Security of E-government; Risks, Threats, and Success Factors

Shareef M. Shareef

Software and Informatics Engineering Department

College of Engineering

Salahaddin University-Erbil

ABSTRACT

The development of Information and Communication technology (ICT) and the rapid growth of the use of internet facilitate the use of government services in both public and private sectors. Hence, users can easily use the available services from places at a time that are convenient to them via internet, anywhere and anytime. On the other hand, together with its perceived positive potential, e-Government also involves threats and risks. Therefore, E-government has to be secure as technology develops and the consumers have to follow the procedures to make their own transactions safe. The effective management of information security is a key factor as readiness, of the different consumers to use e-Government services will greatly depend on the trust they have on the security of information. This paper reviews and discusses the security threats and risks in e-Government also provide critical success factors might help to reduce the risks and threats of information security in e-government system.

Keywords: Risks, threats, Vulnerability, eGovernment security, success factors.

1. Introduction

Since 20th century the wide spread of technology, particularly internet created vast change in political, economical, societal, and human beings live. The globalization concept emerged and increased dominance as use of the internet spread the worldwide with a short period of time altered the world into small, global village. This encouraged many, international organizations, consultants, government expertise and, researchers to evolve and adopt ICT in public services. Consequently, emerged a new notion called electronic government (e-government), which is refers to the use of internet and other digital means to deliver information and services to their citizens (Shareef, et. al. 2012; Panagiotopoulos, et. al. 2012).

Despite the fact that the achievement appropriation of e-government dependent upon citizen’s trust and their eagerness to utilize it, little thought has been paid to investigate the selection of e-government from the citizens' trust viewpoint (Alzahrani, et. al. 2017). This lack of trust comes from the issues of threats and risks in citizen information. The potential efforts in this regard, many governments across the globe are still suffering from the lack of public participation in the e-government services (Al-Hujran, et. al. 2015; Shareef, et. al. 2012; Gupta, et. al. 2008; Rana & Dwivedi, 2015). The security threats even in developed countries; some people still do not use electronic means in its transaction. These issues require extra research attention, since the development of e-government mainly depends upon the public participation and the use of e-services.

In order to encourage citizen to use the e-government services, it is essential to make the people, trust in the government system, and make sure their information and its privacy are protected. However, from the citizen’ perspective the government is seen as one entity; so a security of one department of government might be viewed as a failure of the entire government system. Therefore, the process of protecting information security of the entire government departments is viewed as a vital process. This paper reviews and discusses the security risks and threats and identifies success factors to protect the security of information in e-government.

The rest of the paper is organized as follows: in the next section information security will be presented. In section three, the security threats and risks in e-government will be reviewed and explained. However, in section four, analysis of the success factors which might help in securing e-government system will be tackled, and the conclusion of this work will be presented in section five.

2. Information Security

In twenty-first Century, the ICT has quickly spread throughout into each field of human community. Shape the Large national or international fields to the small families or people, increasingly individuals’ utilization of information innovation to offer advantageous, quick and effective work and business. Gradually we have entered into another world, the information age. In any case, the data framework advancement is a "twofold edged sword". It made tremendous advantages for the humanity; in the meantime, the issue of data security was to bring an extraordinary misfortune and burden. The infection, programmers uncontrolled, the spillage of insider facts, framework disappointment, interference of administration and different PC wrongdoings developed in an interminable stream. With the human's higher reliance on informatization, misfortune created by information security is turning out to be increasingly striking (Yuan, and Chen, 2012).

Information Security is the cornerstone of an effective e-government system. The information system is a process of identifying issues that have the possibility to cause damage or threat situations and implementing protections to eliminate this potential. This process of the countermeasures will be achieved by the security process (Schechter, 2004). The development of new technology has created various security methods to secure information to individuals, institutions, armies and nations. These methods vary in terms of the context; some were based on rules, regulation, policies and mathematical approach and others based on pure cryptographic knowledge (Shareef, 2012). Since the number of security models increased, the challenges continued to increase and researchers continued to investigate to find out various solutions via new models and development of existing once. One of the main challenges of the e-government system is how the advanced technology can be used not only to raise efficiency for government, but also to reinforce confidence in privacy measures by making transparent environment between citizen and government (UN, 2012). The e-government system will remain susceptible to security breaches in absence of proper and robust security policy.

Information security before has concentrated on confidentiality of information stored electronically. The brisk advancement in the volume of such data and the support of online business inside associations has definitely the need for expanded security to ensure the protection of this data and avoid unauthorized access activities. There is a promising need to improve security of information, privacy and trust in government in order to raise confidence in e-government as recognized in developed and developing countries (EC, 2010).The quick growth in computer security incidents consequently eases in obtaining and using hacking tools, steady advance in sophistication and effectiveness of attack technology and the dire warnings of new and more destructive cyber-attacks etc., could affect the e-government system. On the other hand, cyberspace is being used not merely by government also used broadly by individuals for social interaction, financial interactions as well as for commercial purposes via unsecured, unreliable wires or wireless technology. Cyber security has to deal with cyber regulations on e-Commerce, e-Banking, e-Government, e-Healthcare and e-Markets. All these rely on upon the administration of the internet to encourage the utilization of the web as a medium to support general exchange without the risks.

In any case, everyone with the exception of those profiting from insecure digital world is looking forward for a dependable technology environment that provides security, privacy, confidentiality, integrity, and availability of reliable and authentic information (Spanos, and Angelis, 2016). In this respect, different information security standards are well represented in the open literature (Saint-Germain, 2005). These standards attempt to characterize the various procedures and controls required for effectively executing an information security policy, rather than advising what the policy should look like (Wang, 2009). The Security policy is intended to figure out what is normal from an establishment concerning security of Information Systems. For the most part, these principles have been produced to control and direct human behavior to avoid the risk to information assets by accidental or deliberate actions. Also, it supports the security and well-being of information resources through the experiences of leading (Shailendra, and Singh, 2011).

3. Security threats, risks, and vulnerability in e-government

There are many researches and articles written to attempt to define each of threats, risks, and vulnerability individually. In any case it is the interactive relationship of every one of the three of these parts that merge to make the fundamental assessment and suggested action plan for risk administration. As the individual responsible for the oversight of the security of your agency, the more that you can excuse this procedure, in a way like the approach of an expert with high level security expert. The better is your knowledge and clarification of the after effects of their security reviews, and also your capability to execute their discoveries in a way most suited to your own particular agency or establishment.

In order to understand the process of managing risk, we think that risk, threat and vulnerability are not exchangeable terms in spite of the fact that risk and vulnerability are a part of the risk. It’s essential to define these terms individually. The risk refers to the probability of being focused by a given attack, of an attack being effective and generally present to a given threat. A risk assessment is performed to decide the most important potential security breaches to address now, as opposed to later (Perrin, 2009). However, the threat is anything be influenced or harmed by a particular thing, deliberately or by mistake, and obtain, damage, or destroy an asset. Off course asset is what we are attempting to protect. The vulnerability is weaknesses or gaps in a security program that can be used by threats to obtain unauthorized access to an asset (Coelho, 2007).

The development and the spread of e-services impacted the effectiveness of the e-government system, and hence raised extra threats, and risks for governments in developing and even in developed countries. The government information will require an extra attention to secure programs in order to avoid any unauthorized access might impact the government operation and reveal citizen's private information. When we talk about government information security, we have to identify various aspects might affect the security of information. The security framework of e-government consists of the main three elements; people, processes and technologies. In this paper, our focus would be on the E-government information security in terms of the threats and risks in technological perspectives.

There are many threats that face compelling and proficient sharing of data between government institutions on one hand, and between governments, business, and citizen on the other hand. These threats are based on the lack of trust and transparency in information system design, to ethical and legal issues when integrating information systems (Mattord, and Whitman, 2006). This legitimizes the requirement for an inclusive security system that takes into consideration the systems integration components.

3.1. Threats of Information security in E-government

Events are coming in various structures and sizes, and it be entered from anyplace on the Web, though some attacks must be started from particular networks or systems and some need access to uncommon accounts. A cyber attack might be a small event engaging a site or a big event in which many sites are influenced. A characteristic attack made up by accessing a customer's account, getting advantage access, and utilizing the victim's system as a bargain on a platform for attacks on other sites. It is conceivable to obtain all these steps manually in a couple of seconds; with automation, the time reduces further. However, it is hard to identify the people who cause events (Hector, 2012). Many researches have revealed that there is a link between security and e-Government (Siponen and Oinas-Kukkonen, 2007). Numerous researches were analyzed to provide various models to address the security threats of the e-government and to measure confidentiality, integrity, and availability known as the C.I.A triangle. Security threats are expected to convince the public in using e-government services and government administration and departments to access, share and exchange information securely (Al-Azizi, S. 2008). There are various technical and physical threats influencing the security of e-government information (Chen, et. Al. 2015; Khalid, et. al. 2014; Louie, 2014;

Zu’bi, and Al-Onizat, 2012; Rodgers, 2012; Mazumdar, and Banerjee, 2009; Conklin, and White, 2006; Omura, 2000; Polk, and Hastings, 2000) such as;

Information sharing: Exchange of information between government institutions was always considered a significant concern. This exchange is necessary for government institutions to complete an e-service process. For instance, sharing the citizen profile, or authenticating an applicant.

Electronic Authentication*:* To succeed e-government system, it’s vital to offer a highly reliable individual identification system for both private and public sectors as well as for government institutions. In which they handle forms and make decision on their contents. Public Key Infrastructure (PKI) is the technology has been identified as the best e-authentication for e-government.

Identification: Securing the participant’s safety in terms of unique identification.

Privacy: Threat of disclosing confidential information, and unauthorized access to the citizen’s private data.

Access Control: Is a user-oriented type which comprises on identification, authentication and authorization issues. In other words, protect systems in order to avoid intruders to use access control mechanism to gain government and citizen’s information. Insufficient logical access controls reduce the reliability of department’s computerized data and increase the risk of unauthorized revelation.

Out-of Band data denial of service*:* When an attacker sends out-of-band data port 139, an attacker can cause a Windows system to lose network ability and perhaps damage.

Land denial of service: Local Area Network Denial, occurs when an attacker sends an IP spoofing packet. The transmission can fool the machine into thinking it was sent itself a message which, depending on the operating system, and then will crash the machine.

Teardrop denial of service*:* When an attacker sends a traditional user datagram protocol (UDP) packet causing the system to not respond.

Network Security: Lack of internet availability and high cost, particularly in developing country along with Network attacks, systems architecture and network topology issues, are threats needs to be considered.

Data type: Classifying data is the process of sorting data resources based on nominal values according to its sensitivity (i.e., effect of applicable laws and regulations. Data and information resources are classified based on the risk of unauthorized access, for instance lost or stolen accidentally. Data with high risk classified as a Confidential, in which requires a greater level of protection, while lower risk data, possibly labeled “internal” requires proportionally less protection.

Work flow: Work flow technology is a technique used to manage the flow of work and data during the planning, execution, and evaluation phases in e-government system. For example, it can illustrate an individual or an organization’s progress of online application, which is very important for e-government.

Bridge Certification Authority (BCA): Government departments are using Public Key Infrastructures (PKIs) to execute internal transaction processes, by implementing virtual private networks (VPNs), to secure the resources of the government. Also, most government departments are connected with other departments to execute a one-stop-process. If these connected department’s desire to use their internal security capabilities for government to government (G2G) relations. The connection of their corporate PKIs will be required. Though, corporate PKIs can implement different architectures, security policies, and cryptographic sets. The Bridge Certification Authority can be used to link these corporate PKIs and translate these corporate relationships into the e-world.

Network infrastructure*:* lack of proper installation of network firewalls, Network security configurations, Internet protocol vulnerabilities, and Internet Dependence are the main challenges that impact the security of e-government.

Internet infrastructure*:* Serious attacks include elements of internet infrastructure rather than particular systems on the internet. For instance, network access providers, network name servers, and huge archive sites on which several users depend on. Despite of these, automated attack might also influence the threat of infrastructure. Hence, might seriously delay the daily operation of many sites.

Malware: Is short for “malicious software” and it is a computer program (e.g., scripts, active content, code, and other software) precisely designed to harm and destroy a computer system. Hence, leads to loss of privacy or misuse, and obtain unauthorized access to assets, and other abusive behavior.

Packet Sniffer: It is a tool or network analyzer used by technicians to diagnose network related problems. However, this tool can also be used by an attacker to collect passwords and cause a serious breach in e-business and secured transmission.

Probe: It is an action used to check the connectivity between two ends, for instance an empty message can be sent to know the receiving end really exists. An attacker can use the information during this connectivity to notice for exploiting for example, ipsweep, portsweep, nmap, satan.

Communication Channel threats: Normally messages are traveling through the internet taking various paths from the source to the destination. It will be difficult to guarantee that every node on the internet through which message travel, is secure, safe, and non-hostile.

Server End threats: Server is one of the main parts of the network. It is subject to vulnerabilities which can be abused by an attacker to cause damage or to illegally obtain information.

Firewalls: A firewall is a set of related programs, or hardware, situated at a network gateway server, which defends the assets of a network from users. It also means the security policy that is used with the programs.

In addition, from a technical perception, in the scope of both e-commerce and e-government, in general, there are three main kinds of threats: unauthorized access that impacts the confidentiality, unauthorized modification or change to the information which impacts the integrity of information, and availability that impacts the availability of both information and services. All those threats, according to its nature can seriously create issues and problems for all e-government, business and citizens.

3.2. Risks of Information security in E-government:

Information sharing between government institutions is always considered as an anxiety. Despite the fact that it's essentially this is due to the completion of e-services process securely. Information security risks e-government facing includes the following: (Chen, et. al. 2015; Webb, et. al. 2014; Anders, et. al. 2013; Al-shboul, 2012; UN, 2012; Zu'bi, and Al-Onizat, 2012; Iivonen, 2011; Mazumdar, and Banerjee, 2009; Al-fawaz, et. al. 2008; Al-Azazi, 2008; Zhou, and Hu, 2008).

Interoperability: The capability of systems or business processes to work together to achieve a common task has remained a long standing in developing and even in the developed countries aims. The effectiveness of the communication between and among government, business and citizens, needs that the product they use are capable of sharing and exchanging of data. The lack of interoperability due to semantics, lack of standards, different classification systems will influence destructively the effectiveness of the e-government system.

Usability: Usability is concentrated on creating applications, programs, and services to be easy for citizens to use. The usability challenge is based on the security concern, if the security level is high and consequently, increases the potential of usability.

Information faking: is the process when the attacker knows the rules of the data in the network, or after they decodes the program information; they could pretend legal users or create false information to cheat other users, the main forms involve pretending users to get illegitimate certifications, faking e-mails, and etc.

Security Standards: These standards deal with regulatory authorities and governing bodies that define e-government security policies to guarantee secure working environment. It includes e-voting, e-democracy, e-signature and other agreements, between government and users, and other stakeholders.

Security policy: Is a plan to determine the institution's fundamental resources with a detailed explanation of the acceptance or not and rational behavior from citizen and other stakeholders in order to efficiently guaranty information security. This plan has to accompany with the performance level of e-government. This performance must be evaluated to fulfill the security measures.

Service denies: It is the total invalidation of the system's network or the servers of the system at some stage. It mostly creates by the attack of the hackers or the virus, and the man-made damage of the devices too.

Legal Framework: Includes aspects such; as laws and regulations that pose a lot of problems related to security crime and security risks if not considered seriously. Lack of laws and regulations on information security will impact negatively the trust in government. For instance, hacker attacks, viruses, masquerades of unauthorized identity and computer forgery. There have to be certain laws and regulations to judge and hence, to make e-government solutions legally binding. A suitable policy framework for IT security determines to strict norms and processes in the system for ensuring confidentiality, integrity and availability of reliable and authentic information.

Privacy: The use of advanced technology not merely to increase efficiency of public administration, however, to strengthen confidence in the privacy process by making common transparency between citizens and public administration. For instance, while there is a demand for a secure system to obstruct unauthorized access to data, these personal data have to be available to citizen to access who wishes to verify the use, authenticity and accuracy of his/her own personal data.

Culture: Security culture generally is observed as part of national culture. It indicates the predominant attitude towards styles to a secure institutional environment. Regulatory interference is vital in creating rules and regulation for using and defending information resources. These challenges are influenced by legislative and regulatory frameworks, and national, and institutional cultures.

In addition, the cultures are varied between developed and developing countries. Developing countries are facing cultural difficulties when trying to implement technology was created abroad. For instance, the lack of citizen participation in decision making, division between government and citizens, traditional values, and conservatism might hinder the effectiveness of information security programs there.

Information Intercepting: It means that the related e-government consumers or attackers catch or take the e-information from governments or different clients**.**

Awareness: Is the ability of human beings to feel, observe, and aware of what is happening around him/her, also to understand the meaning of information now and in the future. This awareness is determined by the type of information, whether it’s good or bad for a particular work or aim. The information security awareness is crucial to understand the feasibility of the security used in this regard. For example, finding risks related to intangible knowledge resources requires new human and technical resources. Such as experts from outside, and software for the collection and analysis of data to be accomplished in order to gather the right data, to introduce and support of the bigger picture of risk assessment.

In addition, the user awareness is always observed as a main point and a challenge in any ICT system, particularly in developing countries. The lack of security awareness and the lack of knowing the importance of information security impact the misuse of the system due to the lack of an appropriate awareness program. For example, where institution employees doing activities such as: deliberate or accidental entry of dire data (i.e. sharing of passwords; introduction of computer viruses; suppression and destruction of the output; unauthorized document visibility; directing prints and disseminated information) to people who are not allowed to have them.

Information Tampering: The internet inventor interferes, insert or delete original data via different technical ways, and transfer them to the destination, in order to harm the integrity of the data.

Trust: The trust risk plays a significant role in the acceptance of e-government services and adoption. The trust in government mainly depends on the relationship between the e-government authority and the other governmental institutions on how convinces the government infrastructure, the internet service providers (ISP) and the other government institutions. To obtain a high level of confidence and trust, it’s vital to have a high level of security awareness. This will be achieved, by engaging government employees to learn about the security policies, architectures, competencies, supporting the security purposes and the operational procedures in the government institutions. Hence, will aid in raising the level of confidence and increases the level of trust in government. Trust in government ensures that transactions are observable and accountable to authenticated person and cannot subsequently be denied.

In addition, making a trusted framework for digital authentication is a vital aspect in promising the integrity of online and mobile financial transactions. A high level of trust among the people and government institutions will also be the important focal point of a successful e-government deployment.

Political*:* The political issue is also a significant risk that influences the security of information on e-government. The electronic intelligence works between the countries through surveillance the systems. Attempting to access or damage these systems by sending viruses, or personalized identification for the employees, or hacking the passwords. In order to accomplish utilization in the commercial field by knowing some secrets about these systems and utilize it against them or in the competition.

4. SUCCESS FACTORS IN SECURING E-GOVERNMENT

Different reviews were investigated to distinguish and measure the success factors confronted by the government institutions in executing e-government strategies.

Aljifri et al, (2003), declared the holistic approach for providing success factors for security solutions, particularly in developing countries. The lack of necessary security technology structures such as Public-Key Infrastructures (PKI) and adequate encryption systems, are tangible challenges which affect to enable a high quality of electronic information. These types of technologies can ensure confidentiality and provide access control, integrity, authentication and non-repudiation services for organizations moving into the information age.

In most developing countries, there is no governmental infrastructure that supports authentication, confidentiality, and integrity, such as; PKI, and satisfactory encryption system to assist a high quality of e-information. Therefore, establishing and developing secure technical infrastructure objectives for the information security targets and the operating environments is crucial. For example, the vital point apart from preservation of confidentiality, integrity and availability of information about security services are the authenticity, accountability, non-repudiation and reliability of information. Security properties are techniques that offer the security facilities such as; digital signature, firewall, and passwords. These technical infrastructures are able to handle the requisite volume and kind of transactions in a secure way is an inevitability in obtaining the information assurance goals. It can also offer access control, integrity, authentication and non-repudiation services for institutions moving into the e-information stage.

In addition, a few organizations see specialized arrangements as prompt solutions for their data security issues, security items: firewalls, antivirus programs, PKI frameworks, and VPNs are exceptionally profitable weapons, yet this approach suggests critical cost. Recommended security innovation is especially costly, so a qualified person to execute and work the innovation are required. Measuring e-government services in the context of both the quality and the quantity of security services and thus, provides enhanced and secure e-government services. Initially applying the model as a checklist for identifying, developing and implementing e-government security requirements is essential. Then creating a plan for security requirements of a given e-government services projects, this will be done before, during and after implementation of the project.

Furthermore, the security necessities of any e-government system should analyze the threats and attacks that may face it. This is typically integrated into the secure application development using a modern software risk analysis methodology. Those will be capable government institutions to prepare themselves for any vulnerable or undesirable issue in the context of assurance of confidentiality, integrity and availability of consistent and reliable information. The effective selection of an information security management system (ISO/IEC, 2016) essential to ensure information assets, permitting an association to achieve more noteworthy confirmation that its information assets are sufficiently insured against information security risks on a nonstop premise. Also, maintaining an organized and complete system for distinguishing and surveying information security risks, selecting and applying material controls, and measuring and enhancing their adequacy. Along with continually enhancing its control surroundings, and effectively accomplish legitimate and administrative consistence.

In the context of the hardware/software point of view, the government administrations have to advance the ICT framework for e-government. However, from the legal perspective, it is important to set up a legal framework with a specific end goal to give chances to individuals to be equivalent before the law. With regards to the procedure, powerful security benchmarks, and information administration must be executed for e-government. The arrangement of specific administrations and the declaration of its quality likewise are fundamental. Alongside the making of an international authentication center, which help the user to utilize the administrations with their individual identities and all transactions are registered in the national file management center to save the e-documents from any damage or abuse. Securing the protection of people information is significant to raise the level of trust in government. In the meantime, from the user point of view, government administration needs to encourage and support its representatives to get knowledge-based security skills. Likewise, need to have a high acceptance of users, clearly outline the authority and responsibility of users and it has to enhance the users' information technology skills. Government authority likewise needs to make different electronic means, which is crucial to support e-government system, for example, video phones, wireless communication, and video conferencing.

Despite the fact of the differences of technologies (Singh, and Karaulia, 2011) and tools have been delivered to help establishments to secure their systems and information against intruders. Still, there are threats and risks that influence the security of the users' information and privacy. One of the focal points of reducing the level of risk is risk management, which includes risk identification, risk analyzing, and risk controlling. The security requirements for an e-government system are achieved by system assessments. Risk identification is the initial phase of risk management in order to recognize the security risks of e-government successfully. Risk analysis, with respect to different types of quantitative and qualitative means; for instance analysis, comparison, assessment, and etc., is to make a decision about the importance of each factor of e-government risks, order the factors, and then assess each potentially result in an e-government system. However, risk controlling is to pick and utilize some risk controlling means to ensure the risk can be decreased to a reasonable stage. Risk controlling is the most critical phase in the risk management. It is the focal point to figure out if the risk management is effective or not. The aim of e-government security risk controlling, is to decrease the risk level, which e-government projects tolerating.

The other important success factors in securing e-government information is the establishment of an appropriate strategic framework for ICT security that determines the protection of norms and procedures in the system for guaranteeing confidentiality, integrity and availability of consistent and reliable information. This challenge merits considering by government authorities as a component that drives fruitful information security with regards to e-government. The active support of administration, staff awareness and preparing are additionally factors that should be considered, in light of the fact that at least the managers will be responsible and in charge with the tasks of starting and supporting any venture alongside appropriate security awareness. Moreover, ensuring that the government authorities, employees get information security education and training consistently.

5. CONCLUSION

In this paper, the author reviewed the issues related to the security of information in e-government such as; risks, threats, and vulnerability, also identified the success factors might affect in reducing the level of threats, risks and vulnerability in the e-government system. The author believes that to ensure e-government systems current information security best practices have to be utilized. Security policies, practices and procedures have to be set up and also use of security technology, which ensures e-government systems against attack, identify irregular activities services and to have a demonstrated alternate course of action set up. The findings also revealed that the substantial factors are to have an appropriate public-key infrastructure offering the required level of authentication and integrity and also to have a continuous awareness and training program to guarantee individuals know security risks, understand how to distinguish potential issues and carry on likewise to keep up a secure e-government service.

References

- Al-Azazi, S. (2008). A multi-layer model for e-government information security assessment. PhD thesis. Available at: http://core.ac.uk/download/pdf/370319.pdf. (Accessed on: 21/06/2015).
- Al-fawaz, Salahuddin and May, Lauren J. and Mohanak, Kavoos (2008). E-government security in developing countries: a managerial conceptual framework. In: International Research Society for Public Management Conference, 26-28 March 2008. Queensland University of Technology, Brisbane.
- Al-Hujran, O., Chatfield, M., Migdadi, M., (2015). The imperative of influencing citizen attitude toward e-government adoption and use. Computers in Human Behavior, Vol.53, pp 189–203.
- Aljifri, H.A.; Pons, A.; Collins, D. (2003). “Global e-commerce: a framework for understanding and overcoming the trust barrier”, Information Management & Computer Security, Vol. 11, No. 2/3, pp. 130-138.
- Al-shboul, R., (2012). Security and Vulnerability in the E-Government Society. Contemporary Engineering Sciences, Vol. 5. No. 5, pp. 215 – 226.
- Alzahrani, L., Al-Karagholi, W., and Weerakkody, V., (2017).Analysing the critical factors influencing trust in e-government adoption from citizens’ perspective: A

systematic review and a conceptual framework, International Business Review , Volume 26, Issue 1, February 2017, Pages 164–175.

- Anders, J. Mikkel, L. J., Linda K., Geert, M. and Arnd, W., (2013). The STOA project 'Security of eGovernment System, Final report. Vailable at: http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/513510/IPOL-JOIN_ET(2013)513510_EN.pdf. Accessed on: 4/08/2015).
- Chen, J. V., Jubilado, R. J. M., Capistrano, E. P. S., & Yen, D. C., (2015). Factors affecting online tax filing – An application of the IS Success Model and trust theory. Computers in Human Behavior, 43, 251–262.
- Coelho. (2007). Security Certification For Organizations A Framework To Manage Information Security, Stituto Superior de Ciências do Trabalho e da Empresa.
- Conklin, A., and White, G., B. (2006), e-Government and cyber security: The role of cyber security exercises, Proceedings of the 39th Annual Hawaii International Conference on System Sciences, HICSS'06, Vol. 4, Jan 4-7 2006, Kauai, HI, United States, IEEE, US, pp. 79b.
- European Commission (2010). European eGovernment Action Plan 2011-2015. Available at: http://ec.europa.eu/digital-agenda/en/european-egovernment-action-plan-2011-2015. Accessed on: 26/07/2015.
- Gupta, B., Dasgupta, S., & Gupta, A., (2008). Adoption of ICT in a government organization in a developing country: An empirical study. Journal of Strategic Information Systems, 17(2), 140–154.
- Hector D. Puyosa P., (2012). e-Government: Security Threats', IEEE computer Society, avilavle at: http://stc-egov.ieee.net/blog/e-governmentsecuritythreats. (Accessed on: 22/10/2016).
- ternational Organization for Standardization and the International Electrotechnical Commission (ISO/IEC) (2016). *Information technology — Security techniques — Information security management systems — Overview and vocabulary*. ISO/IEC 27000:2016. Available at: http://www.iso.org/iso/catalogue_detail?csnumber=66435. (Accessed on: 25/11/2016).
- Khalid, M. I. Khreishah, A., and Azeem, M., (2014). Cloud Computing Security: A Survey, Computers -Open Access Journal, Vol 3, pp. 1-35.
- Iivonen, I., (2011). Information Security Culture or Information Safety Culture-What do words Convey? Proceedings of the 10th European Conference on Information Warfare and Security. The Institute of Cybernetics at the Tallin University of Technology, Tallin, Estonia.7-8 July 2011.
- Louie, C., (2014). The truth about cloud security, A Dropbox for Business guide, Available at: https://blogs.dropbox.com/business/2014/06/truth-about-cloud-security/ (Accessed on: 25/07/2015).
- Mazumdar, C. K. K., and Banerjee, P., (2009). On Information Security Issues in Egovernance: Developing Country Views.CSDMS, Journal 6th July.

- Mattord, H., and Whitman, E. M., (2006). Readings and Cases in the Management of Information Security, Thomson.
- Omura, H., (2000). Information technology (IT) for E-government. Available at: http://www.fujitsu.com/downloads/MAG/vol36-2/paper16.pdf. (Accessed on: 12/05/2015).
- Panagiotopoulos, P., Al-Debei, M. M., Fitzgerald, G., & Elliman, T., (2012). A business model perspective for ICTs in public engagement. Government Information Quarterly, 29(2), pp.192–202.
- Perrin, C., (2009). Understanding risk, threat, and vulnerability, in IT Security, July 7, 2009. Available at: http://www.techrepublic.com/blog/it-security/understanding-risk-threat-and-vulnerability/, (Accessed on: 21/10/2016).
- Polk, W.T., and Hastings, N. E., (2000). Bridge Certification Authorities: Connecting B2B Public Key Infrastructures, NIST.
- Rana, N. P., & Dwivedi, Y. K., (2015). Citizen's adoption of an e-government system: Validating extended social cognitive theory (SCT). Government Information Quarterly, 32(2), 172–181.
- Rodgers, C., (2012). Data Classification: Why is it important for Information Security? Available at: https://www.securestate.com/blog/2012/04/03/data-classification-why-is-it-important-for-information-security. (Accessed on: 13/09/2014).
- Saint-Germain, R., (2005). Information Security Management Best Practice Based on ISO/IEC 17799. Information Management Journal, Vol.39, Issue 4, pp. 60-66.
- Schechter, S., (2004). Computer Security Strength & Risk: A Qualitative Approach, the Division of Engineering and Applied Sciences, (PhD thesis in Computer Science thesis), Harvard, US. Available at: http://research.microsoft.com/pubs/192264/thesis.pdf, (Accessed: 29/07/2015).
- Shailendra Singh, S., and Karaulia, D. S., (2011). E-Governance: Information Security Issues. Proceeding of the International Conference on Computer Science and Information Technology (ICCSIT'2011) Pattaya.
- Shareef, M. S., (2012). *Electronic Government Adoption Based on Citizen-Centric Approach in Regional Government in Developing Countries: The Case of Kurdistan Region of Iraq (KRI). PhD thesis, University of East London.*
- Shareef, S. Jahankhani, H. Dastbaz, M., (2012). E-Government Stage Model: Based On Citizen-Centric Approach in Regional Government In Developing Countries. International Journal of Electronic Commerce Studies, Vol 3 (1), pp. 145-164.
- Singh, S., and Singh, K., (2011). E-Governance: Information Security Issues, International Conference on Computer Science and Information Technology (ICCSIT'2011) Pattaya Dec. 2011.
- Siponen, T. M., and Oinas-Kukkonen, H., (2007). A review of information security issues and respective research contributions. ACM SIGMIS Database: the DATABASE for Advances in Information Systems, Volume 38 Issue 1, February 2007, Pages 60-80, ACM New York, NY, USA.
- Spanos, G. and Angelis, L., (2016). The impact of information security events to the stock market: A systematic literature review. Computers & Security, Vol, 58, pp 216–229.

- United Nations (2012). E-Government Survey 2012, E-Government for the People, Department of Economic and Social air. Available at: file:///C:/Users/shareef/Desktop/E_Gov.%20Security/E-Gov.%20survey_MUHIM%20page%2063.pdf. (Accessed on: 23/05/2014).
- United Nations (2012), Department of Economic and Social Affairs (2012). E-Government Survey 2012. E-Government for the People. ISBN: 978-92-1-123190-8. http://unpan1.un.org/intradoc/groups/public/documents/un/unpan048065.pdf (Accessed on 10/11/2016).
- Wang, J. (2009). E-government Security Management: Key Factors and Countermeasure, in the proceeding of the Fifth International Conference on Information Assurance and Security.
- Webb, J. Ahmed, A., and Maynard, B. S., (2014). A Situation Awareness Model for Information Security Risk Management. Computers & Security, Vol. 26. No. 1, pp 56-62.
- Yuan, T., and Chen, P., (2012). Data Mining Applications in E-Government Information Security, 2012 International Workshop on Information and Electronics Engineering, Volume 29, 2012, Pages 235-240.
- Zhou, Z., and Hu, C., (2008). Study on the E-government Security Risk Management, IJCSNS International Journal of Computer Science and Network 208 Security, VOL.8 No.5, May 2008.
- Zu’bi, H. M., and Al-Onizat, H. H., (2012). E-government and Security Requirements for Information Systems and Privacy (Performance Linkage), Journal of Management Research, Vol 4. No.4.

الملخص

تطور تكنولوجيا المعلومات والاتصالات و النمو السريع لاستخدام الإنترنت سهل استخدام الخدمات الحكومية في كل من القطاعين العام والخاص. وبالتالي، يمكن للمستخدمين بسهولة استخدام الخدمات المتاحة من الأماكن في الوقت الذي هي مريحة لهم عبر الإنترنت، في أي مكان وزمان. من ناحية أخرى، جنبا إلى جنب مع وجود الإمكانات الإيجابية، ينطوي الحكومة الإلكترونية أيضا علی التهديدات والمخاطر. لذلك، الحكومة الإلكترونية يجب أن تكون آمنة مع تطویر التكنولوجيا ، لیتسنی المستهلكين متابعة إجراءات معاملاتهم الخاصة بامان. الإدارة الفعالة لأمن المعلومات هي عامل رئيسي للاستعداد، لمختلف المستهلكين لاستخدام خدمات الحكومة الإلكترونية سوف تعتمد إلى حد كبير على الثقة لديهم على أمن المعلومات. تستعرض هذه الورقة ويناقش التهديدات والمخاطر الأمنية في الحكومة الإلكترونية أيضا توفير عوامل النجاح الحاسمة قد يساعد على الحد من المخاطر والتهديدات لأمن المعلومات في نظام الحكومة الإلكترونية.