IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 19, Issue 1, Ver. IV (Jan.-Feb. 2017), PP 04-07
www.iosrjournals.org

Study and analysis of E-Governance Information Security (InfoSec) in Indian Context

Deven C. Pandya[1], Dr. Narendra J. Patel[2]
[1]*(Ph.D. Scholar, Department of Computer Application, UVP Engg. College/ Ganpat Uni.,Kherva, Guj. India)*
[2]*((HOD, Department of Computer Application, UVP Engg. College/ Ganpat Uni.,Kherva, Guj. India)*

Abstract: *The purpose of the study is to explore and find a research gap in E-Governance Information Security (InfoSec) domain in Indian Context. The study identifies the research gap in E-Governance InfoSec domain and substantiates given research gap with relevant literature review. The study outcomes clearly depict the requirement of research in the field of InfoSec in e-governance domain in a country like India.*

Keywords: *E-Governance, Information Security, Risk Assessment, Vulnerability, Threat*

I. Introduction

The paper title “Study and analysis of E-Governance Information Security (InfoSec) in Indian Context” requires the review of literature broadly in two directions:
1. E-Governance
2. Information Security.

E-Governance is the public sector’s use of information and communication technologies with the aim of improving information and service delivery, encouraging citizen participation in the decision-making process and making government more accountable, transparent and effective.[1]. Information security, at times, shortened to InfoSec, refers to the processes and methodologies which are designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption.[2]. After a thorough literature review, we have identified following statements leading to the research gaps in the E-Governance InfoSec domain in Indian Context.

- Information Security in E-Governance is different from E-Commerce.
- Information Security is important for successful E-Governance implementation and there is InfoSec risk associated with E-Governance projects.
- Non-Technical factors are important contributors in InfoSec Risk. Understanding its impact on E-Governance InfoSec is essential.
- Absence of comprehensive E-Governance InfoSec Model for a developing country like India which can cover technical as well as nontechnical factors of Information Security risk
- A model driven InfoSec solution is more effective and efficient.
- Analysis and assessment of E-Governance InfoSec Risk is essential. Soft computing techniques like Artificial Neural Network (ANN), Genetic Algorithm, Bayesian network and Fuzzy Systems etc. are very useful for InfoSec Risk assessment.

In the first section, the identified statements are linked with relevant literature survey while the second section contains the conclusion part of the study.

II. Research Gap and Literature review

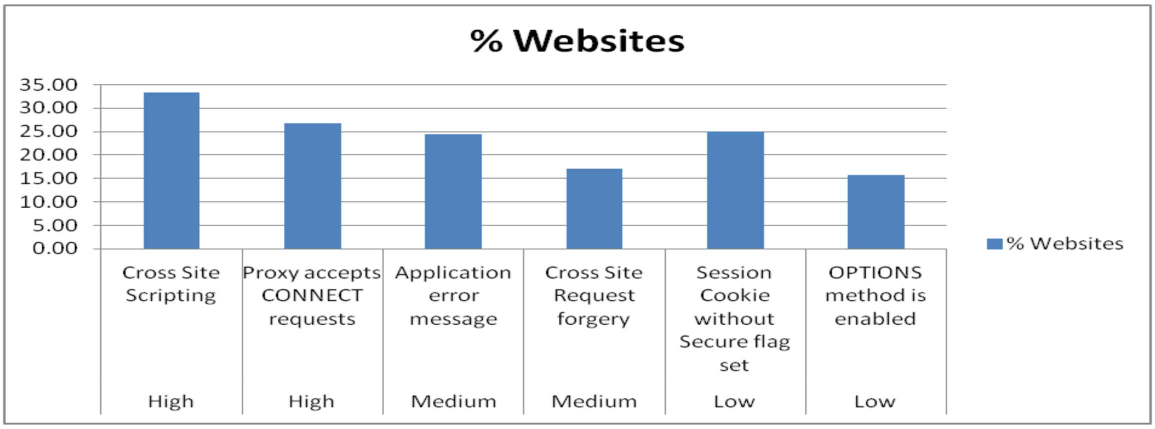
- **Information Security in E-Governance is different from E-Commerce**

There is ample substantiation to support this statement. E-Governance Information Security is different from E-Commerce Information Security since, in e-Government, almost all the data are highly security-sensitive. For example, in the case of E-Governance, a person’s medical record and personal data are more important than in the scope in e-commerce due to sensitive and private nature of data. From the technical point of view, there is not much difference between E-Governance and E-Commerce but the difference lies in the process, strategies, and judicial factors. E-Governance process is more sensitive than the E-commerce process.This is clear when considering that the penalty of misuses of stored citizen data is more crucial than in the scope in e-commerce [3]. The public sector is highly sensitive towards any security incident although such an incident might not be related to E-Government but it can have a negative impact on the implementation of E-governance. Apart from this Government operates in a different environment from the Private organization and hence requires a different approach towards InfoSec.[4] Another crucial reason is that InfoSec requirements are not very clear in the minds of authority managing and approving E-Governance projects while it is more or less clear in the case of private entity running E-commerce application. Hence, we need a different approach for E-Governance InfoSec.

- **Information Security is important for successful E-Governance implementation and there is InfoSec risk associated with E-Governance projects.**

Information security is a key to the successful E-Governance implementation. Since a critical barrier in implementing e-Governance is the privacy and security of an individual's personal data that he/she provides to obtain government services[5]. E-Governance projects are affected by many vulnerabilities and threats. According to the research, 81.6% E-Governance websites from 212 different countries were vulnerable to the cross-site scripting and SQL injection threats.[6] According to the study in Asia 85.44% E-Governance websites were affected with XSS or SQL injection vulnerabilities.[7] According to the E-Governance web security audit study conducted in Gujarat, Indian context high impacting vulnerabilities like Cross Site Scripting and Proxy accepts CONNECT requests etc. have been found in more than 26% websites/web applications. High impacting vulnerabilities like ASP.NET Padding Oracle Vulnerability and Microsoft IIS tilde directory enumeration have been found in more than 13% websites/web applications. Medium impacting vulnerabilities like cross-site request forgery, user credential sent in clear text etc. have been found in more than 14% websites/web applications. From the same study, the given graph is prepared to depict top two vulnerabilities found in Government websites among each severity group viz. High, Medium and Low.[8]

Chart 1



Apart from E-Government implementation, effective InfoSec is essential from State and National security aspect. Effective InfoSec will protect against the threats like Cyber terrorism, state sponsor hacker groups applying attack methods like distributed denial of service, Advance Persistent Threats(APTs), spear-phishing etc. Spear Phishing is targeting a specific individual or small group of people within the Government organization to obtain sensitive information.

- **Non-Technical factors are important contributors in InfoSec Risk. Understanding its impact on E-Governance InfoSec is Essential.**

Based on literature review it can be substantiated that Non-Technical Factors like security policy, security culture, user awareness, computer literacy are equally important factors in contributing security risk related to E-Governance. In Indian e-governance scenario, however, the security aspects are not being taken so seriously. In a large number of cases, it is not difficult to see that the decision-makers in the government prefer to compromise when it comes to high-end technology adoption, implementation, and maintenance [9].When designing e-government projects, the government tends to think about the security of the system, but not the privacy of the data. Security in the minds of the government is achieved through strengthening infrastructure, but they often overlook the human dynamic [10].The study on non-technical perspective in health informatics indicated a significant positive relationship between InfoSec Management and security policy, organizational culture and human behavior actions.[11] Human dynamic is part of non-technical factors affecting InfoSec. The behavior of the end user can expose a system to security threats. Organizations should address the human side as well to fully implement information system security otherwise security will be incomplete and the system remains susceptible to attack.[12]. It indicates that InfoSec in E-Government depends on technical as well as non-technical factors.

- **Absence of comprehensive E-Governance InfoSec Model for developing country like India which can cover technical as well as non-technical factors of Information Security Risk**

It is evident that there is the absence of specific model related to E-Governance Information Security risk assessment in developing countries which will cover technical as well as non-technical factors. Literature review divulged that there is the absence of InfoSec model in India which can cover technical and non-technical factors of Information Security Risk. Apart from this, we have seen many studies depicting the importance of non-technical factors in InfoSec. Author N. Alharbi in his research concluded that there is a lack of comprehensive E-Governance InfoSec model which will cover technical as well as non-technical factors in developing countries.[13].

- **A model driven InfoSec solution is more effective and efficient**

There is an increase in InfoSec threat despite the fact that good InfoSec practice is followed by security professionals. The topmost threat comes from the hacker and there is a research need for a more effective solution against the hackers.[14]The model driven InfoSec solution is more effective and efficient than a conventional solution.[14] Sabri in his research established new InfoSec Model. The model was established in the context of Dubai. The model was useful for assessing the level of security readiness of the Government Department. As a future work Sabari suggests to develop a mathematical representation of the model and converting that model into the framework. [15]The model is a conceptual model and we want a more practical model which will effectively assess and predict the risk. Gangadhar in his research developed the same type of multi-layer InfoSec model in the Indian context. Again this model is a useful model but it is a conceptual model and serves as a checklist to measure security readiness of the Government Department. [16]

- **Analysis and assessment of E-Governance InfoSec Risk is essential. Soft computing techniques like ANN, Genetic Algorithm, Bayesian network and Fuzzy Systems etc. are very useful for InfoSec Risk assessment.**

Literature review shows that the statistical model effectively analyzes the relations between threat, vulnerability, and risk relation but the majority of the research studies were not carried out in the E-Governance context. Our The literature review shows that soft computing techniques like Fuzzy systems, Artificial Neural Network (ANN), Genetic Algorithm etc. are useful in evaluating and predicting Risk associated with Information Security. InfoSec Risk assessment is an important assessment method and decision mechanism in the process of making information security system. The risk evaluation is a process of computing risk value by risk assessment. [15]At present, the methods of security risk evaluation for e-government information system can be divided into three forms: quantitative, qualitative and semi-quantitative. In future research, the trend may be the development of models with the application of soft computing techniques such as Artificial Neural Network(ANN), fuzzy systems, genetic algorithm, support vector machine, rough sets, gray sets, and Bayesian network. The hybrid model may also be developed by integrating two or more existing soft computing models [17]. Other studies also reveal the effective use of the artificial neural network, genetic algorithm, Bayesian network etc. for effective risk assessment. Author R. Sarala constructed Dynamic Bayesian network model to identify multistage attacks. This model is helpful in detecting the uncertain relationship associated with the risk event. [18]. Author Alireza T. applied the genetic algorithm for risk assessment as well as risk reduction. [19] Ahmed U. in his study adopted multi-layer InfoSec model developed by Sabari [15] and modified it to make it more practical risk assessment model. He developed this model using Artificial Neural Network (ANN) and fuzzy techniques. [20] Author Nadir in his study demonstrated fuzzy technique and its application in E-Government security. He further concluded that fuzzy set theory is very useful for evaluation of E-Government Security. [21]

III. Conclusion

With the above study and analysis, it can be concluded that there is an ample scope of research in the field of InfoSec in E-Governance domain in the developing country like India and there is a scope of development of more practical and comprehensive InfoSec model. After thorough literature review following facts emerged to substantiate above statement a) E-Governance InfoSec requirement is different from E-Commerce InfoSec requirement. E-Governance InfoSec implementation required a different approach from E-Commerce.b) E-Governance implementation is not successful without proper InfoSec implementation. c) Non-Technical factors are equal contributor to InfoSec threats and there is a lack of comprehensive model which can cover technical as well as non-technical factors in the developing countries d) Model-based InfoSec solution is more effective and efficient approach than any conventional solution. e) Periodic risk assessment and evaluation is necessary for E-Governance. There is a need for the development of InfoSec model for E-Governance risk assessment using soft computing techniques like artificial neural network, fuzzy systems, genetic algorithm, dynamic bayesian in the developing countries like India.

References

[1]. UNESCO, "E-Governance," UNESCO, 2001. [Online]. Available: http://portal.unesco.org/ci/en/ev.php-URL_ID=3038&URL_DO=DO_TOPIC&URL_SECTION=201.html. [Accessed 14 July 2016].

[2]. SANS Institute, "Information Security Resource," SANS, [Online]. Available: https://www.sans.org/information-security/. [Accessed 14 July 2016].

[3]. M. Wimmer and B. v. Bredow, "A Holistic Approach for providing security solutions in E-Government," in 35th Hawaii International Conference on System Sciences, Hawaii, 2002.

[4]. S. Alfawaz, L. May and K. Mohanak, "E-Governace Security in developing countries:A managerial conceptual framework," International Research Society for Public Management, 2008.

[5]. P. Mittal and Amandeepkaur, "E-Governance - A challenge for India," International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), vol. 2, no. 3, March 2013.

[6]. P. P. Hector D, "e-Government: Security Threats," IEEE Computer Society e-Government STC, 2012.

[7]. R. Alshboul, "Security and Vulnerability in E-Governance Society," Contemporary Engineering and Sciences, vol. 5, pp. 215-226, 2012.

[8]. Pandya Deven, N. J Patel, "AN E-GOVERNANCE WEB SECURITY AUDIT," International Journal of Computer Engineering and Applications, vol. IX, no. VI, June 2015.

[9]. S. K. Shailendra Singh, "E-Governance: Information Security Issues," in International Conference on Computer Science and Information Technology (ICCSIT'2011), Pattaya, 2011.

[10]. Dr Neeta Shah, "Securing E-Governance: Ensuring Data Protection and Privacy," Ahmedabad, 2012.

[11]. M. S. H. Abas Habib Imam, "The impact of non-technical security management factors on InfoSec Management in Health Informatics.," International Journal of Information Technology and Business Management, vol. 26, no. 1, June 2014.

[12]. M. M. Z. Taurayi Rupere, "Towards minimizing human factors in End-User Information Security," International Journal of Computer Sciences and Network Security, vol. 12, no. 12, December 2012.

[13]. Alharbi, "E-Government Security Modeling: Explain Main Factors and Analysing Existing Models," International Journal of Social, Management, Economics and Business Engineering, vol. 7, no. 9, 2013.

[14]. N. B. I. A. H. A.-B. Said K. Al-Wahaibi, "Information Security Solutions Status and the Roadmap for Future Requirements," Journal of Information Assurance & Cybersecurity, 2011.

[15]. Sabari, "A multi-layer model for e-government," 2008.

[16]. B. Gangadhar, "An MULTI-LAYER STRUCTURE FOR INDIAN E-GOVERNANCE INFORMATION SECURITY," International Journal of Engineering and Technology Research, vol. 1, June 2012.

[17]. M.-C. Lee, "Information Security Risk Analysis Methods and Research Trends: AHP and Fuzzy Comprehensive Method," International Journal of Computer Science & Information Technology (IJCSIT), vol. 6, no. 1, February 2014.

[18]. K. M. G. Sarala R, "Information Security Risk assessment under uncertainty using dynamic bayesian networks," International Journal of Research in Engineering and Technology, vol. 3, no. 7, May 2014.

[19]. R. D. Alireza T, "Genetic Algorithm Approach for Risk Reduction of Information Security," International Journal of Cyber-Security and Digital Forensics, vol. 1, no. 1, pp. 59-66, 2012.

[20]. U. Ahmad, "Evaluation of Security issues applied to an electronic Government computer center model," 2011.

[21]. O. I. A. I. A. Y. Nadir O, "Security in E-Government using fuzzy methods," International Journal of Advanced Science and Technology, vol. 37, December 2011.