International Journal of Information Science 2014, 4(1): 13-20
DOI: 10.5923/j.ijis.20140401.03

Assessment of E-Government Weak Points to Enhance Computer Network Security

Yas A. Alsultanny

College of Graduate Studies, Arabian Gulf University, Manama-Kingdom of Bahrain

Abstract This paper determines the e-government weak points to enhance the computer network security and to protect the computer network. A questionnaire of two parts was designed for assessment of e-government; the first part was for demographic information and the second part was consists of 30 statements, these statements distributed into five dimensions, the 5-points Likert scale was used to measure the degree of agreement. The data collected from 356 IT developers. The results conclude that there are some procedures from e-government's managers to secure users' data, there is an evaluation to the information technology used in the e-government network, there is an evaluation to the security level of e-government network, and there are monitoring and improvement to the vulnerability issues in the e-government networks. More attention recommended to overcoming of any possible weak points within the network.

Keywords Weak Point, Vulnerabilities, Computer Network, E-Government Security, Information Technology

1. Introduction

E-government has concentrate on the security factor in order to keep the databases of users' from any unauthorized people or users who misuse these personal information or databases. Because of the importance of the security in the e-government, there are several solutions to avoid any vulnerable issues. That can lead the unauthorized person to access the personal information of the users or the personal information of the government itself (Moen et al., 2007; Karokola and Yngström (2009). However, Saha et al. (2010) defined vulnerability issues as the capability of the system to change the impacts of the events. This means that vulnerability relates to the ability of the system to expose the risks and then change their consequences. Policy makers in the e-governments pay a lot of attention on providing the required security to their files and folders in order to avoid any vulnerability or threats on the data or information in the e-government networks, which then plays a major role in the trust that are provided from the citizens towards e-governmental applications (Syamsuddin and Hwang, 2010).

The significance of security in the e-governments applications relates to the vision of e-governments to provide citizens with applications of high level of security. Therefore, e-governments have provided several techniques to keep security at a highest level (Elssied et al., 2011). Personal information accessing in the e-governmental applications sometimes requires the fingerprint, iris, or voice recognition. The humans can form some vulnerable issues to the e-governmental system either intentionally or by mistakes. Therefore, e-governments mangers must train the computer network security employees before recruiting them in real jobs (United Nations Department of Economics and Social Affairs, 2007; Zhao et al., 2008). E-governmental protected clients' personal information, updating the system regularly to limit the malicious entity, like hackers or attackers, viruses, and unauthorized employees from reaching the sensitive data (Upadhyaya et al, 2012).

Security assessment of e-government computer network is the most important object that all the IT employees responsible for developing e-government applications with the highest level of security. The security must be the first priority for each application before publishing it to users', because the security will increase the users' trust in using applications and reducing the fraud, especially in the applications have money transfer and have the users' information. From these two points the importance of this paper was raised to assess security level from the perspective view of the IT developers who responsible for developing Kuwaiti e-government computer network and its applications to enhance computer network security. The structure of the paper is as follows, we will try to link the objective with the hypotheses that was designed to answer the questions of this paper, and then presenting the results analysis from IT developers' perspective followed by conclusion.

* Corresponding author:
alsultanny@hotmail.com (Yas A. Alsultanny)
Published online at http://journal.sapub.org/ijis

2. Motivations for This Study

The development in ICT tools has identified the concept of e-government as the government applications that are used for different transactions through Internet (Wong et al., 2011). Alfawaz et al (2008) argued that e-government concentrated on the security factor in order to keep the databases of users' from any unauthorized people or users who misuse these personal information or databases.

Vulnerability and weak points of e-government networks are very important. Thus, it is certainly worthwhile to evaluating the vulnerability and weak points of e-government from the perspective of view of IT developers.

3. Research Objective

The major objectives of this research are concerned with answering the following questions:

- Is there measurement to the web effectiveness?
- Is there measurement to the services security?
- Is there evaluation to the information technology use?
- Is there evaluating to the information technology security?
- Is there improvement for the vulnerability issue?
- Is there effect of demographic information on e-government weak points?

4. Literature of E-Government Security

E-governments are established for the benefits of citizens; they can access their needed governmental services anytime and anywhere and perform their transactions easily and rapidly. But these services facing the problems of security issue in the applications of e-governments, Therefore, E-governments must provide a security system in order to avoid any unauthorized people from accessing the E-governments applications (Elssied et al, 2011). E-governments take different procedures to avoid various vulnerabilities; For example, e-governments provide user name and password in order to log in a certain file or folder. Also, E-governments provide antivirus programs to protect the computers while downloading files or folders as well as they provide encryption and decryption tools to protect the computers from any vulnerability issues (United Nations Department of Economics and Social Affairs, 2007).

Security issues are considered as the main framework to ensure the successfulness of any e-governmental; if there is any security vulnerability, the whole system will be at risk. So, these e-governments are seeking more and more to protect and isolate their systems from any sudden danger. E-government must take into consideration the personal information have to be kept secure and private (Schwester, 2009; Upadhyaya et al. 2012).

E-government in Kuwait has offered for their citizens flexible applications where they have the ability to do their different transactions 24 hours/365 days (Kostopoulos, 2003). These applications needs security to avoid any problem faces the users (Boujarwah, 2006). AL-Shehry et al (2006), indicated in their study that the security is an important factor in the e-government applications, because it can provide the required trust to users, and this will increasing the effectiveness and efficiency of interacting the users with e-government's developers. Colesca (2009), argued that major problem facing the Kuwaiti e-government is the security problem which allows unauthorized people to access personal data.

Syamsuddin and Hwang (2010), advised to use different programs and software to solve technical problems facing e-government web applications users. Both of Scarfone and Mell (2010), indicating that the vulnerability issues can be created from the software designer himself, which means that the software designer can cheat the trust of the managers of e-governments by announcing these codes to unauthorized people.

Muthanna (2009), in his study for Bahrain e-government demonstrated that the Bahrain government data network managers should gain a full understanding of any potential risks by noticing the output of information security risk management process; where this process can assess and scan the external and internal environment of Bahrain government data network. AL-Qaisoum (2009) in his study for measuring Saudi Arabia e-government readiness, he found that the main obstacles of the e-government are the network security, legal, and IT skills in the field of computer network security.

Therefore the importance of this paper rise from the necessary of assessing the weak points of the computer network from the perspective of the IT developers, the questionnaire and the hypotheses of this paper were build with the help of the researches such as; Kurose and Ross (2005), Schneier (2005), Panda et al (2010).

5. Research Significance

E-government is one of very important applications implemented on the Internet. The users in all countries gain the usefulness of the e-government application, but on the other side the important point appear here, is how to safe users data from any attack, therefore the significant of this paper comes from the following;

- Provide an appropriate level of security to the personal information and data to the users by avoiding the vulnerability issues that might be happened through accessing unauthorized people to the databases.
- Avoid vulnerability issues that the systems of e-government are clear from any intrusion so that users can do their transactions through e-governmental applications without having any problems as well as having no fear resulted from the feeling of giving the unauthorized people an access to the system which let them steal users' personal information and data.
- Increase the users' engagements with the

e-governmental applications because, it provides enough security level to keep the users' data from any misuse.

6. Research Model and Methodology (Instrument Design and Measurements)

Table (1) shows the supported literature used in designing the factors of the research model. The research model that guides this study is depicted in Figure 1; the model examines the effect of *Web Effectiveness (WE), Services Security* (*SS*), *Information Technology Use (ITU), Information Technology Security* (*ITS*), *Vulnerability Reduction* (*VR*) *on* e-government weak points.

Table 1. Literature related determine e-government weak points

Factors determine e-government Weak Points	Supported literature
Web Effectiveness (*WE*)	Kurose and Ross (2005); White (2008)
Services Security (*SS*)	Kurose and Ross (2005); Schneier (2005); Panda et al (2010)
Information Technology Use (*ITU*)	Kurose and Ross, (2005)
Information Technology Security (*ITS*)	Hwang et al., (2004)
Vulnerability Reduction (*VR*)	Blau, (2006)

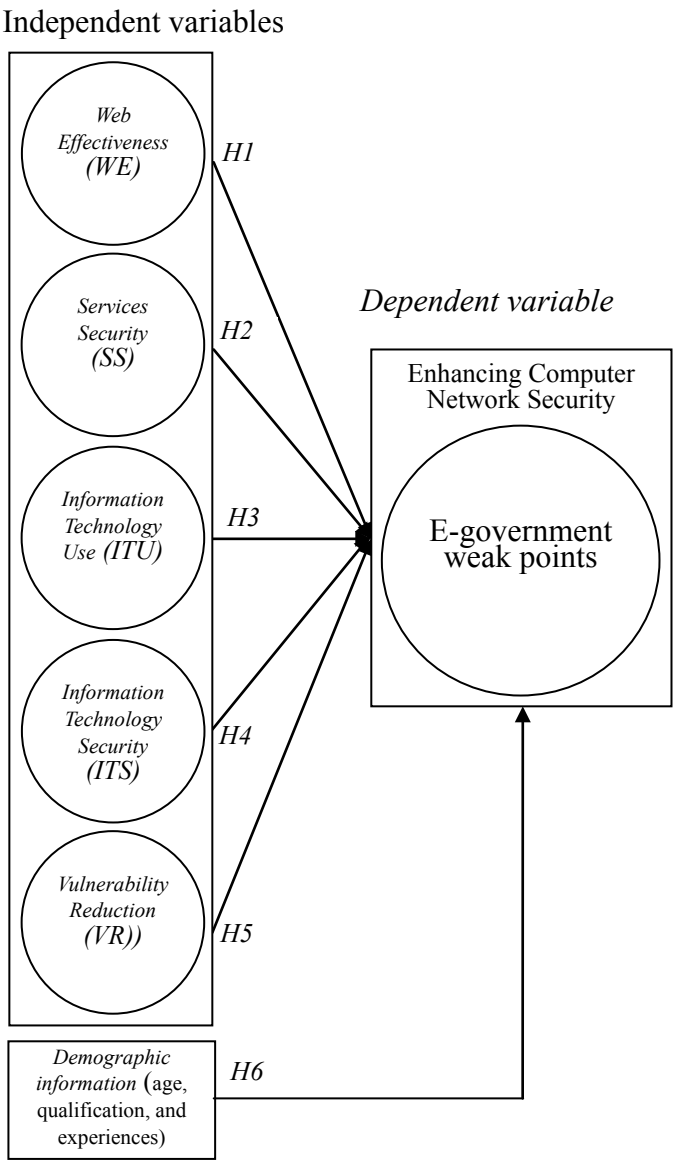

Figure 1. The research model

The hypotheses of this paper are;

H1: There is significant effect of *Web Effectiveness* (*WE*) on e-government weak points.

H2: There is significant effect of *Services Security (SS)* on e-government weak points.

H3: There is significant effect of *Information Technology Use* (*ITU*) on e-government weak points.

H4: There is significant effect of *Information Technology Security* (*ITS*) on e-government weak points.

H5: There is significant effect of *Vulnerability Reduction* (*VR*) on e-government weak points.

H6: There is significant effect of *demographic information* (age, qualification, and experiences) on e-government weak points.

In this paper the quantitative research approach was used. Williams (2007) argued that the quantitative approach does not only work with the theories, but it also works with the questions that are put to describe certain phenomenon. The quantitative approach works with the hypotheses that describe certain phenomenon as the way of analyzing data. Therefore, the quantitative approach collects the information from the participants' members by using the tools that are working with statistical information. These results in the quantitative approach are considered as explanatory and predictive results because they are demonstrated in a numerical form.

Data collection refers to the process of gathering information for a certain purpose by using certain tool as Hox and Boeije (2005) argued. Collecting data can be conducted by two different ways related to the primary and secondary data collection. The primary data collection refers to the process through which required data are gathered from previous literatures related to the same field of research in order to add new information to the existing store of knowledge, while the secondary data collection refers to using certain tool to gather information from the participants' members. In addition to that, the participants' members can provide the answers towards the questions to solve the problem of this study.

According to Malhotra (2006), questionnaire can be defined as a group of questions that are used to gather information from the participants' member. These answers reflect the way of describing certain phenomenon in which the participants' members are able to answer.

7. Data Analysis

Descriptive Statistics

The designed questionnaire was divided into five dimensions of 30 statements. The number of respondents is 356 from the total population 580 IT developer employees.

The reliability test was carried out using Cronbach's alpha, which measured the internal consistency of a construct. The recommended minimum acceptable limit of reliability (alpha) for this measure is 0.60 (Hair et al., 1998). Table (2) shows the Cronbach's alpha values to the dimension of the questionnaire.

The results indicate that the total reliability of the questionnaire was (0.933), which is an acceptable value indicating the tool consistency is at acceptable level. However, based on Hair et al, (1998), all the values of Cronbach's alpha for all the dimensions were accepted.

Table 2. Cronbachs' alpha of the questionnaire

No	Dimension	No. of items	Cronbach's alpha
1	*Web Effectiveness* (*WE*)	7	0.638
2	*Services Security* (*SS*)	5	0.776
3	*Information Technology Use* (*ITU*)	7	0.834
4	*Information Technology Security* (*ITS*)	5	0.768
5	*Vulnerability Reduction* (*VR*)	6	0.826
All	Total	30	0.933

The first section of the questionnaire intends to collect some information about the respondents' background (see Table 3). The respondents distribution regarding age 18-25 years were 44(17.18%), with age 26-35 years were 112(43.76%), with age 36-45 years were 40(15.63%), and who were above 45 years were 60(23.43%). The respondents distribution regarding qualification is as follows; 66(25.78%) had high school and technical diploma, 131(51.18%) had university degree, 59(23.04%) followed higher education MSc and PhD degrees. The respondents' distribution regarding years of experience the respondents with less than one year of experience was 8(3.13%), with 1-5 years were 94(36.72%), with 6-15 years were 74(28.90%), and with more than 15 years were 80(31.25%).

Table 3. Respondents demographic information

Demographic Information	Type or group	Frequency	Percent
Age (years)	18-25 years	44	17.18
	26-35 years	112	43.76
	36-45 years	40	15.63
	Above 45 years	60	23.43
Qualification	High school and technical diploma	66	25.7
	University degree	131	51.18
	MSc and PhD degrees	59	23.04
Experience	Less than one year	8	3.13
	1-5 years	94	36.72
	6-15 years	74	28.90
	More than 15 years	80	31.25

The descriptive statistics (means and standard deviations) were measured to describe the attitudes towards the statements in Table (4). From the table the following appears:

i. The mean of the 1st dimension measured the *web effectiveness* of e-government network is 3.571. It takes order 4.

Table 4. Mean and standard deviation of the questionnaire statements

No	Dimension	Statements	Mean	SD	Order
1	*Web Effectiveness* (*WE*)	S1: The development's process takes into consideration the ease of use	4.057	0.639	2
		S 2: There is a continuous feedback from users that ask for modifying the e-government service providing system	3.514	0.781	6
		S3: Capacity of e-government system is compatible within the multi-use feature	3.542	0.780	5
		S4: The layout of e-government's website is user friendly	4.171	0.663	1
		S5: The network interrupted is frequently occurred resulted from security attacks	2.400	0.811	7
		S6: The defence systems is regularly updated to detect new threats	3.742	0.885	3
		S7: Web designers try to develop a website that is competitive to other countries	3.571	1.170	4
	1st dimension mean		3.571	.4687	4
2	*Services Security* (*SS*)	S8: When any hacker tries to break through the network, a pre-defined risk mitigation plan starts to deal with this situation	3.657	0.764	4
		S9: All the components of any critical network (e.g.: firewalls**,** servers, routers, and hubs) are located in restricted or secured area	4.142	0.974	1
		S10: The available security level is achieving the desired needs and challenges	3.800	1.079	2
		S11: A simulation plan is being set according to the identified vulnerabilities to mitigate risk	3.314	0.993	5
		S12: Lacking of security results in losing users' of the website	3.714	0.957	3
	2nd dimension mean		3.725	.696	2
3	*Information Technology Use* (*ITU*)	S13: The e-government uses the latest IT to develop the capability in addressing the society needs	3.685	0.932	5
		S14: The e-government network is up-to-date and is flexible to install any periodically update that holds through utilizing the state-of-the art programs and technology	3.885	0.932	2
		S15: Network components of e-government are frequently scanned for attacks detection	3.800	0.797	3
		S16: The e-government uses the IT effectively in order to keep users data secure	3.771	0.877	4
		S17: The e-government tries to increase the number of applications online	3.971	0.785	1
		S18: The e-government uses IT utilization to achieve and enhance its goals	3.628	0.731	6
		S19: The e-government uses the IT to publish policies and programs that are related to the citizens	3.628	0.807	7
	3rd dimension mean		3.767	.595	1
4	*Information Technology Security* (*ITS*)	S20: The e-government work and security evaluated by surveys	3.057	1.027	5
		S21: The e-government users have the ability to easily and safely utilize the services at any place and time	3.800	0.833	2
		S22: The e-government offers the required services in a simple and secure way for users	3.857	0.733	1
		S23: The e-government ensures the safety of all the government IT infrastructures construction	3.657	0.838	4
		S24: System security needs are applicable to the e-gov such as truthfulness, secure expense mechanism and security mechanism support	3.714	0.859	3
	4th dimension mean		3.617	0.622	3
5	*Vulnerability Reduction* (V*R*)	S25: Testing and assessing the new technologies that are used in the E-government	3.828	0.821	1
		S26: The e-government measures and describes the financial, political, and social returns of the government technology programs	3.457	0.816	3
		S27: The e-government solves the difficulties of computing the return on investment for the community sector	3.400	0.694	6
		S28: The e-government improves the services of its interior operations as well as its exterior services that are provided for citizens	3.457	1.066	4
		S29: The e-government measures the effects of information and communication technology on users	3.428	0.948	5
		S30: The e-government improves the way of the security to transfer services of the users	3.571	0.850	2
	5th dimension mean		3.523	0.639	5

Table 5. One sample T-test of hypotheses

Hypothesis no	Test Value = 3					
	T	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
H1	7.213	255	.000	.57143	.4104	.7324
H2	6.166	255	.000	.72571	.4865	.9649
H3	7.627	255	.000	.76735	.5629	.9718
H4	5.871	255	.000	.61714	.4035	.8308
H5	4.847	255	.000	.52381	.3042	.7434

ii. The mean of the 2nd dimension measured the *services security* of e-government network is 3.725. It takes order 2.
iii. The mean of the 3rd dimension measured the evaluation of *IT use* in e-government network is 3.767. It takes order 1.
iv. The mean of the 4th dimension measured the evaluation of the *Information Technology Security* of the e-government network is 3.617. It takes order 3.
v. The 5th dimension measured the evaluation of the *Vulnerability Reduction*, of the e-government network is 3.523. It takes order 5.

It was found that there are positive attitudes toward all questions because their means are above the midpoint (3) of the 5-points Likert scale.

One Sample T-Test and One Way -ANOVA

To test hypotheses, two statistical tests were carried One Sample T-Test and One Way-ANOVA. To test hypotheses (*H1, H2, H3, H4, and H5)* related to the five dimensions in the questionnaire. One sample T-test was used to test these hypotheses. Table (5) shows that for *H1* (T=7.213), *H2* (T=6.166), *H3* (T=7.627), *H4* (T=5.871), *and H5* (T=4.847), the P-values to all hypotheses are 0.000, which is less than α=0.05. In this case, all the hypotheses are significant at the α=0.05 level. It is quite clear there are significant effects of (WE, SS, ITU, ITS, and VR) on e-government weak points.

These results argued with Nillhahan et al (2009) and Saint Corporation (2009) that the administrators must detect, find, treat, and manage any problem rapidly and effectively to prevent malicious entities access the e-government computer network. The e-government must identify the security issues in protecting the citizens' personal information from any threats. The results argued with Colesca (2009) results, that the important problem that faces the Kuwaiti e-government is the security problem, which allows unauthorized people to access other personal data. These results also corresponding with results of Syamsuddin and Hwang (2010) that e-government tend to use different programs and software to solve the technical problems that face them such as using web application security, intrusion detection systems, firewall, and penetration system that use open sources of technologies, because security plays a major role in enhancing each of the transparency, effectiveness, and efficiency of e-governmental applications which then affects communication flow between citizens and their e-governments.

Table 6. One way ANOVA test for age effect

Dimension	Sum of Squares	df*	Mean Square	F**	Sig.***
WE	0.701	3	0.234	1.071	0.376
SS	2.194	3	0.731	1.586	0.213
ITU	0.814	3	0.271	0.749	0.531
ITS	0.709	3	0.236	0.589	0.627
VR	0.732	3	0.244	0.574	0.636

*df: degree of freedom
**F: Factor
***Sig.: Significance

To test hypothesis H6 One-Way ANOVA test was used to test if there are any differences on assessment of e-government weak points according to (age, qualification, and experiences).

To test the effect of age on e-government weak points, one way ANOVA was used, and its results are shown in Table (6).

The P-values to all the dimensions are greater than α=0.05. In this case, age have no significant effect at the α=0.05 level on the e-government dimensions weak points.

To test the effect of qualification on e-government weak points, the one way ANOVA was used, and its results are shown in Table (7).

Table 7. One way ANOVA test for qualification effect

Study variable	Sum of Squares	df*	Mean Square	F**	Sig.***
WE	0.759	2	0.379	1.809	0.180
SS	1.314	2	0.657	1.385	0.265
ITU	1.789	2	0.895	2.792	0.076
ITS	1.241	2	0.620	1.667	0.205
VR	1.181	2	0.590	1.486	0.242

*df: degree of freedom
**F: Factor
***Sig.: Significance

The P-values to all the dimensions are greater than α=0.05. In this case, qualification has no significant effect at the α=0.05 level on the e-government dimensions weak points.

Table 8. One way ANOVA test for experiences effect

Study variable	Sum of Squares	df*	Mean Square	F**	Sig.***
WE	0.460	3	0.115	0.492	0.742
SS	0.547	3	0.137	0.258	0.903
ITU	0.455	3	0.114	0.295	0.879
ITS	0.457	3	0.114	0.270	0.895
VR	1.132	3	0.283	0.665	0.621

*df: degree of freedom
**F: Factor
***Sig.: Significance

To test the effect of experiences on e-government weak points, one way ANOVA was used, and its results are shown in Table (8).

The P-values to all the dimensions are greater than α=0.05. In this case, experiences have no significant effect at the α=0.05 level on the e-government dimensions weak points.

The results of the five dimensions of the questionnaire was agree with results of AL-Qaisoum (2009) and Muthanna (2009), that the security and assessing the weak points is very important for any applications, and can be monitored by the number of users using these applications.

8. Discussion and Conclusions

E-governments realized the concept and significance of security and weak points in their applications. Thus, the security and weak points issue in e-governments are controlling the trust of the users, who do their different transactions through Internet. This paper aims to assess the computer network system weak points at the Kuwaiti e-government computer network system. For this aim a questionnaire for IT- developers' was designed. The results showed the IT-developers agree on the significant effect of *Web Effectiveness* (*WE*)*, Services Security* (*SS*), *Information Technology Use* (*ITU*), *Information Technology Security* (*ITS*), *and Vulnerability Reduction* (*VR*) on e-government weak points to enhance computer network security. Their demographic information; age, qualification and experience have no significant effect on their responds for the five dimensions of the questionnaire, and this indicate the importance of these factors on assessing weak points regardless to their background. This concludes that these factors are important and influence the performance of e-government network.

The main contribution of this study is the security must be the first priority of any application or service introduced to users'. In order to eliminate the weak points that may occur in the network, and it will be a risk in using any application, therefore IT developers in any e-government must be continuously monitored the number of users' and compare these numbers statistically with the previous number of users' because the number of users' for each application or service reflect the degree of users satisfaction, which is depended on the users' confidence for the computer network security.

REFERENCES

[1] Alfawaz, S., May, L. J., and Mohannak, K. (2008). E-government Security in Developing Countries: A Managerial Conceptual Framework. *International Research Society for Public Management Conference*, 26-28 March 2008, Queensland University of Technology, Brisbane, Australia.

[2] AL-Qaisoum, A. M. A. (2009). Assessing of E-government Readiness in the Kingdom of Saudi Arabia, unpublished MSC Thesis, Arabian Gulf University, Bahrain.

[3] AL-Shehry, A., Rogerson, S., Fairweather, N. B., and Prior, M. (2006). The Motivations for Change Towards E-government Adoption: Case Studies from Saudi Arabia. Retrieved 3rd January 2014, from www.iseing.org/egov/eGOV06/Accepted%20Papers/604/CRC/eGOV06-604%20CRC.pdf.

[4] Colesca, S. E. (2009). Understanding Trust in E-government. Engineering Economics, 3, 7-15. Retrieved January 2nd 2014, from http://www.ktu.edu/lt/mokslas/zurnalai/inzeko/63/1392-2758-2009-3-63-07.pdf.

[5] Elssied, N. O. F., Ibrahim, O., A. Alaziz, A. A., and Yousif, A. (2011). Review Paper: Security in E-government Using Fuzzy Methods. *International Journal of Advanced Science and Technology*, *37*, 99-112.

[6] Hair, J., Anderson, R., Tatham, R. and Black, W., (1998). Multivariate Data Analysis. 5th ed., Upper Saddle River, NJ: Prentice-Hall.

[7] Hox, L. L. and Boeije, H. R. (2005). Data Collection, Primary vs. Secondary. *Social management*, *1*, 593-599.

[8] Karokola, G. and Yngstrom, L. (2009). Discussing E-government Maturity Models for Developing World – Security View. *Proceedings of ISSA Conference*, University of Johannesburg, 6-8 July 2009, Johannesburg, South Africa.

[9] Kurose, J. F. and Ross, K. W. (2005). *Computer Networking: A Top-Down Approach Featuring the Internet*. 3rd ed. Institute Eurecom, France.

[10] Malhotra, N. K. (2006). Questionnaire Design and Scale Development, in the Handbook of Marketing Research: Uses, Misuses, and Future Advances, R. Grover and M. Vriens, eds. Thousand Oaks, CA, USA: SAGE Publications, 83-94.

[11] Moen, V., Klingsheim, A. N., Simonsen, K. I. F., and Hole, K. J. (2007). Vulnerabilities in E-governments. Retrieved 9th January 2014, from http://www.nowires.org/Papers-PDF/ICGeS_egov.pdf

[12] Muthanna, Y. M. A. (2009). Assessment of Information Security Risk Management in Enhancing Information Security Network _ Applied Study: Bahrain Government Data Network, unpublished MSC Thesis, Arabian Gulf University, Bahrain.

[13] Panda, P., Sahu, G. P. and Gupta, P. (2010). Promoting Transparency and Efficiency in Public Procurement: E-Procurement Initiatives by Government of India. 7th International Conference on E-government (ICEG) 2010, 22-24 April 2010, IIM Banglore, India.

[14] Saha, S., Bhattacharyya, D., Kim, T. H., and Bandyopadhyay, S. K. (2010). Model Based Threat and Vulnerability Analysis of E-Governance Systems. *Science and Technology, 3*(2), 7-22.

[15] Saint Corporation (2009) Saint Corporation. (2009). Integrated Network Vulnerability Scanning and Penetration Testing. USA. Retrieved 3rd January 2014, from http://www.saintcorporation.com/resources/SAINT_integrated_pen_testing.html.

[16] Scarfone, K. and Mell, P. (2010). The Common Configuration Scoring System (CCSS): Metrics for Software Security Configuration Vulnerabilities. USA.

[17] Schneier, B. (2005). The failure of two-factor Authentication. Retrieved 10th March 2014, from www.schneier.com/blog/archives/2005/03/thefailureof.htm.

[18] Schwester, R. W. (2009). Examining the Barriers to E-government Adoption. Journal of E-government, 7(1), 113-122.

[19] Syamsuddin, I. and Hwang, J. (2010). A New Fuzzy MCDM Framework to Evaluate E-government Security Strategy. *IEEE 4th International Conference on Intelligence and Security Informatics*, Hellenic American University, 9-11 August 2010, Athens, Greece.

[20] United Nations Department of Economic and Social Affairs (2007). *Managing knowledge to build trust in government*. 1st ed. United Nations Publication No.: ST/ESA/PAD/SER.E/118, NY, USA.

[21] Upadhyaya, P., Shakya, S. and Pokharel, M. (2012). Information Security Framework for E-government Implementation in Nepal. *Journal of Emerging Trends in Computing and Information Sciences*, *3*(7), 1074-1078.

[22] Williams, C. (2007). Research Methods. *Business & Economic Research*, *5*(3), 65-72.

[23] Wong, M. S., Hideki, N., and George, P. (2011). The Use of Importance Performance Analysis (IPA) in Evaluating Japan's E-government Services. *Theoretical and Applied Electronic Commerce Research*, *6*(2), 17-30.

[24] Zhao, J. J., Truell, A. D., Alexander, M. W., and Davis, R. (2008). A vulnerability Audit of the U.S. state E-government Network Systems. *Journal of Information Systems, 9*(2), 8-13.