International Journal of Computer Applications Technology and Research
Volume 5– Issue 7, 439 - 442, 2016, ISSN:- 2319–8656

E-government Security Models

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: E-government security is a key problem to restrict the construction and development of E-government systems in any country over the world. E-Government security models are widely used in the implementation and development of e- government systems. Due to the deference situation of the countries over the world there are various security models applied in each country. This paper reviews different security models in e-government in order to determine important parameters for e-government strategic planning.

Keywords: E-government, security model, ICT, layers, sub-layer

1. INTRODUCTION

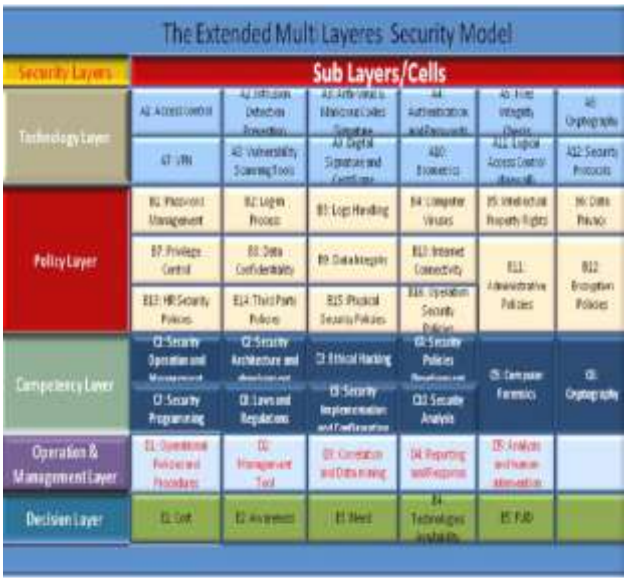
Dependency on Information and Communication Technology (ICT) for supporting core operations to both government and private sector is increasing [1]. Similarly, organization's critical information has developed into a key strategic asset in a competitive world [2]. Nevertheless, the pace of ICT advancement such as development, deployment and use of e-government infrastructures is much faster than the development and deployment of security services, including technical and the existing and new emerging security risks [3, 4]. Technical security aspects include hardware and software solutions such as Access control and Antivirus mechanisms [5, 6, 7]. The application of information security principles in an e-government environment is a complex, multidimensional issue involving people, technology and processes. E-government security is considered one of the crucial factors for achieving an advanced stage of e-government. As the number of e-government services introduced to the user increases, a higher level of e-government security is required.

2. REVIEW

In order to get the maximum decrease of data breaches and get the maximum protection of critical data when using e-government systems in any country over the world there should be a security model to satisfy this purpose. The security models of E-government may be based on layers [9], cloud computing [10], based on service-oriented architecture [15], access control policy [11], and security system based on information security model [12].

2.1 The Five Security Layered-Model in Dubai

In this model there are five layers. Each layer will mitigate group of threats related to an e-services. The model is composed of technology layer, policy layer, competency layer, operational and management layer, and decision layer. The technology layer for example will address all the technological threats while the policy and competency layers will address the threats on an e- service related to the human aspect. Each layer is composed of detailed layer which is called the sub-layer of the main layer [8]. See figure 1 showing the E-government security model in Dubai.



The Extended Mult Layeres Security Model

Security Layers	Sub Layers/Cells					
Technology Layer	A1: Access control	A2: Intrusion Detection Prevention	A3: Anti-virus & Malicious Codes Signature	A4: Authentication and Passwords	A5: Files Integrity Checks	A6: Cryptography
	A7: VPN	A8: Vulnerability Scanning Tools	A9: Digital Signatures and Certificates	A10: Biometrics	A11: Logical Access Control (firewalls)	A12: Security Protocols
Policy Layer	B1: Password Management	B2: Logon Process	B3: Logs Handling	B4: Computer Viruses	B5: Intellectual Property Rights	B6: Data Privacy
	B7: Privilege Control	B8: Data Confidentiality	B9: Data Integrity	B10: Internet Connectivity	B11: Administrative Policies	B12: Encryption Policies
	B13: HR Security Policies	B14: Third Party Policies	B15: Physical Security Policies	B16: Operation Security Policies		
Competency Layer	C1: Security Operation and Management	C2: Security Architecture and development	C3: Ethical Hacking	C4: Security Policies Development	C5: Computer Forensics	C6: Cryptography
	C7: Security Programming	C8: Laws and Regulations	C9: Security Implementation and Configuration	C10: Security Analysis		
Operation & Management Layer	D1: Operational Policies and Procedure	D2: Management Tool	D3: Correlation and Data mining	D4: Reporting and Response	D5: Analysis and human intervention	
Decision Layer	E1: Cost	E2: Awareness	E3: Need	E4: Technologies Availability	E5: R&D	

Figure. 1 E-government security model in Dubai

2.2 Government Cloud Computing Proposed Model: Egyptian E-Government Cloud Computing

The proposed hybrid model for Egyptian E-Government Cloud Computing consists of three computing clouds; Inter-Cloud computing, Intra- Cloud computing and Extra-Cloud computing, Figure 2. The three cloud models are analogs to the terms Internet, Intranet and extranet in their functionality, operation and management. Intra-Cloud computing "I**A**CC" is a private cloud which is dedicated to a single national entity cluster, (see Figure 3). Members of that cluster are the only legitimate users. Extra-Cloud computing "E**X**CC" is a community cloud that enables entities from different clusters to integrate and to aggregate their work as required. There are two types of E**X**CC. The first type connects multiple I**A**CC of a specific national entity cluster, Figure 3. The second type connects different national entity clusters that differ in their functions and services, (see Figure 2). Inter-Cloud computing "I**E**CC" is a public cloud that enables any user (citizen, guest, organizations) to require specific requests and receives their responses or outcomes, (see Figure 2). In I**E**CC, it is expected to store the least sensitive data and to run the related application software.

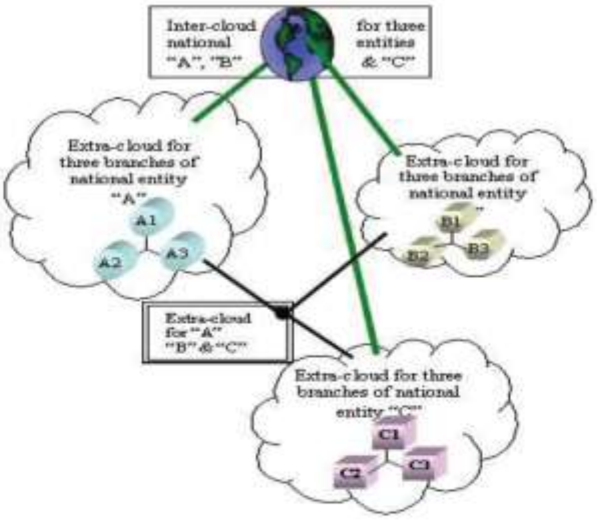

Inter-cloud national "A", "B" for three entities & "C"
Extra-cloud for three branches of national entity "A"
A1
A2
A3
Extra-cloud for three branches of national entity
B1
B2
B3
Extra-cloud for "A" "B" & "C"
Extra-cloud for three branches of national entity "C"
C1
C2
C3

Figure. 2 Proposed model for Egyptian E-Government Cloud Computing

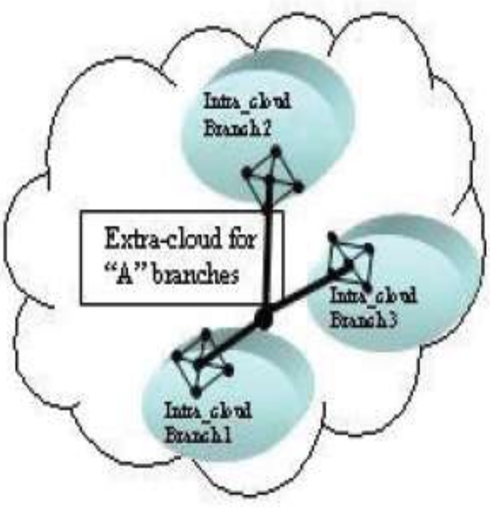


Figure. 3 IACC and EXCC for National entity A.

2.3 A Secure Maturity Model for Protecting e-Government Services: A Case of Tanzania

The 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. The implementation of the proposed model is neither based on a specific technology/protocol nor a certain security system/product, but rather an approach towards a structured and efficient implementation of those technologies. The security layers include technical and non-technical security control elements. The proposed security layers are further described in the following paragraphs. [10]

2.3.1 Secured Digital Presence

This stage involves simple provision of government information through website (static) with basic information that the citizen can access [11]. This is a one-way communication between governments, businesses and citizens. Generally, the information provided by organizations at this stage are public and normally with zero security. At this stage, the security layer should have the ability to verify e- Government services identity in order to build trust between government agencies and users. The users would like to be sure that they are connected to the e-Government service belonging to the administration in question [12].

2.3.2 Secured Interaction

At this stage the interaction between government and the public (Government-to-Citizens and Government-to-Businesses) is stimulated by various applications. Citizens can ask questions via e-mail, use search engines and download forms and documents [12]. The communication is performed in two ways, but the interactions are relatively simple and generally revolve around information provision. At this stage, the security layer should have the ability to authenticate a user/ citizen asking for a service. The most important security aspects at this stage are identity authentication, availability and integrity.

2.3.3 Secured Transaction

At this stage public organizations provide electronic initiatives and services with capabilities and features that facilitate clients to complete their transactions in full without the necessity of visiting government offices [37]. The public can carry out their financial transactions with the government Such services also allow the government to function in a 24/7 mode. The most important security aspects at this stage are personal information confidentiality, identity authentication, availability, non-repudiation, accountability and integrity.

2.3.4 Secured Transformation

This stage allows users of e-Government services to interact with government as one entity instead of Information systems are integrated, and the citizens' individual government organizations [14]. can get services at one virtual counter. The integration of information systems can result in situations where the privacy of individual citizens is in danger. The most important security aspects of this stage are personal information confidentiality, identity authentication, availability, nonrepudiation, accountability and integrity. At this stage, the security layer should restrict the utilization of personal information, and secure such information from access by unintended parties. A government agency should be able to authenticate another government agency that requires a service on behalf of the users.

2.4 A Security E-government Model Based on Service-oriented Architecture

Service-oriented architecture is an IT architectural style that supports integrating business as linked services which users can combine and reuse them in the production of business applications [15]. It provides an effective way for constructing loose coupled web services. It relies on services exposing their functionality via interfaces that other services can understand how to utilize those services. SOA logical architecture is shown in Figure 4 [16].

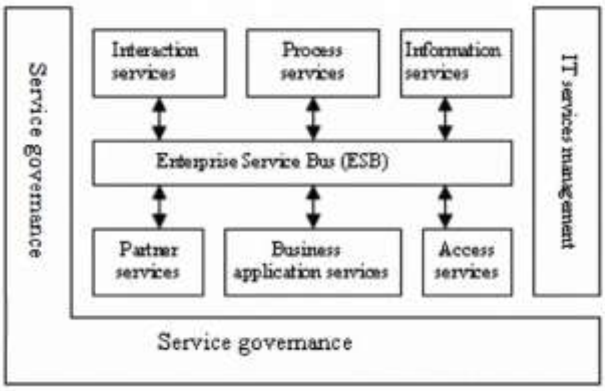


Figure. 4 SOA logical architecture

The SOA technology framework to integrate E-government: using BEPL implement work process; realizing seamless integration between services by ESB. Taking the case of online application processing, a scheme of integration E-government system based on SOA is shown as Figure 5. [16]

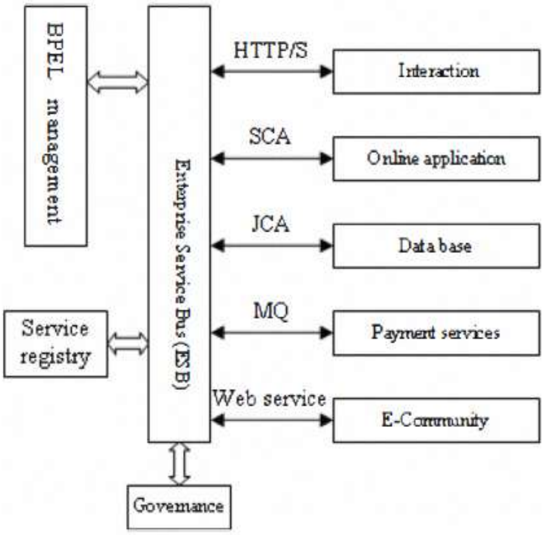


Figure. 5 A scheme of integration E-government system based on SOA

2.5 Research on Role-Based Access Control Policy (RBAC) of E-government

The access control system includes subjects, objects and access control policy, and their relationship is shown in figure 6 [17].

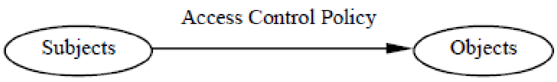


Figure. 6 Access Control System Model

The RBAC is a new access control technique and notion. It is the development and amelioration of DAC and MAC, and it has been regarded as an effective measure to resolve resource unified access control of large information systems by the public. The RBAC contains five kinds of entities, such as users, roles, constraints, permissions, and sessions. In the RBAC model, it injects the idea of roles between users and access permissions, and a user connects with one or more specific roles, and a role connects with one or more permissions, and roles can be created or canceled according to actual working requirements. The sessions show the relationship between users and roles. The users should activate roles by creating sessions every time and get the specific resource access authorities as shown in Figure 7 [18-19].

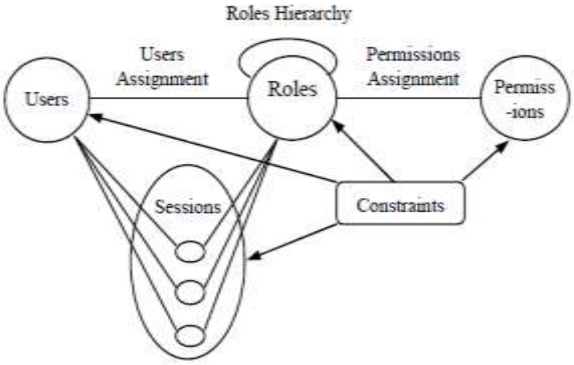


Figure. 7 Basic RBAC Model

2.6 Security System based on Information Security Model

The system is designed through modularization and it is mainly divided into initialization module, management module and various application modules. In which, the initialization module is used to manage the original data of the initial management module and various application modules, the management module is used to manage the content which has effect in the overall system, such as the users, privileges and a series of rules in the system. Various application modules work together by using the initialized data and through the transmission media to complete the overall function of the system. The secure e-government system structure is shown in Figure 8.

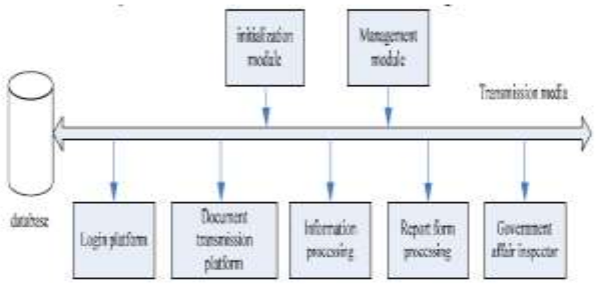


Figure. 8 Secure e-government system

3. CONCLUSION

Based on the research that led up to this paper, the security model for e-government that adopt layers in its structure is more coherent and comprehensive because of covering all threats that faced e-government in each country. Also this type of models is so easy to be understandable to the employees in any organization.

4. REFERENCES

[1] G. Dhillon, (2000). *Challenges in managing Information Security in the millennium,* Idea Group Publisher, Las Vegas, USA.

[2] S. Woodhouse, (2007). Information Security: End User Behavior and Corporate Culture, 7th *International Conference on Computer and Information Technology*. (IEEE). Pp 767-774. University of Aizu. Fukushima, Japan.

[3] G. Karokola, L. Yngström, & S. Kowalski, (2010). A Comparative Analysis of e-Government Maturity Models for Developing Regions: The Need for Security Services. *International Journal of Electronic Government Research*. **8**: 1-25.

[4] P. W. Anderson. (2001). Information security governance. *information security technical report*. **6**: 60 – 70.

[5] G. McGraw, (2005). *Software Security*. *Volume1*. Addison-Wesley software. USA.

[6] M. Bishop, (2006). *Computer Security – Arts and Science*. Volume1. Addison-Wesley, USA.

[7] M. Wimmer, & B. Bredow, (2001). E-Government: Aspect of Security on different layers, In: *Proceedings. 12th International Workshop.* (Database and Expert Systems Applications) Pp 350-355. IEEE, Linz University., Austria

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

[9] Hana, M (2013). E-Government Cloud Computing Proposed Model: Egyptian E_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

[10] 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.

[11] G. Karokola and L. Yngström, (2009). Discussing E-Government Maturity Models for the Developing World-Security View. *Information Systems Security Association* Pp81-98.

[12] Zhang, F. (2008). Design of E-government Security System based on Information Security Model. *2008 International Conference on Advanced Computer Theory and Engineering*. **(***Research Center of Cluster and Enterprise Development***) Pp**359-362. Jiangxi University of Finance and Economics. China

[13] www.clknet.or.tz J. Yonazi, Adoption of Transactional Level e-Government Initiatives in Tanzania. (Retrieved 13Apr2014)

[14] www.utumishi.go.tz, President's Office, Public Service Managements, Tanzania e-Government Strategy, ed, 2012. (Retrieved 10Feb2013)

[15] Erl, T, (2005). *Service-oriented Architecture: Concepts, Technology, and Design*. Volume2. Upper Saddle River: Prentice Hall PTR, USA

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

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

[18] Zeng Zhongping, Li Zonghua, Lu Xinhai. (2007). The Access Control Policy Study of E-government Information Resource Based on RBAC. *Journal of Information*, **10**:39-41

[19] Barka E, Sandhu R S. (2000). Framework for role-based delegation models. *In: Proc. of the 16th Annual Computer Security Application Conf. IEEE Computer Society Press*. Pp 168-176