ACSIJ Advances in Computer Science: an International Journal, Vol. 3, Issue 5, No.11 , September 2014
ISSN : 2322-5157
www.ACSIJ.org

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

Mohamed D. Waziri[1] and Zaipuna O. Yonah[2]
The Nelson Mandela African Institution of Science and Technology (NM-AIST)
School of Computational and Communication Science and Engineering
P. O. Box 447, Arusha, Tanzania
Email: {dewam[1], zaipuna.yonah[2]}@nm-aist.ac.tz

Abstract

E-Government Maturity Models (eGMMs) are widely used in the implementation and development of e-Government services. These models outline various stages for e-Government development. Information security and privacy are considered as the most significant challenges in implementing e-Government services, but unfortunately very few designs of eGMMs have considered security as a specific issue. However, even these few security responsive models consider security mostly at the transaction stage, and as such it is insecure to depend on security mechanisms provided at transaction stage only. This paper develops a four-stage holistic secured eGMM for protecting e-Government services with Tanzania used as a case study. The proposed secured e-Government maturity model has been designed by including the security layers which consist of technical and non-technical security related aspects in each of its four maturity stages. The model design process is based on the ISO/ IEC 27002 security standard and is guided by a design science research methodology. The paper main contribution is the proposed secured eGMM that addresses both technical and non-technical security related aspects at its maturity stages.

Keywords: *e-Government Maturity Model, e-Government services, security threats, access control, security policy*

1. Introduction

E-Government refers to the use by government agencies of information technologies (such as Wide Area Networks, the Internet and mobile computing) that have the ability to transform relations with citizens, businesses and other arms of government [1]. The use of Information and Communication Technologies (ICTs) in government operations facilitates speedy, transparent, accountable, efficient and effective interaction with the public, citizens, business and other agencies. E-Government is a cost-effective solution that improves communication between government agencies and their constituents by providing access to information and services online [2].

E-Government has many benefits to our modern world through services provided over the internet as follows: (1) it increases transparency, (2) enhancing efficiency and quality, (3) enables full access to information and individual services [3], and (4) enables citizens to interact and receive services from public organizations 24 hours a day, seven days a week (24/7 – basis). However, despite the potential benefits provided by e-Government services, there are a number of challenges that could prevent achieving these expected benefits. The most significant challenges for implementing e-Government initiatives are information security and privacy [4]. Typical citizens, especially those who don't use the Internet frequently, feel vulnerable when using e-Government services, they may have little trust that their information can be transmitted through websites securely. Most of these citizens fear that government is spying on them and they are not wishing to have history retained. It was observed that majority of the e-Government services users distrust the information security measures used to protect e-Government services [5].

The government of Tanzania developed the e-Government strategy in 2009 to facilitate provision of sustainable e-Government services to the public, particularly to citizens. It is noted in the strategy that during implementation of e-Government applications, consideration should be given on using security and privacy mechanisms to ensure proper use and handling of personal information and transactions [6]. Unfortunately, the government has not adopted any standard or issued guidelines to public organizations with regards to information security.

E-Government Maturity Models are widely used in development and implementation of e-Government services. An e-Government maturity model is a set of stages (from basic to advanced ones) that determines the maturity of the e-Government [7]. The advantage of having a staged approach is the ability to generate momentum that can be sustained. This allows public sector organizations to attract more citizens to use e-Government services to a point where it becomes natural, as well as securing business trust and confidence to deal with an e-Government portals as part of their standard service chain operations [8]. The main benefit of maturity models is to offer a way to rank e-Government services and a way to enhance their quality. Information security and privacy are considered as the most significant challenges in implementing e-Government services. But unfortunately very few cases of eGMMs designs

have considered security as a specific issue; Existing models consider security mostly at the transaction stage [9], and it is insecure to depend only on security mechanisms provided at transaction stage only. Security mechanisms should be considered at all stages of the maturity models. This paper proposes a holistic secured e-Government Maturity Model consisting of both technical and non-technical security aspects for protecting e-Government services in Tanzania. With a holistic approach, security is considered beyond the technical aspects. Social, political, cultural, and legal impacts on security requirements are considered as well [10].

A number of Information Security Maturity Models (ISMMs) have been developed with the aim of maturity assessment of information security and evaluation of the level of security awareness and practice (which are affected by people, process, and technology) at any ICT-enabled organization, be it public or private sector [11]. Furthermore, ISMMs help to better understand where and to what extent the three main processes of security (prevention, detection, and recovery) are implemented and integrated. Despite the fact that these models rather measure quality than quantity of services offered, they also lack much of non-technical security services [12].

The rest of the paper is organized as follows: Section two identifies the technical and non-technical security threats which face e-Government services and presents the related work; Section three outlines the research methodology; Section four presents the proposed model; Lastly, conclusion is given in Section five.

2. Background

The ability to make public services easily available online is an attractive prospect for governments, not just because this gives citizens easy access, but also because of the potential cost-savings. But e-Government services in their current status are not secure; they bring benefits but also security threats that need to be addressed. E-Government services are vulnerable to three different categories of attacks: server-side attacks (i.e. on the government servers), client-side attacks (i.e. on the citizen's computing/access device) and network attacks (i.e. on the Internet connection, either by interfering with existing connections/sessions or by an attacker pretending to the server to be a valid client or to the client to be a valid server) [13]. This section identifies the technical and non-technical security threats which impact e-Government services.

2.1 Technical Security Threats of e-Government Services

Technical security threats are those threats by which an attacker perpetrates using software and systems knowledge or expertise. The following are the most known technical security threats on e-Government services.

a. Communication channel threats: The Internet serves as the electronic chain that links a consumer (client) to the e-Government server. Messages on the Internet travel through random paths from a source node to a destination node. It is impossible to guarantee that every computer on the Internet through which messages pass is safe, secure and, non-hostile [14].

b. Server end threats: A server is a running instance of a computer application that accepts requests from the client and provides services as the response accordingly. Servers have vulnerabilities that can be exploited by anyone determined to cause destruction or illegally acquire information [14]. Threats to e-Government servers fall into two general categories: (1) Threats from actual attacker(s); and (2) Technological failure [15]. In terms of the former, the motivation is primarily psychological. The intent is to garner personal information from people for the sheer purposes of exploitation (such as obtaining Credit Card and Bank Account information; Phishing schemes, obtaining usernames and passwords, etc.). With the latter, anything related to the Internet can cause problems. This can be anything from a network not configured properly to data packets being lost, especially in a wireless access environment. Even poorly written programming code upon which e-Government service was developed can be very susceptible to threats [15].

c. Denial of service: (DoS) attacks (loss of availability): The main aim of DoS is the disruption of services by attempting to limit access to a machine or service. The most common DoS attacks target the computer network's bandwidth or connectivity [16]. In bandwidth attacks, the network is flooded with a high volume of traffic leading to the exhaustion of all available network resources, so that legitimate user requests cannot get through, resulting in degraded productivity. In connectivity attacks, a computer is flooded with a high volume of connection requests leading to the exhaustion of all available operating system resources, thus rendering the computer unable to process legitimate user

requests [16]. Therefore, in order to have effective e-government services without interruptions in Web access as well as e-mail and database services, there is a need for protection against DoS attacks.

d. Web spoofing: Web spoofing is an electronic deception related to the Internet. It occurs when the attacker sets up a fake website which almost looks the same with the original website in order to lure consumers to give their credit card numbers or other personal information [15]. E-Government services website should have the capability to authenticate itself in order to gain citizens' trust and confidence towards the security of their information.

e. IP spoofing: IP address spoofing refers to the creation of Internet Protocol packets with a forged source IP address, called spoofing. It is a method of attacking a network in order to gain unauthorized access [17]. The intent here is to change the source address of a data packet to give it the appearance that it originated from another computer. IP Spoofing is typically used to start the launch of a Denial of Service Attack [18]. The real attacker is difficult to be identified with IP spoofing, since all e-Government server logs will show connections from a legitimate source.

f. Spyware threats: A spyware is a serious computer security threat. It is any program that monitors users' online activities or installs programs without users consent for profit or to capture personal Information [19]. E-Government services should have the capability to detect and prevent the activities of spyware in order to gain citizens' trust and confidence towards the security mechanisms provided by e-Government services.

g. Unauthorized information access: Unauthorized information access attack has two types, the first type is where unauthorized users were able to access organizations' ICTs resources. The second type is where authorized users with limited access expand their authorizations illegally (e.g. privilege escalation) [20]. Access control constrains what a user can do directly, as well as what programs executing on behalf of the users are allowed to do. In this way, access control seeks to prevent activity that could lead to breach of security [21].

h. Loss of integrity (unauthorized modification): Integrity means capability to prevent information from unauthorized modification, and ensuring that information can be relied upon and is accurate and complete [22]. Attacks on data integrity involve intentional or unintentional unauthorized modifications of data at some point in their life cycle. E-Government services should have a capability to prevent unauthorized modification of information to assure users that the information received are not fabricated.

2.2 Non-Technical Security Threats of e-Government Services

Non-technical security threats are those threats by which an attacker uses chicanery to trick people into revealing sensitive information or performing actions that compromise the security of a network. Non-technical threats include:

a. Acts of God (Natural Disasters): Nobody can stop nature from taking its course. Earthquakes, hurricanes, floods, lightning, and fire can cause severe damage to computer systems. Information can be lost, downtime or loss of productivity can occur, and damage to hardware can disrupt other essential services [23]. Few safeguards can be implemented against natural disasters. The best approach is to have disaster recovery and contingency plans in place.

b. Physical infrastructure attacks: Physical infrastructure attacks are attacks that directly target physical equipments of ICT assets. These attacks can be in a form of theft or damage of hardware, software or other devices on or over which information is stored or transmitted. This could lead to permanent loss or unauthorized access to critical information. This type of attacks can cause unavailability of e-Government services. Access points such as delivery and loading areas and other points where unauthorized users may enter the premises of the organization should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

c. Internal staff irregularities and illegal operations: Internal staffs are frequently making unintentional errors that contribute to security problems, directly or indirectly. Sometimes these errors can become threats, such as a data entry error or a programming error that crashes a system. To reduce staff irregularities and illegal operations, organizations should conduct security

awareness training and education programs periodically.

d. Social engineering and phishing attacks: Social engineering attacks are usually conducted by hackers who use a variety of psychological tricks to get the computer user to give them the information they need to access a computer or network [24]. Social Engineering is the art of exploiting the weakest link of information security systems: the people who are using them. Victims are deceived in order to release information or perform a malicious action on behalf of the attacker [25]. This attack might involve gaining the confidence of individuals with access to secure information, tricking them into thinking there is a legitimate request to access secures information; physical observation; and eavesdropping on people at work. Social Engineering provides hackers with efficient short cuts, and in many cases facilitates attacks that would not be possible through other means [26]. On the other hand, phishing can be thought of as the marriage of social engineering and technology [27]. Phishing is a form of online identity theft that aims to steal sensitive information from users such as online banking passwords and credit card information [28]. For example, an attacker may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts. Security awareness training and education programs are considered as the effective security countermeasures towards social engineering and phishing attacks.

2.3 Objectives

The general objective of the study reported in this paper was to develop a holistic secured e-Government Maturity Model for protecting e-Government services with Tanzania as a case study. Specific objectives of this study were as follows:

a. To identify technical security threats of e-Government services.
b. To identify non-technical security threats of e-Government services.
c. To design a holistic secured maturity model for protecting e-Government services, Tanzania as a case study.

2.4 Related Work

There are several maturity models of e-Government services that exist today. The design of these models, however, do not consider security as a specific issue. Most of these models consider security at the transaction stage [9]. Various researchers proposed different methods and systems to provide security in e-Government services. In [29], Mwakalinga proposed an integrated security system for e-Government services. This security system provides multiple authorization schemes, information integrity schemes and digital signature schemes. The system integrates a registration system, a certification system, an authorization system, and a smart card system. It is based on the Security Assertion Markup Language (SAML) standard, which is an XML-based framework for exchanging security information. The system can be integrated in existing e-Government systems and can be built-in in new e-Government systems [29]. However, the system neither provides denial of service security service nor support e-Government wireless services' security. The system has not yet been implemented and so there are no results on its performance [29].

In their paper [30], Edwards et al. propose a model that integrates security into eGMMs at the various stages with an e-Government System Security Model (eGSSM). The eGSSM is a theoretical framework, which is multidimensional in construct and employs a risk-based approach to integrating security into eGMMs. The key component to this model is the e-Government Maturity Trigger. This trigger assesses a government's ability to address Key Domain Areas within the e-Government Stage Process Maturity (eGSPM) and mitigate security risk using the National Institute of Standards and Technology, Risk Management Framework (NIST RMF) in the e-Government Security Risk Maturity (eGSRM). Define, Measure, Analyse, Improve and Control (DMAIC) principles are applied for measuring, controlling and reporting process performance, to achieve an optimal capability level that will trigger maturity and onward progression to the successive stages. The model depends on risk management approach, and hence, none of the non-technical security cotrols were considered in its development phases.

In the Tanzanian context reported in [12, 31], Karokola et al. propose a framework for securing e-Government services. The framework was developed by integrating IT security services into e-Government Maturity Model (eGMM) critical stages. The identified critical stages of the proposed eGMM are as follows: (1) web presence; (2) interaction; (3) transaction; (4) transformation; and

(5) continuous improvements [31]. The framework was a result of integrating Information Security Maturity Model (ISMM) critical levels into e-Government Maturity Model (eGMM) critical stages [12]. The identified critical levels of ISMM are as follows: (1) undefined; (2) defined; (3) managed; (4) controlled; and (5) optimized. The framework addresses both technical and non-technical security services within the critical stages of eGMM. The security strengths of the framework depend upon the security services requirements control areas (SCRAs) available in the framework. Unfortunately, the design of those SCRAs are complicated in such a way that it is difficult to be translated into actions by the personnel at the operational level.

In our proposed model, we simplify the task of translating into actions the security related aspects required by e-Government services by including the security layers which consist of technical and non-technical security related aspects at each of the four proposed critical stages of the model as described in Section 4.

3. Methodology

The desk review was conducted to identify technical and non-technical security threats to e-Government services. Information security articles and journal papers were analyzed to extract the mentioned threats as a part of the extensive research background as mentioned in Sections 2.1 and 2.2; the third research objective was to design a holistic secured e-Government maturity model for protecting e-Government services. Since our case study is e-Government in Tanzania context, and we observed that e-Government in Tanzania adopts Gartner's four stage maturity model [6], the proposed secured maturity model for protecting e-Government services was designed by including security layers which consist of technical and non-technical security related aspects in each of its four stages (*presence*, *interaction*, *transaction* and *transformation*). The model designing process was done based on the ISO/ IEC 27002 security standard and guided by a Design Science Research Methodology (DSR) [32]. The applied DSR steps were: problem identification and motivation, definition of the objectives for a solution, developing the model [32]. Design Science Research methodology was chosen because it focuses on the development and performance of (designed) artifacts with the explicit intention of improving the functional performance of the artifact [33].

4. The Proposed Model

E-Government services development is guided by the so called maturity models that outline various stages for e-Government development. In order to achieve a secure e-Government services delivery, we recommend security related aspects to be addressed as a specific issue at various maturity models stages and not just at the transaction stage [5, 34]. However, no stage is immune to security related issues. This means that there is potential for security being a significant component impacting e-Government at all stages of the maturity levels. This therefore calls for security to be equally addressed at every stage of the e-Government maturity model. 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. We summarize the proposed secured e-Government maturity model in Table 1. The table shows the security layers to be included into the model. The security layers include technical and non-technical security control elements. The proposed security layers are further described in the following paragraphs.

a. Secured Digital Presence

This stage involves simple provision of government information through website (static) with basic information that the citizen can access [9]. 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 [35]. The most important security related aspects to be considered at this stage are information availability and entity authentication. These aspects can be obtained through both technical and non-technical security controls. Security practices to be considered at this stage are shown in Table 1. The security controls at this stage aim at preventing unauthorized physical access or interference with the organization or ICT equipments and information assets.

b. 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 [36]. 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. These aspects can be achieved through the implementation of all security practices required at secured digital presence stage together with the implementation of database security controls, audit management and the presence of the adequate bandwidth capacity. Other security practices to be considered at this stage are also shown in Table 1.

c. 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. At this stage, the security layer should include the implementation of certificate/ digital signature and secure data transmission in order to achieve data integrity and confidentiality of citizens' personal information. The exchanged message should be encrypted in order to ensure their confidentiality. The data contained in the e-Government services and exchanged between the different government agencies must remain confidential. Other security practices to be considered at this stage are as well shown in Table 1.

d. Secured Transformation

This stage allows users of e-Government services to interact with government as one entity instead of individual government organizations [6]. Information systems are integrated, and the citizens 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, non-repudiation, 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. The security layer should also have the capability of filtering service access, because some agencies will not have the right to invoke a certain service while others do. At this stage access control mechanisms should be implemented together with other security practices as shown in Table 1.

Table 1: Mapping matrix of ISO/ IEC 27002 domains and the Secured e-Government Maturity Model (SeGMM)

SN	Domain Name	Domain Security Control Elements	SeGMM (Scope of Applicability)			
			Layer			
	Non-Technical Security Control Elements		**1**	**2**	**3**	**4**
1	Risk Assessment and Treatment	Assessing security risks	√	√	√	√
		Treating security risks	√	√	√	√
2	Security Policy	Information security policy	√	√	√	√
3	Organization of Information Security	Internal organization	√	√	√	√
		Security of third parties access	√	√	√	√
		Security outsourcing	√	√	√	√
4	Assets Management	Accountability for Assets	√	√	√	√
		Information classification			√	√
5	Human Resource Security	Security prior to employment	√	√	√	√
		Security during employment	√	√	√	√
		Security after change of employment	√	√	√	√
		Security awareness, training, and education	√	√	√	√

6	Physical and Environmental Security	Secure areas	√	√	√	√
		Equipment security	√	√	√	√
7	Communications and Operations Management Security	Operational procedures and responsibilities	√	√	√	√
		Third party service delivery management	√	√	√	√
		Systems planning and acceptance	√	√	√	√
		Media handling security			√	√
8	Access Control	Business Requirement for access control		√	√	√
		User responsibilities		√	√	√
		Mobile computing and teleworking	√	√	√	√
9	Information Systems Acquisitions, Development and Maintenance	Security requirements of systems	√	√	√	√
		Security in development and support processes	√	√	√	√
10	Information Security Incident Management	Reporting security events and weaknesses	√	√	√	√
		Management of security incidents and improvements	√	√	√	√
11	Business Continuity Management	Disaster Recovery Planning	√	√	√	√
12	Compliance	Compliance with legal requirements			√	√
		Compliance with security policies and standards	√	√	√	√
		Information systems audit considerations			√	√
Technical Security Control Elements						
1	Communications and Operations Management Security	Protection against malicious software	√	√	√	√
		Back-up	√	√	√	√
		Network security management	√	√	√	√
		Exchange of information			√	√
		Electronic services security		√	√	√
		Monitoring system	√	√	√	√
2	Access Control	User access management	√	√	√	√
		Network access control		√	√	√
		Operating systems access control	√	√	√	√
		Application and information access control			√	√
3	Information Systems Acquisitions, Development and Maintenance	Security in processing application			√	√
		Cryptographic controls		√	√	√
		Security of system files			√	√
		Technical Vulnerability Management	√	√	√	√
4	Technical Security Controls	Encryption tools			√	√
		Authentication tools		√	√	√
		Access control tools	√	√	√	√
		Digital signatures	√	√	√	√

5. Conclusion

In this paper, development of a holistic secured e-Government Maturity Model for protecting e-Government services in Tanzania is reported. The technical and non-technical security threats that impact delivery of e-Government services have been identified. The model design process followed the ISO/ IEC 27002 security standard and was guided by a design science research methodology. The proposed secured e-Government maturity model is designed by including the security layers which consist of technical and non-technical security related aspects in each of its four maturity stages. The model can be applied as an information security checklist for e-Government services development activities such as planning, analysis, design, implementation and maintenance. The

model also provides a method by which public organizations can achieve secure e-Government services. Further research work to test and validate the proposed model into one of the earlier studied organizations is recommended.

References

[1] S. Basu, "E-government and developing countries: an overview," *International Review of Law, Computers & Technology*, vol. 18, pp. 109-132, 2004.

[2] Y. Chen, *et al.*, "E-government strategies in developed and developing countries: An implementation framework and case study," *Journal of Global Information Management (JGIM)*, vol. 14, pp. 23-46, 2006.

[3] R. Alshboul, "Security and Vulnerability in the E-Government Society," *Contemporary Engineering Sciences*, vol. 5, pp. 215-226, 2012.

[4] N. Nkwe, "E-government: challenges and opportunities in Botswana," *International Journal of Humanities and Social Science*, vol. 2, pp. 39-48, 2012.

[5] M. Dewa and I. Zlotnikova, "Citizens' Readiness for e-Government Services in Tanzania," *Advances in Computer Science: an International Journal*, vol. 3, pp. 37-45, 2014.

[6] President's Office - Public Service Managements, "Tanzania e-Government Strategy," ed, 2012. Retrieved on 10th February 2013 from the website www.utumishi.go.tz

[7] A. Fath-Allah, *et al.*, "E-Government Maturity Models: A Comparative Study," *International Journal of Software Engineering & Applications (IJSEA)*, vol. 5, pp. 71-91, 2014.

[8] Z. Irani, *et al.*, "Transaction stage of e-government systems: identification of its location and importance," in *System Sciences, 2006. HICSS'06. Proceedings of the 39th Annual Hawaii International Conference on*, 2006, pp. 82c-82c.

[9] G. Karokola and L. Yngström, "Discussing E-Government Maturity Models for the Developing World-Security View," in *ISSA*, pp. 81-98, 2009.

[10] M. Wimmer and B. Von Bredow, "A holistic approach for providing security solutions in e-government," in *System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on*, 2002, pp. 1715-1724.

[11] S. S. Alaboodi, "Towards evaluating security implementations using the Information Security Maturity Model (ISMM)," M.Sc. Thesis, University of Waterloo, Ontario, Canada, 2007.

[12] G. Karokola, *et al.*, "Towards An Information Security Maturity Model for Secure e-Government Services: A Stakeholders View," in *HAISA*, pp. 58-73, 2011.

[13] G. Heiser, "Protecting e-government against attacks," NICTA and University of New South Wales, Sydney, Australia, ed 2013, Retrieved on 17th May 2014 from the website www.nicta.com.au

[14] M. H. Zu'bi and H. H. Al-Onizat, "E-Government and Security Requirements for Information Systems and Privacy," *Journal of Management Research*, vol. 4, pp. 367-375, 2012.

[15] H. Grewal and Shivani, "A Study of Ethical and Social Issues in E-Commerce," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 2, pp. 167-174, 2012.

[16] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: classification and state-of-the-art," *Computer Networks*, vol. 44, pp. 643-666, 2004.

[17] M. Sahu and R. C. Lal, "CONTROLLING IP SPOOFING THROUGH PACKET FILTERING," *International Journal of Computer Technology and Applications*, vol. 3, pp. 155-159, 2012.

[18] A. H. Alqahtani and M. Iftikhar, "TCP/IP Attacks, Defenses and Security Tools," *International Journal of Science and Modern Engineering (IJISME)*, vol. 1, pp. 42-47, 2013.

[19] A. Ahmad, "Type of Security Threats and Its Prevention," *International Journal of Computer Technology & Applications*, vol. 3, pp. 750-752, 2012.

[20] I. Alsmadi, "Security Challenges For Expanding E-governments' Services," *International Journal of Advanced Science and Technology*, vol. 37, pp. 47-60, 2011.

[21] R. S. Sandhu and P. Samarati, "Access control: principle and practice," *Communications Magazine, IEEE*, vol. 32, pp. 40-48, 1994.

[22] C. E. Jiménez, *et al.*, "e-Government: Security Threats," IEEE Special Technical Community on *e-Government*, vol. 11, p. 21, 2012.

[23] H. Eken, "Software Security of Web Application and Web Attacks," *International Journal of eBusiness and eGovernment Studies*, vol. 5, pp. 70-78, 2013.

[24] T. R. Peltier, "Social engineering: concepts and solutions," *Information Systems Security,* vol. 15, pp. 13-21, 2006.

[25] M. Huber, *et al.*, "Towards automating social engineering using social networking sites," in *Computational Science and Engineering, 2009. CSE'09. International Conference on*, 2009, pp. 117-124.

[26] I. S. Winkler and B. Dealy, "Information Security Technology? Don't Rely on It. A Case Study in Social Engineering," in *USENIX Security*, 1995.

[27] M. Jakobsson and A. L. Young, "Distributed Phishing Attacks," *IACR Cryptology ePrint Archive,* 2005. Retrieved on 23rd April 2014 from the website https://eprint.iacr.org

[28] E. Kirda and C. Kruegel, "Protecting users against phishing attacks with antiphish," in *Computer Software and Applications Conference, 2005. COMPSAC 2005. 29th Annual International*, pp. 517-524, 2005.

[29] G. J. Mwakalinga and L. Yngström, "Integrated Security System for E-Government based on SAML Standard," *Proceedings of the Information Security South Africa (ISSA)* 2004.

[30] D. C. Edwards, *et al.*, "E-government system security model (egssm): A multidimensional, risk based approach to e-government," in *Privacy, security, risk and trust (passat), 2011 ieee third international conference on and 2011 ieee third international conference on social computing (socialcom)*, 2011, pp. 1273-1277.

[31] G. Karokola, *et al.*, "Secure e-Government Services: Towards a Framework for Integrating IT Security Services into e-Government Maturity Models," in *Information Security South Africa (ISSA)*, pp. 1-9, *2011*.

[32] K. Peffers, *et al.*, "A design science research methodology for information systems research," *Journal of management information systems,* vol. 24, pp. 45-77, 2007.

[33] L. Teran, "SmartParticipation: A Fuzzy-Based Recommender System for Political Community-Building," PhD Thesis, Springer Publishing Company, Incorporated, 2014.

[34] M. Dewa and I. Zlotnikova, "Current Status of e-Government Services in Tanzania: A Security Perspective," *Advances in Computer Science: an International Journal,* vol. 3, pp. 114-122, 2014.

[35] M. Sellami and M. Jmaiel, "A Secured Service-Oriented Architecture for E-government in Tunisia," *ReDCAD research unit National School of Engineers of Sfax*, 2007. Retrieved on 9th February 2014 from the website http://www.emn.fr/z-info/sellami

[36] H. Yousefi-Azari, "Implementing e-Government in Iran " *Proceedings of the 8th European Conference on Information Warfare and Security*, pp. 696-702, 2009.

[37] J. Yonazi, "Adoption of Transactional Level e-Government Initiatives in Tanzania," 2013. Retrieved on 13th April 2014 from the website www.clknet.or.tz

Authors Biographies

Mohamed D. Waziri[1] is a doctoral student at the Nelson Mandela African Institution of Science and Technology. He holds a M.Sc. in Computer Science from the University of Khartoum (2007). He also holds a B.Sc. in Computer Science from the International University of Africa (2003). Mr. Waziri is currently employed at the University of Dodoma (UDOM) as an Assistant Lecturer. Prior to joining UDOM he was working as an Assistant Lecturer at the International University of Africa, Khartoum, Sudan.

Eng. Dr. Zaipuna O. Yonah[2]: MIET, MIEEE – holds a B.Sc. degree (with Hons – 1985) in Electrical Engineering from University of Dar es Salaam – Tanzania: and M.Sc. (1988) and PhD (1994) Degrees in Computer-Based Instrumentation and Control Engineering from the University of Saskatchewan, Saskatoon – Canada. In Tanzania, he is a Registered Consulting Engineer in ICTs. Dr. Yonah has over 30 years of practice. His work spans the academia, industry and policy making fields. He is currently associated with The Nelson Mandela African Institution of Science and Technology – (school of Computation and Communication Science and Engineering), and the IEEE Inc. He is one of the pioneers driving the national broadband agenda in Tanzania. He believes that ICTs, as tools for development, promise so much: *interactivity, permanent availability, global reach, reduced per unit transaction costs, creates increased productivity and value, jobs and wealth, multiple source of information and knowledge.* Armed with such a belief, his current work aims at creating and delivering value through ICT – enabled services in the shortest times possible. His research interest include: ICT4D, Cyber Security, ICT Policy and Regulation, Mobile and Web applications, high-capacity broadband networks, Intelligent Instrumentation and Control Engineering, and ICT enabled 21st Century Education delivery (ICT4E).