ACSIJ Advances in Computer Science: an International Journal, Vol. 3, Issue 6, No.12 , November 2014
ISSN : 2322-5157
www.ACSIJ.org

ACSIJ
WWW.ACSIJ.ORG

Towards a Secure Maturity Model for Protecting e-Government Services in Tanzania: A Stakeholders View

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 as a tool for guiding the development and implementation of e-Government services. The government of Tanzania recognizes that e-Government services can accelerate the achievement of a sustainable social and economic development in the country. However, despite the good benefits provided by e-Government services, information security and privacy are the most significant obstacles for e-Government services adoption. Unfortunately, very few designs of e-GMMs have considered security as a specific issue. However, even these few security responsive models consider security mostly at the transaction stage. Responding to this security weakness of eGMMs, in our earlier work a holistic secure e-Government maturity model that includes security layers consisting of technical and non-technical security related aspects in each of its four maturity stages was developed, but the model was not yet tested and evaluated. This paper reports on the tests and the validation of the proposed secure model. The applied evaluation criteria were: simplicity, reliability, accessibility and usability, dynamics and flexibility, applicability, coverage and completeness, and compliance with legal aspects. Primary data were collected from five Tanzanian public organization using questionnaires. The collected data were processed and analyzed using the SPSS. The overall results show that the model designs meet all required specifications to successfully secure e-Government services, and the model was accepted by majority of the respondents at different organizational levels (strategic, tactical, and operational).

Keywords**:** e-*Government, e-Government services, e-Government maturity model, information security,security layer*

1. Introduction

With the recent advancements of Internet technologies, majority of governments around the world have adopted Information and Communication Technologies (ICTs) to provide services towards its agencies, businesses and citizens more efficiently and effectively. In general, e-Government refers to the use of ICTs by government organizations to provide and enhance delivery of public services. In the Tanzanian context, e-Government is about delivering quality services to the public through technology [1]. It involves using ICTs to support processes within the government as well as for the delivery of services to beneficiaries, such as citizens, businesses and agencies. In practice, e-Government websites or portals provide governments the best opportunities to improve their administrative processes and procedures, to connect to their citizens effectively as well as to build and bond interactively with its agencies and businesses [2].

Tanzania is one of many developing countries with multiple e-Government initiatives being introduced to support poverty reduction, and sustain good governance, as demonstrated by recent technology implementations and reported in government strategy documents [3]. The government of Tanzania recognizes that through e-Government services a sustainable social and economic development in the country is achievable. As a result, the Government has increased the range and quality of the services provided by public sector [1]. The Government also recognizes the importance of e-Government in promoting and improving efficiency in public services delivery and strengthening citizen's participation and engagement. However, despite the good benefits provided by e-Government services, a number of obstacles exist that hinder achieving these desired benefits. Specifically, information security and privacy are among the most significant obstacles faced when implementing e-Government initiatives [4]. As a result, there are increasing concerns about the reliability and security of the developed e-Government services. These concerns have flagged the need to guarantee and to ensure that services are provided to customers with the maximum possible security, with guaranteed privacy [5]. The current trend is that citizens prefer to use traditional ways rather than using an unsecured e-Government service. Noted also is that citizens' adoption of e-Government services plays an important role in the success of e-Government initiatives. Thus, low adoption, particularly by citizens, indicates inadequate utilization and rejection of the initiatives by the intended users, and this may lead into failure of e-Government initiatives [6].

Various researchers have proposed different methods and systems to provide security in e-

Government services. In [7], Wimmer and Bredow propose in a comprehencive way a holistic approach that integrates security aspects from the strategic level down to the data and information level in order to address different security aspects of e-Government services. Their holistic approach consists of four layers, namely: strategic, process level, interaction and information.

In the Tanzanian context reported in [8], Dewa and Yonah propose a holistic secured e-Government Maturity Model consisting of both technical and non-technical security aspects for protecting e-Government services with Tanzania as a case study. With a holistic approach, security is considered beyond the technical aspects. Social, political, cultural, and legal impacts on security requirements are considered as well [9]. The model design process was based on ISO/ IEC 27002 and was guided by a Design Science Research methodology (DSR). The applied DSR steps were: problem identification and motivation, definition of the objectives for a solution, and development of the model [10]. However, one step remained to be applied that is: model evaluation, to test if the model meets the specifications and that it fulfils its intended purpose. Thus, the purpose of this paper is to report on the tests and validation of the holistic secure maturity model for protecting e-Government services with Tanzania as a case study proposed in [8].

The rest of the paper is organized as follows: Section two presents the background of the designed secure maturity model; Section three outlines the research methodology; Section four presents the results and discussion; Section five outlines recommendations; and lastly, the conclusion is given in Section six.

2. Background

Information security and privacy have been widely recognized as the main obstacles to the adoption of e-Government services. In [11], Dewa and Zlotinikova identify the information security requirements to e-Government services. Those security requirements include confidentiality, integrity, availability, non-repudiation, authentication, authorization (access control), traceability, accountability, user anonymity, and security awareness. However, e-Government services may not require the application of all identified security requirements. Typically, each e-Government service has its own specific security requirements depending on the services it provides.

Practically, information security of e-Government services is influenced by how these services were developed, and e-Government Maturity Models (eGMMs) are widely used as a tool for guiding the development and implementation of e-Government services. An eGMM is a set of stages (from basic to advanced ones) that determines the maturity of the e-Government [12]. For instance, West proposes a three stage model [13], Layne and Lee propose a four stage model [14], Hiller and Belanger propose a model with five stages [15], and Deloitte and Touche propose a six stage model [16]. The critical weakness of the existing models is the consideration of security related issues at the transaction stage only [17]. In order to secure eGMMs, both technical and non-technical security related aspects should be considered at all stages of the maturity models. Responding to the eGMMs weakness, a secure e-Government maturity model was developed as presented in [8]. The following paragraphs briefly describe the model.

A secure e-Government maturity model includes security layers that consist of technical and non-technical security related aspects at each of the four proposed critical stages of the model. The critical stages of the model are: (a) secured digital presence, (b) secured interaction, (c) secured transaction, and (d) secured transformation [8]. It was recommended that implementation of the model should be based neither on a specific technology/protocol nor on a certain security system/product, but rather be based on an approach towards a structured and efficient implementation of those technologies.

At secured digital presence 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 most important security related aspects to be considered at this stage are information availability and entity authentication. The security controls at this stage aim at preventing unauthorized physical access or interference with the organization or ICT equipment and information assets.

The second stage of the model is secured interaction stage. At this stage, security layer should have the ability to authenticate a user/ citizen asking for a service. The most important security aspects of 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.

At secured transaction stage the most important security aspects 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.

A security layer at secured transformation stage 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. The most important security aspects of this stage are personal information confidentiality, identity authentication, availability, non-repudiation, accountability and integrity. At this stage, access control mechanisms should be implemented together with other security practices.

2.1 Objectives

The general objective of the study reported in this paper was to test and validate the proposed holistic secure maturity model for protecting e-Government services with Tanzania as a case study. Specific objectives of this study were as follows:

a. To identify the criteria used to evaluate the model.
b. To test and validate the model.
c. To recommend activities for improving the model and security of e-Government services in Tanzania.

3. Methodology

For the purpose of testing and validating the proposed holistic secure maturity model for protecting e-Government services in Tanzania, data were collected using structured questionnaires. The questionnaires were distributed to staffs with ICTs skills or ICTs security expertise at three different organizational levels: strategic, tactical and operational. In order to achieve a comprehensive model evaluation, it was important to identify evaluation criteria. Based on literature [18-21] seven model evaluation criteria were selected. The identified criteria were: simplicity, reliability, accessibility and usability, dynamics and flexibility, applicability, coverage and completeness, and compliance with legal aspects. The validation plan is further explained in the following sub-sections.

3.1 Population and Sampling Method

A population of government organizations staff was consulted to test and validate the model. Specifically staffs with ICTs skills or ICTs security expertise at strategic, tactical and operational levels were consulted. The targeted research sample involved the five government organizations studied earlier [11]. Due to confidentiality reasons, we referred them as Organizations A, B, C, D and E as follows [11]: Organization A is a public organization responsible for managing the overall revenue, expenditure and financing of the government. Organization B is a public organization responsible for management of public services. Organization C is a public organization responsible for managing the assessment, collection and accounting of all central government revenue. Organization D is a public organization responsible for generating, transmitting, distributing and selling electricity. Organization E is a public organization responsible for coordinating, encouraging, promoting and facilitating investment. Initially, the sample size of the population was estimated at 60. We distributed 70 questionnaires, and 45 responses were received.

3.2 Data Collection

Primary data were collected by using the questionnaires. In order to ensure validity of the questionnaires, a pilot study was conducted prior to distributing the questionnaires to respondents. Twenty five questionnaires were delivered to the respondents, but only 11 responded. Necessary improvements to the questionnaire were done, and the improved version of the questionnaires was distributed to the sample population. Table 1 shows the distribution of the respondents within the studied organizations.

Table 1: Summary of the respondents in the studied organization

Organization name	**Responded Staff**		
	Strategic Level	**Tactical Level**	**Opera-tional Level**
A	1	2	8
B	1	2	7
C	1	2	9
D	1	1	5
E	-	1	4
Total	**4**	**8**	**33**
	45		

3.3 Reliability and Goodness of Fit Measurement.

Analysis of internal consistency of the questions was conducted by doing a reliability test by using the Statistical Package for Social Sciences (SPSS). The calculated Cronbach's alpha was 0.966 and

since it is generally agreed that an alpha of 0.70 and above is acceptable [22], therefore, the calculated Cronbach's alpha was found suitable. To assess goodness of fit for all survey questions, a Chi-square test was conducted and the results showed statistical significance because all the variables had p-value 0.000 (degree of freedom = 4) which is less than any level of significance that is 1% , 5% and 10%.

3.4 Data Processing and Analysis

The content analysis technique was used for processing and analyzing descriptive data. SPSS and Microsoft Excel were used for data analysis. Various analysis techniques including descriptive statistics, especially frequency and a Chi-square test were used to measure both goodness of fit and relationship between variables. The results were presented using charts as presented in Section 4.

4. Results and Discussions

4.1 Model Testing and Validation

The purpose of this paper was to test and validate the model. The aim of this process is to evaluate the proposed model to assess if it is correct, complete, being implemented as intended, and delivering the intended outcome. Typically, an evaluation process involves comparing the objectives of a solution to actual observed results from the use of the developed model. In our case, this was done through identification and analysis of the model evaluation criteria. The identified criteria were as follows: (1) simplicity; (2) reliability; (3) accessibility and usability; (4) flexibility; (5) applicability; (6) coverage and completeness; and (7) compliance with legal aspects. As mentioned earlier, we received 45 responses, and these responses were processed and analyzed by using the Statistical Package for Social Sciences.

4.1.1 Simplicity

Simplicity is the state or quality of being easy to understand or use. The aim of this evaluation criterion was not only to assess if the model was designed in such a way that it is clear and easily understandable to e-Government services implementation team, but also to assess if the model was designed in such a way that it is easy to implement. Figure 1 shows the results of the analysis of collected data against the simplicity criterion interms of the model clarity and comprehensibility.

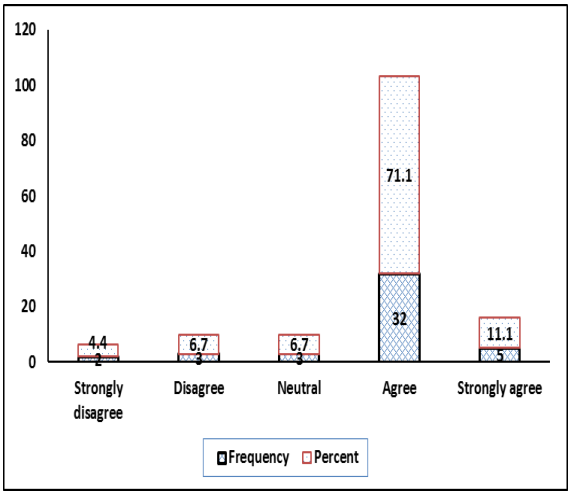

Figure 1: Respondents' responses on the model clarity and comprehensibility satisfaction.

Evident from this figure is that 82.2% (summation of 71.1% and 11.1%) of the respondents were satisfied with the simplicity of the model in terms of its clarity and comprehensibility to e-Government services developers. The analysis also shows that 75.6% (summation of 66.7% and 8.9%) of the respondents were also satisfied with the simplicity of the model in terms of the model implementation as shown in Fig. 2. These results imply that the respondents observed the model design to be clear and easily understandable to e-Government developers and implementers. Therefore, the model design reflects and considers the implementation environment in terms of in-house e-Government services developers' skills.

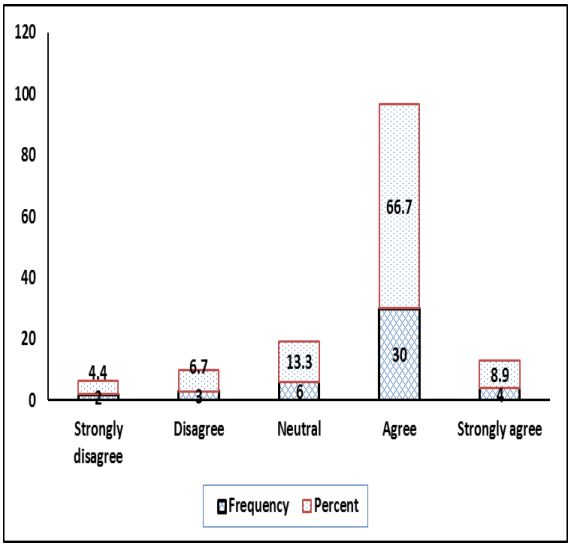

Figure 2: Respondents' responses on the model ease to implement satisfaction.

4.1.2 Reliability

Reliability is a quality of being reliable, dependable or trustworthy. The aim of this evaluation criterion was to assess if the model performs its required functions under stated conditions for a specified

period of time. Specifically, this criterion assesses if the implementation of the model is capable of treating security risks and threats posed to the current e-Government services consistently. Information security risk assessment provides organizations a capability of discovering, correcting and preventing security problems in e-Government services. The risk assessment helps each organization to determine the acceptable level of risk and the resulting security requirements for each system.

The results show that 84.4% (summation of 71.1% and 13.3%) of the respondents were satisfied with the reliability of the model. This implies that the model design considers information security risk assessment and treatment consistently. Figure 3 shows the respondents' responses on the model reliability satisfaction.

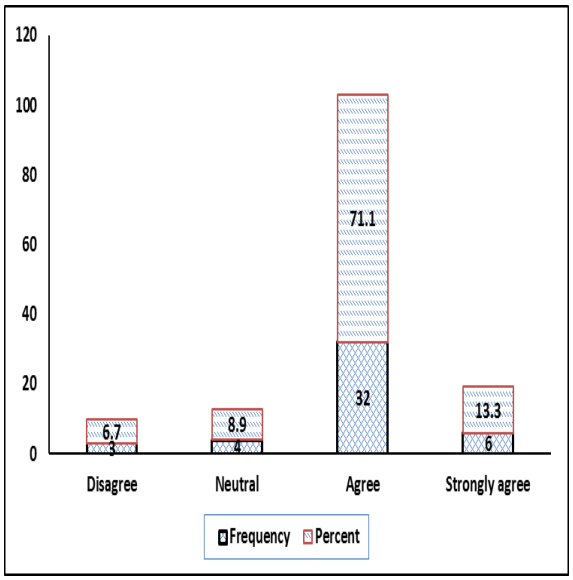

Figure 3: Respondents' responses on the model reliability satisfaction.

4.1.3 Accessibility and Usability

Accessibility is the state of being easily accessible, while usability is the ease of use of an object. The object of use can be a software application, website, framework, model, machine, process, or anything a human interacts with. The aim of this evaluation criterion was to assess if after the implementation of the model in e-Government services, the legitimate users can access the e-Government services easily. Specifically, in this criterion we assess if the implementation of the model affects negatively the accessibility and usability of e-Government services to legitimate users. Normally, information security controls weaken the accessibility and usability of the information systems. To reduce this weakness, the model should balance between achieving information security and accessibility or usability of e-Government services. Figure 4 shows the respondents' responses on the model accessibility and usability satisfaction.

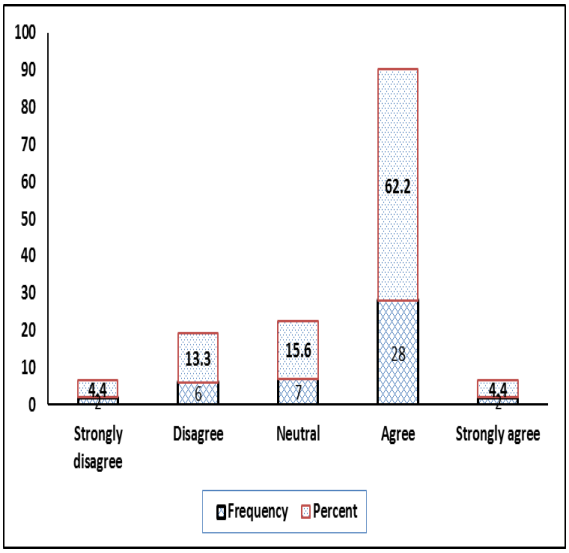

Figure 4: Respondents' responses on the model accessibility and usability satisfaction.

The results show that 66.6% (summation of 62.2% and 4.4%) of the respondents were satisfied with the accessibility and usability of the model. In addition, the results show that the model designs have the capacity make sure that security aspects do not compromise accessibility and usability of e-Government services.

4.1.4 Flexibility

Flexibility is the ability to be easily modified or responsive to change. Given that ICTs are advancing rapidly, computer hackers and attackers are also advancing their techniques. Attackers are always coming up with new ways to defeat the improved security protection. In this situation, any security design tool or method should have a capability of being flexible to catch up any technological advances. Therefore, the aim of flexibility criterion was to assess if the model is dynamic enough to deal with possible future security risks and threats. Figure 5 shows respondents' responses on the model flexibility satisfaction.

The results show that 71.1% (summation of 64.4% and 6.7%) of the respondents were satisfied with the capability of the model to respond rapidly with the technology advancement to deal with possible future security risks and threats. This outcome implies that the model design enables the organization to review security risks and threats of the e-Government services periodically.

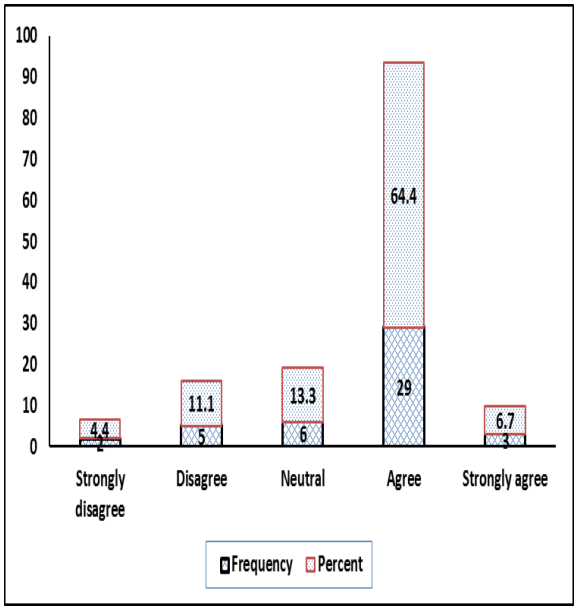

Figure 5: Respondents responses on the model flexibility satisfaction.

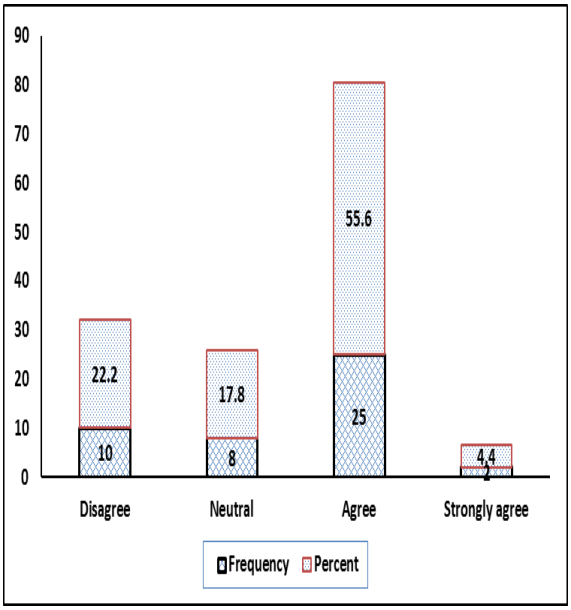

Figure 6: Respondents' responses on the model relevance to the organizations' ICTs infrastructure.

4.1.5 Applicability

Applicability is the state of being pertinent, relevant or appropriate. The aim of this evaluation criterion was to assess if the model was designed in such a way that it fits in with both existing organizations' ICTs infrastructure and operational environment, and whether the adoption of the model is supported by the top management of the organizations.

The analysis of the collected data shows that 60.0% (summation of 55.6% and 4.4%) of the respondents) were satisfied with the organizations' ICTs infrastructure to accommodate the model as shown in Fig. 6. It was also observed that 53.4% (summation of 46.7% and 6.7%) of the respondents were satisfied with the organizations' operational environment to accommodate the model as shown in Fig. 7. Finally, the analysis results for this criterion show that 66.6% (summation of 53.3% and 13.3%) of the respondents were satisfied with the support provided by the top management of their organizations for the adoption of the model as shown in Fig. 8. These results carries the assurance that the model designs relatively can be applied in approximately 50 percent of the public organizations in the country.

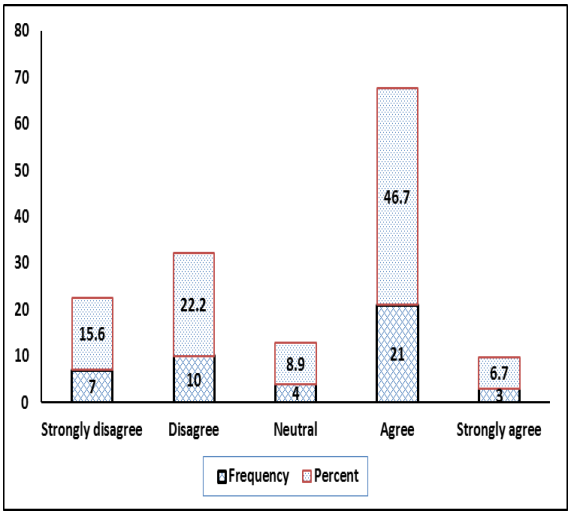

Figure 7: Respondents' responses on the model relevance to the organizations' operational environment.

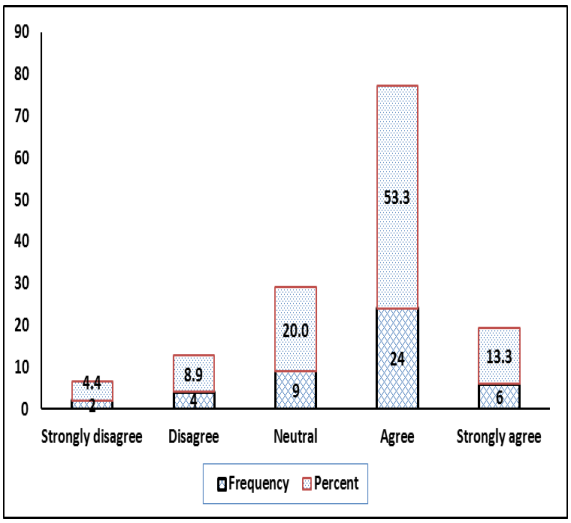

Figure 8: Respondents' responses on the model relevance to the organizations' top management support.

4.1.6 Coverage and Completeness

Coverage and completeness is the extent to which something considers all parts or elements as originally planned. In designing a model, a developer should consider all aspects to make it complete and perfect. The aim of this evaluation criterion was to assess if the model was designed in such a way that it adequately addresses technical, non-technical, practice-related, and theory-related security issues.

The outcome of the analysis of the collected data shows that 80.0% (summation of 71.1% and 8.9%) of the respondents were satisfied with the technical security issues accommodated in the model as shown in Fig. 9. It was also observed that 75.6% (summation of 66.7% and 8.9%) of the respondents were satisfied with the non-technical security issues accommodated in the model as shown in Fig. 10. The results also show that 75.6% (summation of 68.9% and 6.7%) of the respondents percent of the respondents were satisfied with the practice-related security issues accommodated in the model. Finally, it was observed that 73.4 (summation of 66.7% and 6.7%) of the respondents were satisfied with the theory-related security issues accommodated in the model as shown in Fig. 11. The results imply that the model designs in the proposed eGMM has considered all security related aspects to achieve a holistic secure model. Information security is a process; accordingly there is no equipment or tool that can replace the process. The reality is that no technical solution alone can make e-Government services more secure. This means the proposed eGMM is also open for improvement.

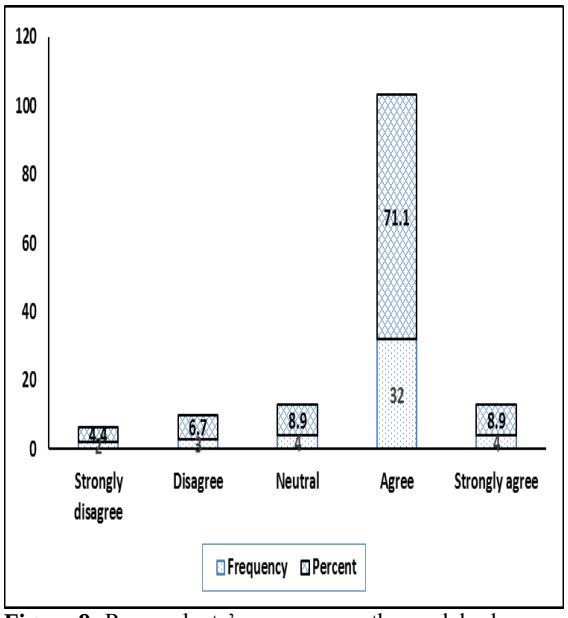

Figure 9: Respondents' responses on the model relevance to the technical security issues.

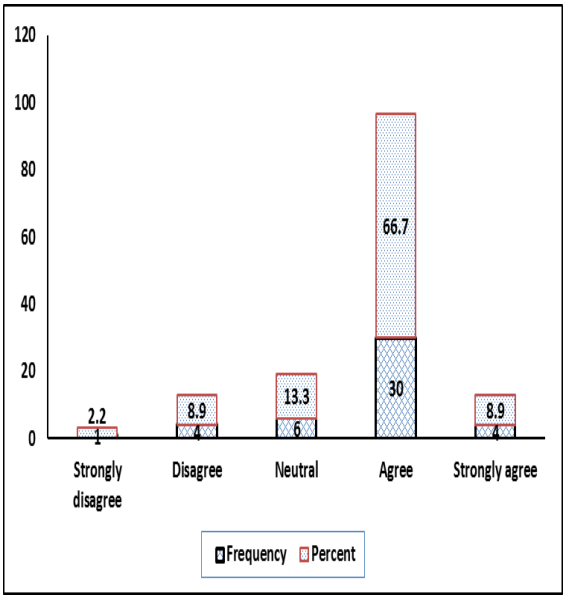

Figure 10: Respondents' responses on the model relevance to the non-technical security issues.

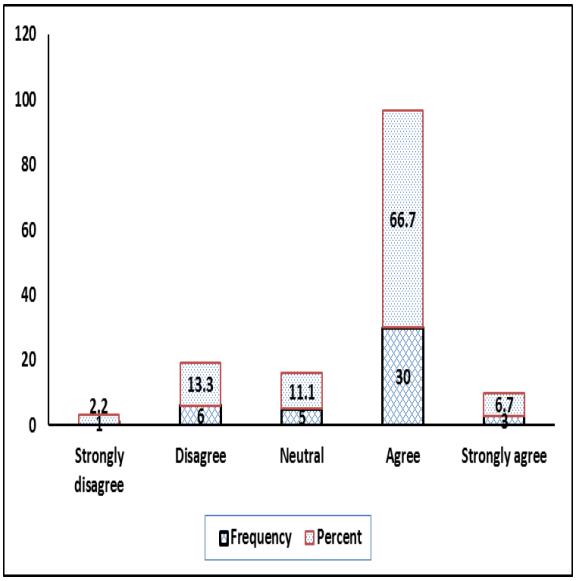

Figure 11: Respondents' responses on the model relevance to the theory-related security issues.

4.1.7 Compliance with Legal Aspects

Compliance means conforming to a rule, such as a specification, policy, standard or law. Security controls whether are technical or non-technical should be backed by policies, regulation, rules or laws. Unfortunately, information security policies and regulations if available in public organizations, they are not followed and most of them are outdated. The aim of this evaluation criterion was to assess if the model was designed in such a way that its implementation is supported by the country's Acts, laws and regulations.

The outcome of the analysis of the collected data shows that 84.4% (summation of 73.3% and 11.1%) of the respondents were not satisfied with the

support provided by the country's Acts, laws and regulations as shown in Fig. 12. The result confirms the fact that Tanzania lacks cyber laws that govern the protection of the online transactions. In general, security policies are applied to describe how organization plans to protect its ICTs assets. These plans should be supported by the country's laws in case any of the organization member or citizen commits a cyber crime.

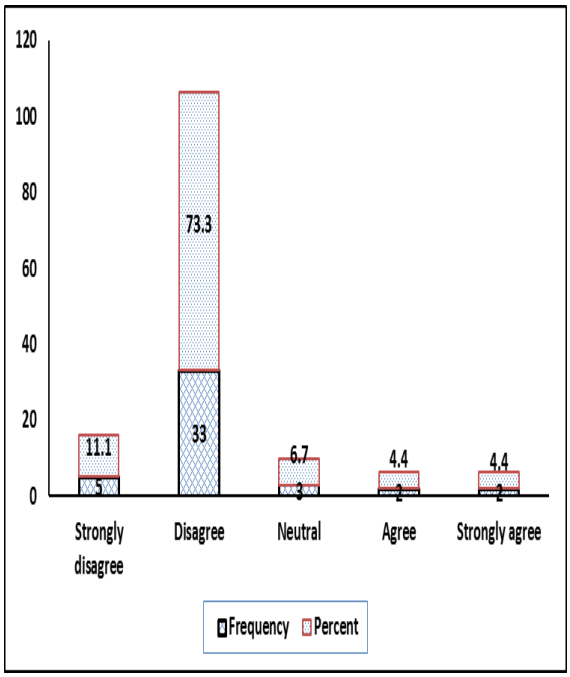

Figure 12: Respondents' responses on the support of legal aspects to the implementation of the model

5. Recommendations

Based on the findings presented in this paper, we recommend the following activities to be done in order to improve both the model and security of e-Government services in the country:

1. Noting that, the presented results show that approximately 33 percent (one third) of the respondents expressed observation that the implementation of the proposed model in public organizations reduces the accessibility and usability of the e-Government services. For this reason therefore, we recommend that, the model be reviewed to provide a balance between achieving organizations' information security and accessibility or usability of e-Government services.
2. Noting that, the results show that 40 percent of the respondents were not satisfied with organizations' ICTs infrastructure to accommodate the model. We therefore recommend to target public organizations to improve their ICTs infrastructure in order to be able to use well the model for better security of e-Government services.
3. It was observed that approximately 47 percent of the respondents were not satisfied with organizations' operational environments to accommodate the model. We recommend organizations to improve the condition of their operational environment. This improvement should also include the provision of an adequate budget to the organizations' ICTs departments, and to support security awareness programs and training.
4. We recommend organizations to make more efforts in implementing both technical and non-technical security measures in order to protect e-Government services and gain citizens' trust towards e-Government services.
5. Currently, Tanzania does not have specific legislations dealing with cyber security. There are no specific laws that govern and protect electronic transactions. For example illegal intrusion into a computer system cannot be prosecuted by the current legislations. Therefore, we recommend the government to hasten the enactment process of cyber laws to deal with data protection, cybercrime and electronic transactions, and e-Government services protection.

6. Conclusions

In this paper, evaluation of a holistic secured e-Government Maturity Model for protecting e-Government services in Tanzania is reported. A theoretical evaluation approach has been followed to test and validate the model. Specific evaluation criteria were selected and used to test and validate the model. The selected criteria include the following: simplicity, reliability, accessibility and usability, dynamics and flexibility, applicability, coverage and completeness, and compliance with legal aspects. Primary data were collected through questionnaires. The data were then processed and analyzed using the SPSS software. The overall evaluation result shows that the model designs meet all required specifications to successfully secure e-Government services, and the model is widely accepted by majority of the respondents at different organizational levels (strategic, tactical, and operational). Majority of the respondents expect that the model would enhance security by mitigating the current and future information security risks and threats posed to e-Government services. However, more efforts and time are needed to secure e-Government services properly. Further research work is recommended to test and validate the proposed model practically within the earlier studied organizations.

References

[1] Tanzania e-Government Strategy, *Government document,* accessed on 10 February, 2013 from the website www.utumishi.go.tz

[2] M. Tan, *et al.*, "An Investigation of e-Government Services in China," *The Electronic Journal of Information Systems in Developing Countries,* vol. 57, pp. 1-20, 2013.

[3] Ø. Sæbø, "E-government in Tanzania: Current Status and Future Challenges," in the Preceedings of *11th International Federation for Information Processing (IFIP) International Conference, e-Government,* (Edited by Springer Berlin Heidelberg), 3-6 September 2012, Kristiansand, Norway, 198-209.

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

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

[6] J. Yonazi, *et al.*, "Exploring Issues Underlying Citizen Adoption of eGovernment Initiatives in Developing Countries: The Case of Tanzania," *Electronic Journal of e-Government,* vol. 8, pp. 176-188, 2010.

[7] M. Wimmer and B. von Bredow, "E-government: Aspects of security on different layers," in the Preceedings of the *12th International Workshop on Database and Expert Systems Applications*, 2001, pp. 350-355.

[8] M. Dewa and Z. O. Yonah, "A Secure Maturity Model for Protecting e-Government Services: A Case of Tanzania," *Advances in Computer Science: an International Journal,* vol. 3, pp. 98-106, 2014.

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

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

[11] 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.

[12] 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.

[13] D. M. West, "E-Government and the Transformation of Service Delivery and Citizen Attitudes," *Public administration review,* vol. 64, pp. 15-27, 2004.

[14] K. Layne and J. Lee, "Developing fully functional E-government: A four stage model," *Government Information Quarterly,* vol. 18, pp. 122-136, 2001.

[15] J. S. Hiller and F. Belanger, "Privacy strategies for electronic government," *E-government,* vol. 2001, p. 173, 2001.

[16] K. Siau and Y. Long, "Synthesizing e-government stage models–a meta-synthesis based on meta-ethnography approach," *Industrial Management & Data Systems,* vol. 105, pp. 443-458, 2005.

[17] G. Karokola and L. Yngström, "Discussing E-Government Maturity Models for the Developing World-Security View," *in the Preceedings of the Information Security South Africa, 2009,* pp. 81-98.

[18] V. Venkatesh and H. Bala, "Technology acceptance model 3 and a research agenda on interventions," *Decision sciences,* vol. 39, pp. 273-315, 2008.

[19] G. Karokola, *et al.*, "Evaluating a Framework for Securing E-Government Services-A Case of Tanzania," *in the Preceedings of the 46th Hawaii International Conference on System Sciences (HICSS), 2013,* pp. 1792-1801.

[20] E. G. Guba, "Criteria for assessing the trustworthiness of naturalistic inquiries," *Educational Communication Technology Journal,* vol. 29, pp. 75-91, 1981.

[21] L. Krefting, "Rigor in qualitative research: The assessment of trustworthiness," *American journal of occupational therapy,* vol. 45, pp. 214-222, 1991.

[22] B. Hafiz and J. A. N. Shaari, "Confirmatory Factor Analysis (CFA) of First Order Factor Measurement Model-ICT Empowerment in Nigeria," *International Journal of Business Management and Administration,* vol. 2, pp. 81-88, 2013.

Authors Biographies

Mohamed D. Waziri is a doctoral student at the Nelson Mandela African Institution of Science and Technology. He holds a M.Sc. 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 MIET, MIEEE – holds a B.Sc. degree (with Hons – 1985) in Electrical Engineering from University of Dar es Salaam – Tanzania: and M.Sc. (1986) 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).