International Journal of Computer Applications Technology and Research
Volume 5 issue 7, 443 – 447, 2016, ISSN: - 2319-8656

Design and Implementation Security Model for Sudanese E-government

Omar A. Ali
Department of Information Systems
Najran University
Najran KSA

Talaat M. Wahbi
Department of Computer Science and Technology
Sudan University of Science and Technology
Khartoum, Sudan

Izzeldin M. Osman
Department of Computer Science
Sudan University of Science and Technology
Khartoum, Sudan

Abstract: Security is one of the most important issues in E-government projects. E-government applications will be increasingly used by the citizens of many countries to access a set of services. Currently, the use of the E-government applications arises many challenges; one of these challenges is the security issues. E-government applications security is a very important characteristic that should be taken into account. This paper makes an analysis over the security as required for E-government and specify the risks and challenges that faces E-government projects in Sudan. Finally, the study has proposed security model for Sudanese E-government. The proposed security model for the Sudanese electronic government is a four layers' model that is divided into sub layers. Each layer will mitigate group of threats related to an e-services. The model is not generic; it cannot be applied by other countries. It is precisely designed for Sudanese situation.

Keywords: E-government, security model, countermeasures, NIC, IT infrastructure, managerial layer

1. INTRODUCTION

E-government security is facing a wide range of threats. The threats may be technical or non-technical. Modeling is the specific description of the link between the objective world and the abstract things. Constructing the security model of E-government for any country depends on its situation. Holistic security is a form of security which operates on multiple, fully integrated levels or layers. This approach to security can be taken to secure a structure, a computer network, a campus, and any number of other things which might need securing. The underlying idea behind holistic security is that systems need to be considered as wholes to achieve the greatest level of security; while it is important to be aware of individual aspects of a system, the ways in which these aspects work together are also a key part of a security system. There are four layers in Sudanese electronic government security proposed model, and each layer is composed of sub-layers. The purpose of this paper is to construct a comprehensive model which will consist of multiple layers that complement each other.

2. STATEMENT OF THE PROBLEM

The Electronic Government is the high efficient, good quality management and service, in which the government employs technology of modern network communication and computer to realize its functions on network by such means of reduction, optimization, conformity and recombination. Because E-government is involved in government policy and the country's secrets, people always pay close attention to its security. How to ensure E-government's security is a longstanding key problem for E-government. The security model for E-government of Sudan can help to guide IT managers recognise the technological and organisational requirements for securing E-government in public sector organisations. The security model for Sudanese E-government can also help the decision makers to set a vision and strategic action plan for future direction in the information technology age through identifying key elements and stages for action.

3. RELATED WORK

Many studies have been conducted to propose security models of E-government in deferent countries over the world. Al-Azazi, in a study presents five security layers models in Dubai E-governments [3]. The model is composed of technology layer, policy layer, competency layer, operational and management layer, and decision layer. Each layer is composed of detailed layer which is called the sub-layer of the main layer. Hana, in her study proposed hybrid model for Egyptian E-Government Cloud Computing consists of three computing clouds; Inter-Cloud computing, Intra- Cloud computing and Extra-Cloud computing [4]. Waziri, and Yonah, in their study proposed secured E- Government maturity model consists of four layers, namely: (1) secured digital presence, (2) secured interaction, (3) secured transaction, and (4) secured transformation [5]. Ziyao Junjie, Duan introduced service-oriented architecture which is an IT architectural style that supports integrating business as linked services which users can combine and reuse in the production of business applications [6]. Lin, Yongzhao and Yi introduced the access control system which includes subjects, objects and access control policy, and their relationship [7].

4. MATERIALS AND METHODS

4.1 Study area

Sudan is located in the north-eastern part of Africa (see Figure 1), and occupies the central region between Africa and the Arab World. The location results in Sudan's unique characteristics, as it is the main passage between north and south of Africa. Sudan was also the main route for the pilgrim and trade convoys that crossed from the west of Africa to the

Holy Lands in Makah, until the middle of the current century [1].

4.2 The data

A preliminary study is an initial study to gather basic information –not full information- to specify the research problem. The main aim of a preliminary study for this research is to make a general idea about the security of e-government in Sudan. Also an interview with specialists in National Information Centre (NIC) which is a responsible body for E-government project in Sudan will be conducted, there are many detailed points related to this issue. Direct observation also is an important resource to gain information about the E-government security in Sudan.

Figure. 1 Map of Sudan

5. THE PROPOSED MODEL

Implemented the research methodology consists of series of actions or steps necessary to effectively carry out research and the desired sequencing of these steps. The chart shown in (Figure 2) will illustrate the implemented research methodology. The following section describes each step.

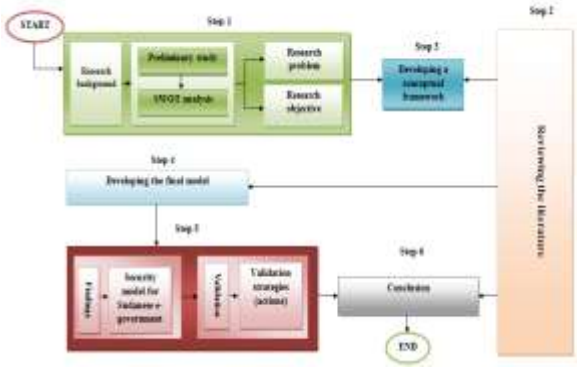

Figure. 2 Shows the implemented research methodology

Step 1: Conducting the preliminary study, SWOT analysis and identifying the research problem to achieve the research objectives

After establishing the research background, a pilot study was conducted with state e-government authorities, IT professionals; and academics. The findings from the preliminary study directly contributed to building the initial conceptual framework. Additional data was gathered through informal dialogue, government agency websites, publications and articles highlighted issues and challenges related to a variety of aspects; IT infrastructure, managerial, legal and technical. The interview was then collated data and analyzed using the SWOT tool of analysis.

Step 2: Reviewing the literature

The literature review explaining the existing security models addressing policies and the security triad (confidentiality, integrity, availability) which act as the high level objectives of any security architecture or model. Different types of models were analyzed. Models addressing confidentiality or integrity only were such as BLP or Biba were analyzed. Social and human behavioral model and theories were searched to build the concept of the human aspect in the information security field. In addition, e-government assessment and stages of growth, models and frameworks developed in e- government and other disciplines (IT and IS) were thoroughly reviewed.

The review of the literature led to different ideas on how to pursue constructing the new model. More significantly, was the deep review of the key issues that have impact upon the adoption of new technology in general, and e-government innovation in particular; such as, organizational and environmental issues. The majority of the literature was addressing technological security solutions or approaches to solve issues related to data integrity or confidentiality. These technological solutions were presented as architectures required or programmes to be installed in the IT infrastructure.

Step 3: Developing a conceptual framework

After identifying the research problem and reviewing the related literature the initial framework was provided. The framework is based on the IT infrastructure, managerial, legal and technical. The framework and its critical factors according to the initial findings from the SWOT analysis of the preliminary study, combined with the identified factors and key elements from the literature review were constructed. The development of the conceptual framework step is a major step in theory building and it is considered a type of intermediate theory [2], that attempts to connect all aspects of inquiry (problem definition, purpose, literature review methodology, data collection and analysis). The development of the initial conceptual framework will help develop understanding of the research problem and lead to developing the final model.

Step 4: Developing the final model

In this step of research, the details of each category of challenges and barriers to e-government in Sudan were specified according to its source. The information which was collected from interviewees, observations and documents were formulated into layers, and then these layers were focused studied to provide sub-layers into each category of the layer.

Step 5: Validation

In this step three actions have been implemented in the same time.

Action 1: According to specialists the security layers and sub-layers that mentioned in this research were specified.

Action 2: The criteria that extrapolated from Wood's book [8] for the success of the model were set.

Action 3: The guidelines of modeling presented by [9] were followed.

Step 6: Drawing conclusion

This is the final step of The implemented research methodology. See figure 2.

6. RESULTS

6.1 The security layers, risks and countermeasures

The idea of this model is stemmed from the risk analysis that facing the Sudanese electronic government are listed in the second column of the table 1. The third column of the table 'countermeasures of risks' compose the sub-layer of the model. The collection of the same issues (sub-layers) that mentioned in the third column of the table1 are collected together to form the main layer of the model which are listed in the first column of the table 1 and figure 1.

Table. 1 Illlustrates the layers, risk analysis and Countermeasure of risks

Layer	Risk analysis	Countermeasure of risks
Technical layer	Unauthorized access to a place or other resource.	• Access control • Authentication password
	Information interception	• Cryptography • Training and awareness
	Information tampering	• Authentication password • Using tamper-resistant protocol across communication links • Secure communication links with protocols that provide message integrity. • Cryptography
	Denial of services attacks	• Analysis tools • Monitoring tools • Using resource and bandwidth throttling techniques • Validate and filter input
	System resources stealing	• Access control • Authentication password • Analysis tools • Monitoring tools
	Information faking	• One-time password • Cryptography
IT infrastructure layer	Lack of e-government projects	• Availability of staff skilled • Reliability of infrastructure • Consultation • Software houses
		•
Managerial layer	Lack of e-government projects	• Budget • Policies and mechanism to enforce it • Willingness to change in top management and administration • Conflict of interest
Developing legislative protection and law	Lack of e-government projects	

6.2 The security layers for Sudanese e-government

In order to reach to a comprehensive method to check the security requirements for any electronic enabled organization to allow or not the interchange of information with other e-organizations in Sudan; the multiple security layer was proposed. (See figure 3).

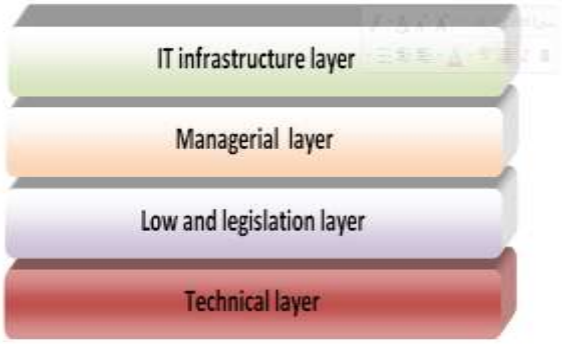

Figure. 3 Illustrates the security layers for Sudanese e-government security model

Any model contains more than one level or layer of security is comprehensive model, and prevent organization from wide range of threats related to a single or multiple e-services. Each layer will mitigate group of threats related to an e-services. For example, the technical layer will address all the technological threats while the IT infrastructure will address the threats on e-services related to the requirements that are important to continuity to e-government projects. There are four security layers that contribute in construct the security model for Sudanese security e-government model see figure 3. The model extracted from the interviews and collected data

from the responsible body of the e-government projects in Sudan. Each layer of the model contains of detailed layer or sub-layer (see Figure 4).

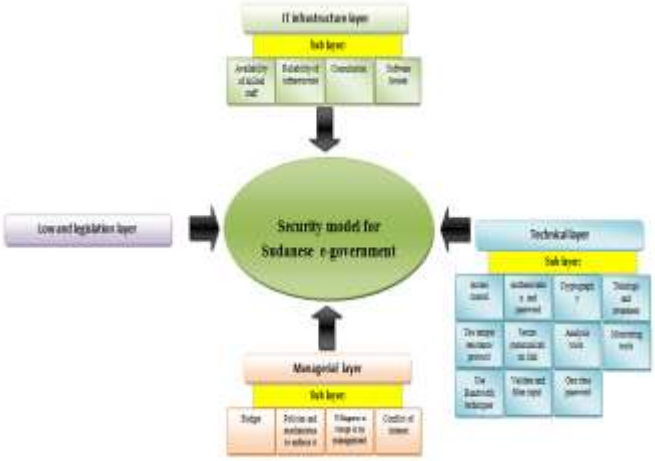

Figure. 4 Illustrate the sub layer of the model

The final model in this research composed of vertical axis that represent the main layers and horizontal axis that represent the sub-layers. The main layers (vertical axis) are positioned according to Sudanese security situation, they are the aspects or risks that facing the security of e-government in Sudan. The sub-layers (horizontal axis) are detailed layers with respect to each main layer. The final model is a coherent and understandable model because of its structure vertical and horizontal axis. (See Figure 5).

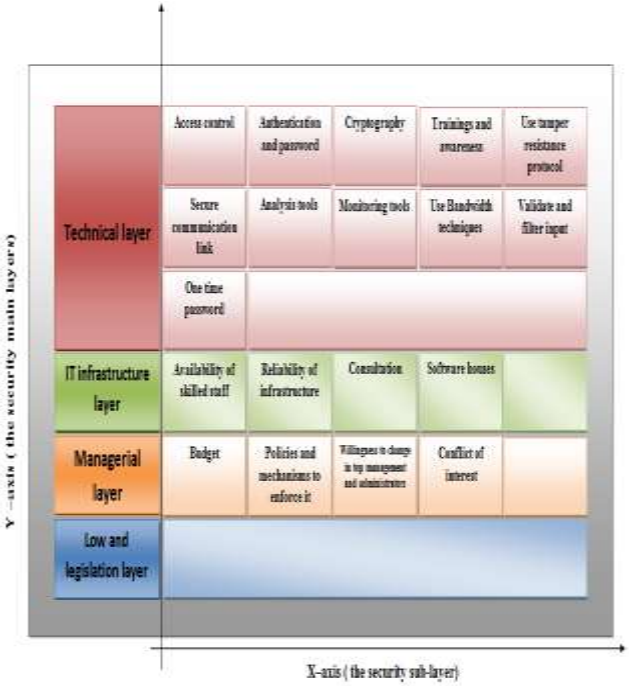

Figure. 5 Illustrate the layers and sub-layers of e-government security model for Sudan

7. THE MODEL EVOLUTION

Figure 6 depicts the evolution of the final model from the risks specification stage to the last one.

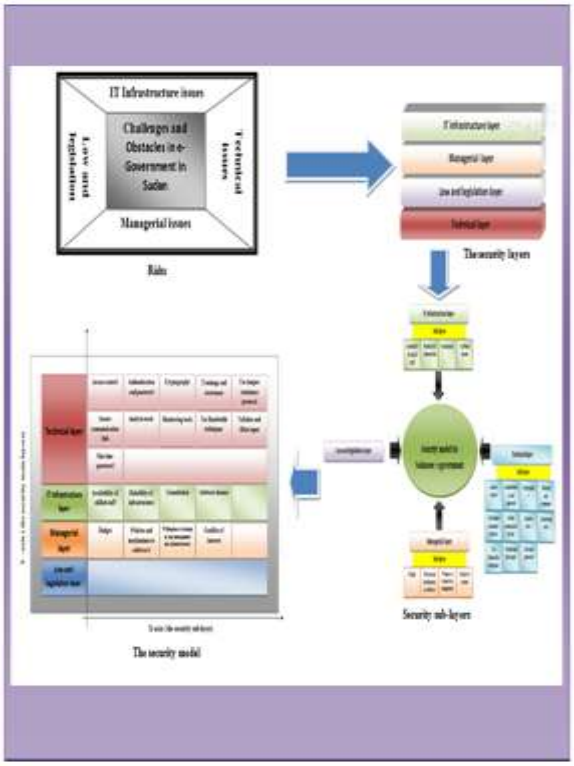

Figure. 6 Illustrates the stages of the model to reach the final model

8. CONCLUSION

The purpose of this paper is to design the security model for Sudanese electronic government. The model with more than one aspects of security is a comprehensive model. All factors that affected the security issue in Sudanese electronic government were found and formed in applicable form in any organization in Sudan.

9. ACKNOWLEDGMENTS

Deep thanks to Prof. Izzeldin M. Osman and Dr Talaat M. Wahbi for their support

10. REFERENCES

[1]http://www.sudan.gov.sd/index.php/en/pages/details/57/About%20Sudan#.ViO_v27evW4 (retrieved 18 Oct 2015)

[2] Carroll, J. M. and Swatman, P. A. (2000). Structured-case: a methodological framework for building theory in information systems research, European Journal of Information Systems, 9: 235-242.

[3] Al-Azazi, S (2008). Amulti-layer model for e-government information security assessment. Grandfield university, dubai.

[4] Hana, M (2013). E-Government Cloud Computing Proposed Model: Egyptian Government Cloud Computing. International Conference on Advances in Computing. Communications and Informatics (ICACCI). Pp 848-852.

Electrical and Communication Department Canadian International College ElSheikh Zaid. Egypt.

[5] Waziri, M. Yonah, Z. (2014). A Secure Maturity Model for Protecting e-Government Services: A Case of Tanzania. Advances in Computer Science: An International Journal 3: 98-106.

[6] Ziyao W, Junjie N, Z Duan, (2008). SOA core technologies and application, Publishing House of Electronics Industry, Beijing, Pp.495-497.

[7] L Lin, Yongzhao Z, Yi N. (2006) Improved RBAC model based on organization. Journal of Jiangsu University (Natural Science Edition) 27(2):147-150.

[8] Wood, C, 2005. Information Security Policies Made Easy Version 9. Information Shield, U.S.

[9] Lankhorst, M. (2005). Enterprise Architecture at Work, 1st ed, Springer, Berlin.