government in public administration so as to improve public service delivery. The government has installed the national data transmission and e-government backbone infrastructure to achieve this goal. The districts of Kampala, Mukono, Jinja plus 27 ministries have been connected to the e-government network [17]. Despite the e-government initiatives in place and peoples awareness of the program in Uganda, use of this government infrastructure is still limited. This has greatly contributed to the poor performance of e-government adoption and the failure of full realization of the benefits that should be attained from the system.

To improve e-government adoption, so as to attain the full range of benefits resulting from its services, Uganda still requires information security initiatives in order to build citizen trust. Currently Uganda is rated at level 1, the undefined level on the information security maturity management model. This is a level under immaturity where security is not acknowledged as a desirable property of the organisation. This is due to lack of a skilled human resource base, inadequate funding of information security activities, inadequate security culture, inadequate legal framework in place among others [18]. Information security management in Uganda is thus still inadequate and a challenge that needs to be
addressed. The extent to which information security is a factor for the successful adoption of e-government services in Uganda still remains an open research issue. To address this issue the study sought to answer the following related questions: What information security factors affect the process of e-government adoption in Uganda? How do such factors help to explain the process of e-government adoption in the Ugandan context?

This study aimed to develop a model for the successful adoption of e-government services in Uganda based on information security factors (confidentiality, accountability) and trust. A descriptive field survey was conducted using questionnaires. Requirements for the information security model were collected and used to describe the model. The model affirms the role of information security factors in the process of e-government adoption in Uganda. The model is generic and can find application in other technologically transitioning countries.

2. Information Security

Information security (IS) is the process by which an organisation protects and secures its systems, media and facilities that process and maintain information vital to its operations with security, as an ongoing process and not a state at a point in time [12]. Traditionally this security encompasses information properties of confidentiality, integrity and availability which properties underpin user services such as authentication, authorisation, accountability and reliability [3]. E-government itself due to its basic concepts of openness and availability is a major contributor to security issues. Security of information used in e-government is achieved through incorporation of information security.

Although information security is an important process for the protection and security of e-government systems, its implementation has not been uniform within Government ministries, departments, agencies and local governments having different levels of ICT development and IS implementations. This situation has been worsened by the lack of a national co-ordination approach for handling IS incidents, lack of IS strategies in place, limited top management support and the too little financial support in implementing IS measures [18].

Based on the key indicators currently existent in Uganda that determine IS, maturity continuity of operations management is rated at 16%, IS incident management at 25%, physical and environmental security controls in place at 44%, human resource security considerations at 36%, IS governance structure in place at 32.5% and existence of a security norms framework that is applied at 10% [18]. As per these statistics, IS management in Uganda is still inadequate and a challenge that needs to be addressed. It is thus important to investigate information security in regards to e-government adoption so as to determine how to attain the desired IS management maturity needed for successful e-government adoption in Uganda.

The factors used to measure the existing level of information security in e-government include trust, confidentiality, integrity, availability and accountability, IS policy, security [21], and perceived risk [10][6][23][8]. Therefore identifying the information security factors existing in the e-government process in Uganda help to create understanding of how e-government adoption can be enhanced. This study therefore looked at the different challenges facing the adoption process in Uganda in a bid to understand the Ugandan e-government adoption environment.

3. E-Government

As a term, e-government reflects 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 [9][20][14]. e-government is broadly related to good governance. Governance refers to the mode in which power is exercised by governments, in managing a country’s social and economic resources [16]. E-government is therefore important for any adopting country as regards to public service delivery.

E-government advantages are unquestionable [2]. These include improved service delivery and convenience to the people, minimisation of the national digital divide, improved productivity of government agencies, strengthened good governance, promotion of democracy and commerce facilitation [17]. However 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 [2]. This study thus sought to establish with a focus on information security how to bridge that gap for the value and importance of e-government adoption to be effectively realized.

3.1 E-Government Adoption in Uganda

E-government adoption is the intention to use e-government services [4]. It is the utilization of e-government services to include e-mail, e-tax, e-voting, e-health, e-banking, e-commerce among others. Its adoption involves active participation and contribution from a number of stakeholders to include government, implementers and end-users [16]. E-government definition is incomplete unless all its customers are identified and considered [15]. However for end-users to engage there should be transparency and confidence in the system plus the provided services as these impact on end-users’ trust and acceptance of the e-government system [21]. Trust negatively affects perceived risk and this in turn impacts on the intention to use e-government [6]. These when not addressed affect e-government adoption rates.

Uganda formulated the e-government strategy in 2004 and set up numerous ICT projects in various sectors of Uganda society with the help of donor agencies to facilitate e-government [16][19]. This platform is being deployed with projected benefits of increased transparency of government activities, enabling government departments to share public data and enhance interdepartmental coordination thus reducing costs and generally work efficiency [13]. However this process of adoption in Uganda with regards to online service data provision on the national portal and five ministries is still limited with the transactional service provision level at 0%, emerging at 26%, enhanced at 26% and connected at 6% [22]. Even the deployed e-government platform is already facing challenges such as minimal use with application of most ICT investments still basic like computers being used as word processors [17].

There remains a need for a thorough understanding of these challenges being faced as well as the different issues that these impose on e-government adoption for them to be effectively addressed with measures suitable for the study area. 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 [3].

3.2 Challenges to E-Government Adoption in Uganda

In Uganda the problems hindering successful e-government adoption include inadequacy in the supporting legal framework both international and national, persistent poor IS awareness and culture, difficulty in attracting, recruiting as well as retaining skilled staff and inadequacy in the review of business processes for the efficient application of electronic government processes as well as applications to mention but a few [19][18]. 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. With increased reliance on open data networks in e-government adoption, information security has become one of the most crucial success factors to consider for both public and private organisations [3]. 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. E-government service provision at the transactional level is at a performance of 0% [22].

Improving this situation requires a solid e-government foundation to enable timely, relevant information availability at all level. This also necessitates building the trust relationship with the users as well. However for users to trust the e-government system, information quality in terms accuracy, relevance, and validity becomes a crucial factor to consider [21]. This critical analysis and evaluation of e-government adoption in Uganda thus provided the information needed to answer the question of which conceptual model to develop that solves the study problem and which is best suited for advancing e-government adoption in Uganda from an information security perspective.

3.3 E-Government Adoption Models

E-government services are built superimposed on information technology infrastructure. Addressing e-government adoption hence necessitates a discussion of the different information technology adoption models. This is so as to attain understanding of information technology adoption. Several models in previous works were looked at and analysed to include those addressing the IS aspect such as the Technology Acceptance

<table>
<thead>
<tr>
<th>Measures (Factors)</th>
<th>Models</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perceived Usefulness</td>
<td>Yes</td>
</tr>
<tr>
<td>Perceived Ease of Use</td>
<td>Yes</td>
</tr>
<tr>
<td>Social influence</td>
<td>No</td>
</tr>
<tr>
<td>Information Security</td>
<td>No</td>
</tr>
<tr>
<td>Intention to use</td>
<td>Yes</td>
</tr>
<tr>
<td>Management</td>
<td>No</td>
</tr>
<tr>
<td>Change management</td>
<td>No</td>
</tr>
<tr>
<td>Privacy and Security</td>
<td>No</td>
</tr>
<tr>
<td>Facilitating conditions</td>
<td>No</td>
</tr>
<tr>
<td>Willingness to adopt</td>
<td>No</td>
</tr>
</tbody>
</table>

Table 1: A Generic view of E-Government Adoption Measures
Model [1][11], the Unified Theory of Acceptance and Use of Technology Model [24], A model for managing e-government security to promote inclusion [21], TAM model with moderating effects [10], the conceptual framework for e-government security management [3] and the conceptual model of citizen’s adoption of e-government [8]. These models were compared as per their address of the e-government adoption measures and are presented in Table 1. Table 1 shows that of the seven models, four do not address the factor of information security. This study is needed to address this information security aspect as it plays an important role in determining users’ acceptance or rejection of e-government systems.

4. Methodology

A Quantitative research approach was used to determine the information security factors affecting the adoption process, done using a field survey. The field survey was used with questionnaires as the main data collection technique. A descriptive field survey was used to determine factors for a successful e-government adoption process in Uganda. The procedure followed during data collection, analysis, validation and interpretation is discussed in the following subsection. The field study enabled the obtaining of requirements needed for an information security e-government adoption model for the Ugandan context, thereby addressing the first objective to this study.

4.1 Data Collection Methods

A survey was used for data collection to determine requirements for successful e-government adoption in Uganda. The survey method enabled the gathering of data from the large study sample so that inferences about the population are made. 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 assigned to each of the responses was used to measure a set of variables in the questionnaire qualitatively describing information security factors for e-government systems adoption. A pilot survey was conducted to test the questionnaires and the corrections plus the experience gained were applied to improve and make the final questionnaire.

4.2 Sample Selection

To obtain a sample of the study population, the sampling design included selection of some sampling units such as districts and government headquarter ministries in Kampala. 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 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. The aggregate of elementary units from which a sample could be drawn was from the population of a district. 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.

Purposive sampling was chosen for use in this research. Purposive sampling is a method where there is deliberate selection of particular units of the universe by the researcher for constituting a sample which represents the universe. 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. This method was chosen therefore so as to capture respondents who are 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 and 2 government ministry headquarters were deliberately chosen for the study as representative of the entire study population.

The respondents included employees working as departmental heads and staff in these units. These were selected as 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. The departmental heads and staff were 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.

4.3 Sample Size

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 had to be established as below in order to determine the sample size.

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, confidence or risk level that is the likelihood that the answer will fall within that range and degree of variability which is the distribution of attributes in the population. Use of these criteria enabled determination of an appropriate sample size. The size of the sample was also influenced by budgetary and time constraints.

5. Analysis and Interpretation of Results

Questionnaires were given out to employees in Mbale plus Sironko districts and ministry headquarter offices of ICT and Local government, Kampala. Out of 241 questionnaires given out, 225 were returned valid and fully filled by departmental heads and staff in these units. Data collected was analysed and presented in themes based on the research objectives of the study. The questionnaire asked about confidentiality as a factor for IS in e-government systems and the results are shown in Figure 1.

5.1 Summary of Results on Confidentiality

![Figure 1: Confidentiality for e-Government Systems](image-url)
Respondents agreed to the need to ensure confidentiality in e-government systems to achieve information security with those agreeing in the e-tax service at 61.3%, e-mail at 63.1%, e-health at 80.4%, e-commerce 75.6%, e-banking 50.2% and e-voting at 75.1%.

5.2 Summary of Results on Integrity

Respondents’ views were also obtained on the factor of integrity and illustrated in Figure 2.

![Figure 2: Integrity for e-Government Systems](image)

The findings in the above figure show that most respondents agreed to integrity as an important factor for information security in e-government services with those agreeing highest in the e-banking service at 87.1% and lowest in the e-commerce service at 82.7%.

5.3 Summary of Results on Accountability

Data collected on the factor of accountability are as depicted in Figure 3 below.

![Figure 3: Accountability for e-Government Systems](image)
According to the results, majority of the respondent agreed to the factor of accountability with 82.2% agreeing for e-tax data recipients, 86.7% for e-tax data senders, 82.7% for e-mail data recipients, 88% for e-mail data senders, 82.7% for e-commerce data senders and 83.1% for e-banking data recipients.

5.4 Summary of Results on Trust

The study also elicited responses on the factor of trust. Findings are presented in Figure 4.

![Figure 4: Trust for Security in e-Government Systems](image)

Figure 4 above illustrates that though in general respondents agreed to the importance of trust in e-government adoption, trust as an information security factor was considered most essential in as regards to information accuracy and least important for the need to have content in the local language.

5.5 Summary of Results on Security culture

Figure 5 below shows responses obtained on the factor of security culture.

![Figure 5: Security Culture to Ensure e-Government Adoption](image)
The findings in figure 5 indicate that security culture was considered an essential factor for information security in e-government adoption with all the variables having a high response rate of above 80% for agree.

5.6 An Information Security E-Government Adoption Model

5.6.1 Theoretical Contributions from the Technology Adoption Model

The proposed model borrows from TAM [11]. TAM has been empirically tested in different parts of the world and been proven as one of the most reliable and easy models of explaining an individual’s intention of adopting technology [8]. It is a leading model in explaining and predicting system use. This model extended TAM to include other attributes and constructs relevant to the local context of SADC [3]. Moon and Kim in their study as cited in [8], stipulated that TAM has to be given extra factors or included with other technology acceptance models to address any given environment.

Using the requirements attained from the field survey the model by [8] was extended to come up with the model shown in Figure 2. Factors obtained together with existing factors of apt ICT infrastructure and lower access costs, both English and local language content, perceived ease of use, perceived usefulness, risks and local culture, data privacy and security, apt legal, regulatory frameworks, apt and continued user support, e-government adoption and finally continuance use of e-government were used to develop the IS model.

---

![Information Security e-Government Adoption Model Extending the Model by [8]](image_url)

Figure 7 is an outline of the extended model by [8] to include new constructs of security culture, information security and trust that are vital for adopting e-government from an IS perspective for a transitioning country such as Uganda. Security culture factors: IS awareness, supporting legislation, staff training, security and privacy policies; IS factors: confidentiality, Integrity and accountability and finally trust factors: information accuracy,
reliability, relevancy, easy to use systems and local language influence e-government services adoption from an IS view which in turn influences continuance use of this system.

5.6.2 Discussion

The findings show that inadequacy in security culture factors to include IS awareness, supporting legislation, staff training, security and privacy policies affect e-government adoption. Security culture refers to the prevailing attitude towards securing the e-government environment. Lack of a security culture hinders implementation of soft management factors such as the legal framework, users’ awareness of risks arising from e-government use and the solutions available to avoid possible threats. This affects their trust and acceptance of the availed e-services. Inadequacy in security culture is thus important as it tends to strengthen resistance to e-government adoption as well as fail compliance to the existing soft management factors [3].

Information security factors of confidentiality, integrity and accountability in e-government impact on the protection and securing of systems and information central to e-government operations. Information security is the process by which an organisation protects and secures its systems, media and facilities that process and maintain information vital to its operations with security, as an ongoing process and not a state at a point in time [12]. Not securing information in e-government directly affects e-government users’ perception of the security existing in the electronic services. This affects their trust of these services which in turn has a significant impact on their participation, adoption of the e-government system as well as its continued use.

Trust factors are vital as regards to determining the kind of relationship that is to exist between the government providing the e-services and the users of the services. The type of relationship to be built so as to have successful e-government adoption is dependent on the trust factors like ensuring information accuracy, having content in local language, information reliability, relevancy and ease of using the e-government system. Trust is the expectation that the promise of an individual or group can be relied upon [6]. If trust is not ensured in e-government, users won’t have confidence in the e-services provided. This will affect the trust relationship built between the government and users and in turn their participation and adoption of the e-government services. This with time negatively affects the continued use of the e-government systems by the users.

6. Conclusion and Further Work

The study identified the requirements for success in e-government adoption from an information security perspective as trust, information security and security culture. Using these requirements the study provided an e-government adoption model for Uganda that extends an earlier model [8]. This model is important as a guide to government for successful deployment of information security in e-government in Uganda. It also provides vital information needed for the users to understand the interplay between e-government and information security for them to adopt these e-services and continue using them. The model is also generic and can be used by other technologically transitioning countries similar to Uganda.

To enhance e-government adoption from an IS view, Uganda as a country needs to integrate IS in e-government. This will help build the long term trust relationship needed for successful adoption between it and the users. It should also set up an adequate national disaster recovery plan and a system for timely cyber crime so that crimes and attacks are easily detected and dealt with thereby ensuring continuity of operations.

As per further work the different factors of the grouped constructs need to be examined to expand the explanatory power of the model.
References


