DISCUSSING E-GOVERNMENT MATURITY MODELS

FOR DEVELOPING WORLD – SECURITY VIEW

Geoffrey Karokola[1] and Louise Yngström[2]

Department of Computer and System Sciences
Stockholm University/Royal Institute of Technology
Forum 100, SE-164 40 Kista, Sweden
Tel: +46 (0)8 16 1697, Fax: +46 (0)8 703 90 25
E-mails: {karokola[1], louise[2]}@dsv.su.se

ABSTRACT

The development of Information and Communication Technology (ICT) systems towards materialization into e-Government applications is expected to tremendously change the ways governments deliver their core business services to citizens and how citizens can interact with their governments. There are also high expectations that these changes will play major roles in the socio-economic developments. For these reasons there are several so called maturity models being developed to guide and benchmark e-government developments in developing countries. These models describe various stages, three to six, referring to technological complexity. However, we do not see explicitly that security is addressed as a specific issue at the various stages, nor do we see how cultural, legal, economical and managerial security related issues are incorporated.

Being part of the ongoing research in the area, the paper attempts to critically investigate, evaluate and analyze eleven existing e-government maturity models, and discuss the findings in the light of research findings from four government institutions located in the Sub-Saharan Africa.

KEY WORDS

e-Government, Maturity Model, ICT/IT Security, Technical, Non-technical, Developing Countries

DISCUSSING E-GOVERNMENT MATURITY MODELS FOR DEVELOPING WORLD – SECURITY VIEW

1 INTRODUCTION

Over recent years there has been an enormous development of Information and Communication Technology (ICT) systems towards e-government applications. Similarly, governments have also considered e-government as a powerful tool that can change ways they conduct and deliver their core business services to citizens and how citizens can interact with their governments. Also, there are higher expectations that adoption and use of e-government application could improve efficiency, effectiveness, accountability, and transparency of government service delivery, and at the same time improve active participation of citizen in public decision-making processes – hence realization of socio-economic development [2, 9, 11, 13, 22]. Various studies [2, 13] show that while most of the developed countries are in the final stages of e-government development - developing countries are still in the early stages of e-government development. This gap is heavily influenced by the existence of technological and non-technological related issues including lack of proper ICT infrastructures, readiness, awareness, economical, and political will.

However, to guide and benchmark e-government development, researchers and academia proposed different types of e-government development models, so called maturity models. These models outline various stages for e-government development. For instance West [23] proposed a three stage model, Layne & Lee [11] four stage models, while Deloitte & Touche [21] proposed a six stage model. Nevertheless, as governments' moves towards adoption of e-government applications – security has become a critical factor influencing its development at all stages of e-government development [1, 5, 9, 10, 11, 12, 20]. This creates need for holistic approach to explicitly addressing and incorporating security as a specific issue at the various stages of the development models [1, 19]. These include technical and non-technical security related issues such as cultural, legal, economical and managerial. According to the World Bank [25] e-government is defined as "the government owned or

operated systems of information and communication technologies that transform relations with citizens, the private sector and/or other government agencies so as to promote citizens' empowerment, improve service delivery, strengthen accountability, increase transparency, and improve government efficiency". However, the concept of e-government has no clear definition; because it is defined by objective of activities rather than by the technology – therefore it requires broad definition and wider understanding for a government to be able to implement it successful [2, 6, 13].

> *This paper should not be read as a critique to the e-government maturity models to be evaluated but lather should be read as a catalyst towards enhancing security to these models.*

The paper attempts to critically investigate, evaluate and analyze eleven existing e-government maturity models, and discusses the findings in the light of research findings from four government institutions located in Tanzania – one of the countries located in the Sub-Saharan Africa. The rest of the paper is organized as follows: chapter two outlines the research process and methodology used, the third chapter presents an overview of e-government development maturity models and specific security related issues. Chapter four presents and discusses the research findings, and lastly conclusion and recommendation is given in chapter five.

2 RESEARCH PROCESS

The research methodology used in this study is based on qualitative and quantitative methods. The process was divided it into two phases. Phase one was to conduct a desk review in the area of e-government, e-government development models, and security documentations. The second phase employs a research survey where questionnaires and in-depth interviews were conducted. This phase was later complemented with documentation reviews from the studied settings such as e-government strategies, and ICT security policies. Six Tanzanian government institutions including ministries, departments and agencies were earmarked and contacted.

The Contacted groups were at the strategic level (Directors and decision makers), tactical level (Managers) and operational level (Technical staff and users). All interviewees were in one way or other

responsible for delivery of e-government services to the public. Interviews were conducted between mid to late April 2009. In the analysis process data triangulation method was used to facilitate validation and verification of research findings of primary data with secondary information. However for the purpose of this paper – findings from four institutions (three ministries and one agency) are used.

3 AN OVERVIEW OF E-GOVERNMENT DEVELOPMENT MODELS AND SECURITY ISSUES

E-Government developments are influenced by so called e-government development models [9, 11, 14]. These models are specifically designed to guide the implementation and development of e-government applications in a stage-wise manner – from immature (one-way communication) to the mature (digital democracy) stage. The advantage of having a stage-wise approach is to offer governments abilities to measure the progress and also to generate momentum that could subsequently be maintained [9].

Therefore, in this section, based on the ISO 17799 security standards ten principles *(i.e Business Continuity Planning, System Access Control; System Development and Maintenance; Physical and Environmental Security; Compliance; Personnel Security; Security Organization; Computer & Network Management; Asset Classification and Control; and Security Policy)*[19], we critically investigate, evaluate, and present the short-listed widely known eleven (11) e-government maturity models, namely: Asia Pacific, Chandler and Emmanuel, Deloitte and Touche, Gartner, Hiller and Blanger, Moon, Howard, Layne and Lee, UN and DPEPA, Darral West, and World Bank. In the process, we give a synopsis of each model. Finally, the models' summary is given.

3.1 Layne and Lee's four stage model

Layne and Lee (2001) regard e-government as an evolutionary phenomenon based on the authors' observation and experience in the area. They propose four stages of e-government development. Basically, the model is based on technical, organizational, and managerial dimensions. The full description of the models' four stages is given: *Cataloging* – this stage is meant for delivery of some basic information through website. In most cases the websites are considered to be static; it enables citizens as users to access on-line presentation and downloadable forms.

Transactional - is a stage that propagates the former, whereby it enables citizens to do on-line transactions (two-ways communication). *Vertical integration* – this stage focuses on the automation of more government workflows and also transformation of government services; it includes integrating government functions at different levels such as these of local and states governments. And finally *Horizontal integration* – this focuses on systems integration between different levels and functions for providing users with a unified and seamless service.

Synopsis–1: In spite of the model being focused on functionality which is grounded on combination of technical, organizational and managerial feasibility – it does not consider the potential benefit of political changes. In addition, the model design has fairly considers technical security related issues in particular at the transactional; and gave very low consideration non-technical ones, such as cultural and ethical, legal and regulatory, and economical [11].

3.2 Chandler and Emanuel's four stage model

Chandler and Emanuel (2002) developed a four stage model. The narrations of the stages are: *Information* – this is a preliminary stage, were most of government services delivery is available on-line. Citizen can access government information over a website (static) – this is a one-way communication between government and citizen. *Interaction* – this is the advanced stage of the former; simple interaction between citizens and governments are enhanced; various website features and functionality are available including search, and emails; at this stage the communication is two ways. *Transaction* – refers to services that enable transactions of values between citizen and government; citizen can pay taxes, submit forms on-line. And *Integration* – this is the final stage where vertical and horizontal integration of services across government and agencies occurs. Citizen can access information on-line from one service centre.

Synopsis–2: Chandler and Emanuel [6] model focuses partly on citizen-centric and functionality. Also it gave fairly little technical security consideration at the transaction stage. However, the model ignores not only the specific non-technical security related issues but also the potential benefits of political changes [6].

3.3 Gartner's four stage model

Gartner group (2000) developed an e-government maturity model with four stages. These are: *Web presence* – this is the initial stage where government provides website (static) with basic information that the citizen can access. *Interaction* – government provides a website with various capabilities such as search engines, documents downloading and emails; this is used as a tool for interaction between parties involved (government, agencies and citizen). *Transaction* – citizen (users) can conduct complete on-line transaction including buying and selling activities. And *Transformation* – this is the last phase, where all government operational processes are integrated, unified and personalized.

Synopsis–3: In general, the model focuses on citizen-centric and partly functionality which is grounded on technology, organizational and managerial feasibility. In addition, the model partly considers technical security at its transaction stage while on the other hand the model fairly consider specific security (non-technical) related issues or the potential benefit of political changes [22].

3.4 United Nation's five stage model

United Nation (2001) proposed a five stage model with a focuses on web-based public service delivery. Description of the model stages are: *Emerging web presence* – this is the initial stage were government websites provides mostly basic and limited static information with less options for citizens. *Enhanced web presence* – this is the second stage were there are improvement of government websites in-terms of providing dynamic, specialized and regularly updated information. Among the website features include search facilities, on-line help, and site maps. And *Interactive web presence* – users and service providers are connected to government portals (websites); Interaction became more sophisticated than in the former stage. Services such as search facilities and accessibility of various forms are enhanced. Others are *Transactional web presenc*e – this stage allows two-way interactions between the citizen and the government; users can conduct complete on-line transaction including buying and selling activities. And *Seamless/Networked web presence* – this is the most sophisticated level of e-government service delivery; all services and functions across all government levels are integrated; citizens can access any kind of services from a central location at any given time.

Synopsis–4: The model is centered to web-based and functionality. The model development is based on technology and managerial aspects. In addition, the model fairly considers specific issues related to technical security at its transactional stage. Furthermore, the model does not consider the potential benefit of political changes [17].

3.5 West's four stage model

Darral West (2000) proposed a four stage model of e-government development. The stages and description of the model are: *Billboard* – this is the stage were websites (static) are used for information display. Various types of information can be posted on the website including reports and publication; this way citizen (visitor) could easily access and consume the displayed information. *Partial service delivery* – at this stage government starts to set services on-line for citizen to access; at this level the on-line website has more capabilities and functionalities include sorting and searching of information. *Full integrated service delivery* – one stop centre is created (government portal) with full integrated online services; citizen can easily access government and agencies information from one service centre. And *Interactive democracy with public outreach and accountability* – according to West [23] this is the final stage of e-government development. Government website develops into a system wide political transformation with executable and integrated on-line services. Citizens can easily access government information and also customize the on-line government information service delivery system(s).

Synopsis–5: Darral West [23] model focuses on functionality and citizen-centric. In addition, the model gave fairly little consideration security (technical and non-technical) as a specific issue. However, it considers the potential benefit of political changes at its highest stage [23].

3.6 Hiller and Blanger's five stage model

Hiller and Blanger (2001) proposed a model with five stages, namely: *Information dissemination* – this is the initial stage of the government to disseminate information to the citizen by posting it on the website (static), the communication is one-way. *Two-way communication* – at this stage government uses enhanced websites with various capabilities such as emails and downloadable forms to interact with citizen (users). And *Service and financial transaction* – this is advanced stage than the

previous one, government offers online services including financial transaction to citizen (users). This phase requires more sophisticated technology. Others are *Vertical and horizontal integration* – the government integrates various systems at different levels vertically and horizontally. Finally is Political participation – government involves citizen in political participation activities including online voting and forums.

Synopsis–6: We see that the model focuses on functionality and it considers the potential benefit of political changes. However, the model gave attention to security at its financial transaction stage – and ignores other specific security related issues including these of non-technical [24].

3.7 Moon's five stage model

Moon (2002) developed a five stage model. The stages are One way communication, Two-way communication, Transformation, Vertical and horizontal integration, and Political participation. However, if we compare the two models Moon (2002) and Hiller and Blanger (2001 there are large similarities in particular from stage two to five, which were already described above, under 3.6. For that reason, we only give the description of stage one of the model (*One way communication*), which is considered as the preliminary stage of e-government developments where government disseminates information to the citizen by posting on the website, and citizens can access online.

Synopsis–7: As the model stages are similar to Hiller and Blanger, the model focuses on functionality and also considers the potential benefit of political changes. However, the model gave attention to security at its financial transaction stage – and ignores other specific security related issues including these of non-technical [24].

3.8 Asia Pacific's six stage model

Asia Pacific (2004) region based on their experience of e-government development – proposed a six stage model. The model stages and their description are: *Setting up an email system and internal network* – this is the initial stage where most of government systems focuses on internal processes that supports basic administrative functions such as e-mails and payroll. *Enabling inter-organizational and public access to information* – this stage involves government into developing systems that will help in

managing its workflow from paper based to electronic format (inter-organizational); Also at this stage citizen (public) are able to access government information through the use of internet. *Allowing 2-way communication* – government and the citizen (public) use ICT as enabler for communication. For instance telephone, fax numbers or email addresses are posted on a website, this encourage public to send messages to the government and receive response. And *Allowing exchange of value* – at this level, ICT is used to support development of more flexible and convenient ways for citizens to conduct business with the government. Citizens have the opportunity to utilize the available on-line government services including tax assessment, visa application and license renewals. Others are: *Digital democracy* – citizen use ICT as an enabler that can potentially support participatory and democratic processes. For instance use of on-line applications that empowers citizen and civil organization to vote. The final stage is *Joined-up government* - this is the final stage were there is both vertical and horizontal integration of service delivery, a web-portal integrates information and services from various government bodies/agencies. This way citizen and other stakeholders get seamless services without needing to know what government, department or agency is responsible.

Synopsis–8: This model focuses on citizen-centric and functionality. Also it considers the potential benefit of political changes. However, with the exception of one stage (Allowing of exchange of value) - security related issues (technical and non-technical) are not explicitly addressed as specific issues [3].

3.9 Deloitte and Touche's six stage model

Deloitte and Touch (2001) presents a six stage model based on the view that e-government objectives should serve citizens building a long term relationship. The full description of each of the stage is as follows: *Information publishing* – at this stage government sets up websites (static) for providing information to citizen /users. At this stage the communication is on-way; *Official-two way transaction* – this is an advanced stage of the former were information are transacted and exchanged between citizen as users and government/agencies as service providers; *Multipurpose portal* – government uses a single portal as a single point of entry to effectively provide services to its departments,

agencies and to citizen; *Portal personalization* – this stage provides citizen/users with the opportunity to customize the portal based on their desired features; *Clustering of common services* – all government services and operational processes are clustered along common lines so as to provide unified and seamless services to citizen; and the last stage is *Full integration and enterprise transaction* – government changes its structure and provide more sophisticated, integrated and personalized services to citizen.

Synopsis–9: Like other models, the model focus is grounded on citizen-centric. However, apart from ignoring the potential benefit of political changes, it also gave fairly little attention to specific related security issues - technical and non-technical [21].

3.10 Howard's three stage model

Howard (2001) developed a three stage model. The stages of the model are: *Publishing* – this is the initial stage of e-government development were Information about activities of government is available online. *Interacting* – this is the advanced stage of the former, citizens have the ability to do simple interactions with governments; available services at this level include sending e-mail, chat rooms, and/or filling and sending forms. And finally *Transacting* – based on the model design this is the highest stage of e-government development. The stage enables citizens to conduct transactions over the Internet, including purchasing /payment of licenses and permits.

Synopsis–10: The model focuses on functionality and at the same time on citizen-centric. Unfortunately, the model does not consider the potential benefit of political changes nor the specific security related issues in particular non-technical [8].

3.11 Word Bank's three stage model

Word Bank (2003) proposed a three stage model. These are: *Publishing* – this is the first stage, government disseminates information to citizen through website; all important information is posted on the website. *Interactivity* – at this phase government interacts with citizen. Websites are enhanced with interactive capabilities such as feedback forms and email. And lastly is *Completing transaction* – this is the final stage of e-government development; citizen/users can use the opportunity of the

available technically enhanced website to conduct complete and secure transactions on-line.

Synopsis–11: The model focus is on both functionality and citizen-centric. Also the model development does not consider the potential benefit of political changes. Security is addressed only at its final stage, completing transaction. Therefore the model lacks most security related issues [25].

4 FINDINGS AND DISCUSSION

4.1 Findings

This section presents our research findings regarding the specific related security issues and challenges.

4.1.1 Security Issues and Challenges for the Evaluated e-Government Development Models

Given the criticality of e-government applications in supporting institution/organizational core business processes, it is essential that e-government applications be implemented and operated in a secure way [5, 9, 12]. Therefore, it is imperative for e-government maturity models to include security layer that clearly defined the specific security requirements (technical and non-technical) at each of the e-government development stages. Being guided by the ISO 17799 standards ten principles [18] and the systemic holistic approach [19], we therefore highlight some specific security issues and challenges transpired in the course of this study. It is very unfortunately that from the evaluation of the eleven models presented above – very few models design had considered security as a specific issue. These models considered security mostly at the transaction stage [9]. It is imperative for e-government development models to include security layer at each of the stages. The security layers would comprise of specific technical and non-technical security related issues based on the model's stage requirement.

Stage one referred by all model as the beginning of e-government development/ implementation. Hence it requires much of security awareness and training programmes. Awareness at this level will create ownership and trust not only to government, and stakeholders but also to citizens [9, 11]. Also, at this stage the security layer should include

security issues related to: development and maintenance of e-government systems application – this will ensures security becomes part of systems operation, protection of confidentiality, integrity and authenticity of information, and also maintaining security of application system software and data; Access Control – that control access to information, prevent unauthorized access to systems, and networked services. Also Compliance matrix to security standards and personal security should be considered as part of the security layer. Furthermore the security layer should integrate non-technical security related issues including managerial and operations – at different levels; legal laws and regulations (i.e cyber laws); cultural and ethical; and economical issues – government support [4, 5, 9, 18].

Therefore, as the e-government model stages grows in terms of technological sophistication and complexity (i.e from one-way to two-way communication and so on) – the security layer needs to be updated to match with the security requirement at that particular stage of the e-government development model.

4.1.2 Findings from the Research Survey

The research findings from the four institutions revealed that Tanzania has got a national level e-government implementation strategy of which is propagated to the rest of the ministries, departments and agencies (MDA's). As of today Tanzania has a total of twenty Ministries, fifteen departments, and more than seventeen agencies. In the analysis, we code the named institutions in the following order: *Ministry of Lands, Housing and Human Settlement Development (MLHHSD) referred as W; Prime Minister's Office – Regional Administrative and Local Governments (PMO-RALG) as X; President's Office – Public Service Management (PO-PSM) as Y; and The Tanzania Ports Authority (TPA) referred as Z.*

- *The state of e-government development* (e-government maturity level) –choosing Gartner's e-government development model as our reference, the research findings from four institutions revealed that all three ministries (W, X, Y) were still at stage two (interaction stage) of e-government development, while the named agency (Z) is in the process of moving towards stage three (transactional stage). Agency Z is now heavily enhancing its ICT infrastructure and resources to meet stage three functional and operational requirements.

- *Necessity of security being part of e-government development models* – When asked if there is a need for having specific security (technical and non-technical) related issues integrated into stages of e-government development models – the result was that more than 95% of the respondent ranked it higher (fully agree). Likewise, when asked the importance of having benchmarking standards that clearly define the security requirements at each of the e-government development stage – more than 90% of interviewee ranked it higher (fully agree).
- *Ranking of requirements for security components and related issues* – when asked to rank the given security components (technical and non-technical issues) – the result was as shown in the table 1 below followed by its pictorial presentation in figure 1:

Table 1: Survey results for how important it is deemed that technical and non-technical security requirements are addressed.

Description of technical and Non-technical related issues	**Score ranges from 0 – 100 % , 100% being Fully Agree**				
	W	**X**	**Y**	**Z**	**Average Score**
Technical related security issues					
• Use of strong Access Control mechanisms	80	100	100	100	95
• Encryption of classified critical information	80	60	80	60	70
• Network security mechanism i.e use of Firewalls, IDPS, VPN	80	80	100	100	90
• Backups (BCP and Disaster recovery)	80	80	80	80	80
• Use of anti-virus and malicious codes software's	100	100	100	100	100
Non-technical related security issues					
• Managerial and operational	80	80	80	100	85
• Economical	80	80	100	80	85
• Legal and Regulatory	80	80	60	80	60.75
• Cultural and ethical	60	80	60	60	65

• Citizens/public trust	80	80	80	100	85
• Awareness	100	100	100	100	100

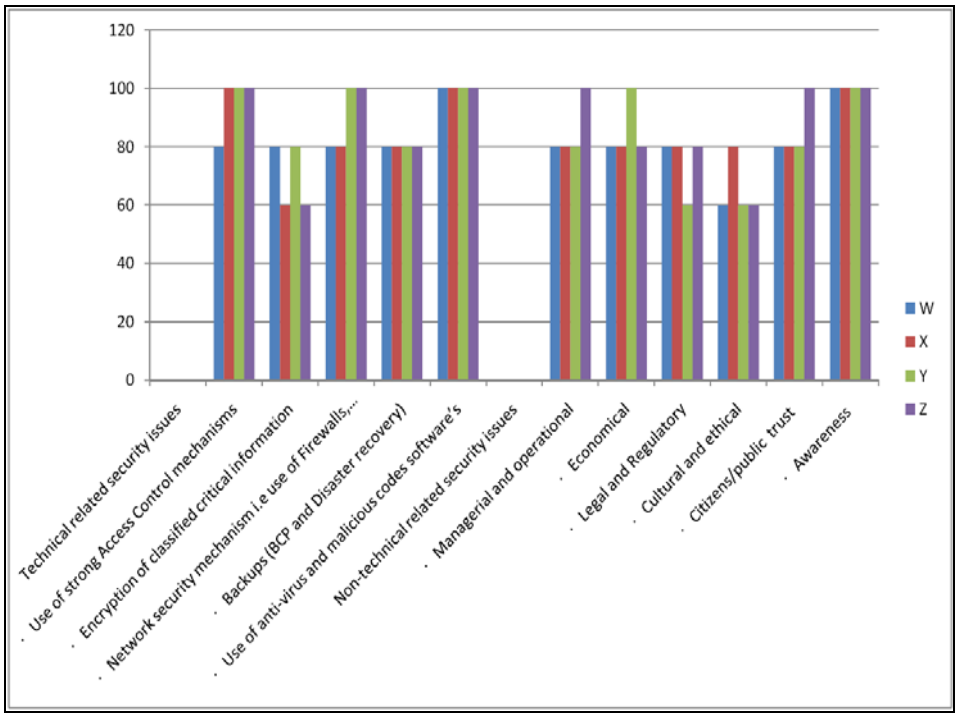

Figure 1: Security related issues (technical and non-technical) – survey results showing level of importance to be addressed

In addition, other issues related to security facets such as confidentiality of data supplied, integrity, non-repudiation, identification of who did what, services availability mechanisms and implementation were also cited as major obstacles to current e-government development in the area [15, 16].

4.2 Discussion

The findings analysis presented above shows that more than 40% of the eleven evaluated e-government development models did not consider security as a specific issue related to both technical and non-technical requirements. The rest of the models like Layne and Lee [11] slightly

presented technical security related issues in particular at the transactional stage. However, the research survey conducted in four institutions, presented above, shows that for effective and efficient e-government service delivery – security related issues and challenges needs to be explicitly addressed [2, 16]. Developing a security layer that integrates technical and non-technical security related issues should be the way forward. The security layer needs to reflect the pertinent requirements of each stage of e-government development model. The security layer requirements at stage one is given in section 4.1.1. Thus, as the e-government model stages grow in terms of technological complexity (i.e from one-way to two-ways communication and so on) – it is important to have security layers at higher stages upgraded to match with the security requirements at that particular stage. Moreover, the challenge remains; currently we don't have a common e-government maturity model that reflects standard stages, i.e the same stage is now defined with different names and focus.

5 CONCLUSION AND RECOMMENDATION

The paper critically investigates, evaluates, analyzed and presented findings from the eleven e-government development models. The findings were later complemented with the research findings from four government institutions located in Tanzania – one of the developing countries located in the sub-Saharan Africa. In the course of the analysis ISO 17799 ten principles were used to guide the analysis and discussion. Various security issues and challenges related to technical and non-technical requirements - were presented and discussed in a wider dimension with the main focus on the e-government development model stages. Finally, the security layer was proposed. However, in the course of this process, the following are worth mentioning:

- The evaluated e-government development models focuses either on functionality, or citizen-centric or both.
- The naming of the stages, particularly stage one and two, includes many buzzwords with slightly different focus, even though the main foci were conceptually more or less the same.
- Security requirements (technical and non-technical) related issues are not the main foci for the design/ development of the model.

- Few models consider lower level technical security requirements; in particular at the transaction stage.
- Some of the models did consider at all neither the transactional stage nor the potential benefit of digital democratic stage.
- The security layer that comprehensively covers critical specific technical and non-technical security related requirements at all of the model stages (based on the selected/new model) needs to be developed.

Therefore, in light of our analyses and interviews, we have identified that it is demanded important for e-government development models to include a security layer at each of the model's stages. The security layers should comprise of specific technical and non-technical security related requirements based on the model's stage requirements, and possibly, founded on the ISO 17799/27000 standard principles. Though there are a number of studies focusing on reviewing the stages of existing e-government development models – development process of any new model should consider the inclusion of a security layer as a specific issue at each of the model stages.

6 REFERENCES

[1] B. Bredow, M. Wimmer, (2002) A Holistic Approach for Providing Security Solution in e-Government; *Proceedings of the 35th Hawaii International Conference on System Sciences; [Also available at http://www. csdl.computer.org/comp/proceedings/hics s/2002/1435/05/14350128b.pdf., Last accessed on 15th of April, 2009]*

[2] Basu, Subhajit (2004) "e-Government and Developing Countries: An Overview"; International review of law computers & technology, Volume 18, No. 1, Pages 109-132

[3] Clay G. Wescott "e-Government in the Asia-Pacific Region; *[Also available at http://www.adb.org/documents/papers/e_government/egovernment.pdf; last accessed on 05th of April, 2009]*

[4] Bishop, Matt (2006), "Computer Security – Arts and Science" *Addison-Wesley, ISBN: 978-0-201-44099-7*

[5] C. Lambrinoudakis, S. Gritzalis, F. Dridi, G. Pernul, "Security requirements for e-Government services: a methodological approach for developing a

common PKI-based security Policy" Elsevier. Computer Communication 26 (2003) 1873-1883

[6] Chandler, S., and Emanuels, S.(2002), 'Transformation Not Automation', Proceedings of 2nd European Conference on EGovernment, St Catherine's College Oxford, UK, 2002, 91-102

[7] Ebrahim, Z., Irani, Z., and Al Shawi, S., 'E-Government Adoption: Analysis of Adoption staged Models' *Proceedings of the 3rd European Conference on e-Government; Jul 3-4, 2003; Trinity College Dublin, Ireland*

[8] Howard, M., 'e-Government Across the Globe: How Will 'e' Change Government?', [Available at http://www.gfoa.org/services/gfr/archives/2001/08/gfr0801.pdf; Last accessed on 26th of March, 2009]

[9] Irani, Z Al-Sebie M, Elliman T: "Transaction stage of e-Government system: identification of its location & importance" *Proceedings of the 39th Hawaii International Conference on System Sciences*

[10] J. Gil-Garcia, T. Pardo, e-Government Success Factors: Mapping Practical Tools to Theoretical Foundations; *Government Information Quarterly, 2005 - Elsevier*

[11] Layne, K, & Lee, L. (2001). Developing fully functional e-government: A four stage models, Government information Quarterly 8, 122-136.;

[12] M. Just, D. Rosmarin Meeting the challenges of Canada's Secure Delivery of e-Government Services.[Available at http://middleware.internet2.edu/pki05/proceedings/just-canada_egov.pdf *[Accessed on February 15th, 2009]*

[13] Ndou, Valentina, e-Government for Developing Countries: Opportunities and Challenges; *[Available at http://publications.ksu.edu.sa/IT%20Papers/eGov/unpan018634.pdf; Last accessed 10th of March, 2009]*

[14] O. Signore, F. Chesi, M. Pallotti (2005), e-Government: challenges and Opportunities *[Available at http://www.w3c.it/papers/cmg2005Italy.pdf; Last accessed on 23rd of February, 2009*]

[15] TZ-eGov, Tanzania e-Government Strategy (2008)

[16] TZ-ICT, Tanzania National ICT Policy, March 2003. *[Available at http://www.tanzania.go.tz/*]

[17] UN, "Benchmarking E-government: A Global Perspective ", Assessing the Progress of the UN Member States, Available at: http://www.unpan.org/egovernment.asp

[18] ISO 17799, *[available at http://www.17799central.com/, Last accessed on 20th of April, 2009]*

[19] Yngström, Louise (1996) "A Systemic-Holistic Approach to Academic Programmes in IT Security" PhD Thesis, Department of Computer and Systems Sciences, University of Stockholm and the Royal Institute of Technology, Stockholm, ISBN: 91-7153-521-7

[20] Z. Zhou, C. Hu (2008), "Study on the e-Government Security Risk Management". IJCSNM International Journal of Computer Science and Network security, VOL 8 No. 5; [Also available at http://paper.ijcsns.org/07_book/200805/20080531.pdf, Last accessed on 25th of March, 2009]

[21] Deloitte and Touche (2001), "The citizen as customer" CMA management VOL 74 No. 10, p.58

[22] Baum C & Maio, D (2000) Gartner's Four phases of e-government model, Gartner's group

[23] D. M West (2004) "E-government and the transformation of service delivery and citizen attitudes" Vol. 64, No. 1

[24] M J Moon (2002), "The Evolution of e-Government among Municipalities: Rhetoric or Reality? *[Available at http://www.jstor.org/stable/3110357?seq=2, Accessed on 218th of April, 2009]*

[25] World Bank (2001) Issue Note: E-Government and the World Bank. November 5, and World Bank (2003) World Development Indicators, *[Available at http://www.worldbank.org/data/wdi2003/, Last accessed on 10 of January, 2009]*