Secured And Sustainable E-Governance: Hedging The Risk By Cybersecurity

Bhubaneswari Bisoyi, Biswajit Nayak, Biswajit Das

Abstract: In the present scenario, it has become very challenging to mend the relationship within a community. Therefore, the government has taken controlling steps through e-governance. By introducing stringent rule and regulation for controlling the circulation of data and securing it under the e-governance. The research methodology used in this research paper is based on a content analysis of secondary data. This research paper focuses on the best practices followed for the security of information and different models of e-governance. This paper also highlights the security technologies that protect the data from being used wrongly. The security technology that protects from abnormal activities and provides authentication has also been discussed in this research paper. The essential factors for developing strong cybersecurity is to have an immune infrastructure that shall provide better security against threat and cyberattacks. This paper also focuses on the classification of the user's communities for e-governance and the steps taken by each community for hedging against cyberattacks.

Index Terms: E-governance, Cybersecurity, Information and Communication Technology, Sustainability, E-Advocacy, Mobilization

1 INTRODUCTION

This mounting increase in the internet and mobile connection has created interest among the consumers to exploit a new mode of access towards seeking a wide range of information. They have increased their expectation for wanting more information and services to flow in from the government and from a business organization to satisfy their community, profession and family, thereby creating a new buzz word called e-citizenship. With globalization, a shift towards the use of information system that has led for increased disposition of IT by the government and this is supported by the introduction of the World Wide Web in the nineties. With the rise in global population had also led to a rise in the number of internet and mobile connections. The primary concern by the government is more focused on the security of the information and the technology that is shaping automation and computerization. ICT tools are being used implemented for securing the connectivity, networking, and system setups for delivering information and services. The IT policy document has been outlined by every state government by the implementation of an IT task force. The It policy has been set for both organization and citizen agreements are displayed on the government website Alhomode et al. 2012, Anandakrishnan 2003 [1] [2]. The term e-governance refers to the application of information and communication technologies by administrative agencies such as government for the several reason like rapid and faster delivery of community services, refinement of internal efficiency, Interchange of information between citizens, community, government, and other related departments, Cost reduction and maximizing the profit level, Re-building of government processes.

- *Bhubaneswari Bisoyi, PhD in Management, Assistant Professor in Management Studies at Sri Sri University, Cuttack, Odisha, India. bhubaneswari.b@srisriuniversity.edu.in*
- *Biswajit Nayak, Assistant Professor, Faculty of Management Studies, in Sri Sri University, Cuttack, Odisha, India. Mr Biswajit Nayak biswajit.n@srisriuniversity.edu.in*
- *Biswajit Das, Professor at KIIT School of Management, KIIT University, Bhubaneswar, India.*
- *biswajit@ksom.ac.in*

The commonly accepted delineation is: E-governance is the solicitation of information and communication technologies to transmute the competence, usefulness, transparency, and responsibility of informational and operational exchange within administration, between government, and agencies belonging to different levels such as national, state, central, citizens and business and to enable citizens to access and utilize the information (Jaju, 2003). There are similarly limitless ways to apply information and communication technology for providing an efficient and effective solution to each individual by protecting the information against security threats Bisoyi and Das (2016) (2018) [3][4].

2 E-GOVERNANCE IN INDIA

The models of e-governance have been developed based on primary and secondary research and have been examined based on several factors like societal development of knowledge and applications, Applicability of e-governance process on information and connectivity between e-governance and ICT. There does not exist any definite model that fits into the dynamic change globally. The developing countries have been experimenting with different models and trying to find out the best fil model for e-governance. Few of these models have used simple technology but the results are significant on the way information is distributed and its applicability on the society. There are several models prescribed such as Broadcasting Model, comparative analysis model, Critical flow model, E-Advocacy model, and Interactive Access Model (Juillet Allen, 2010), [10] [11]. This broadcasting model is a concept which is based on the propagation of large amount of data related to governance-related information that is available to the public but to spread to a broader public domain by means of ICTs. The application of this model by using technology can help in reducing the information failure situation. This model has the provision of providing alternate channels that provide information related to the changes occurring in e-governance and validate the information that is also available from other means as explained in Figure.1 Nath, 2000 [14].

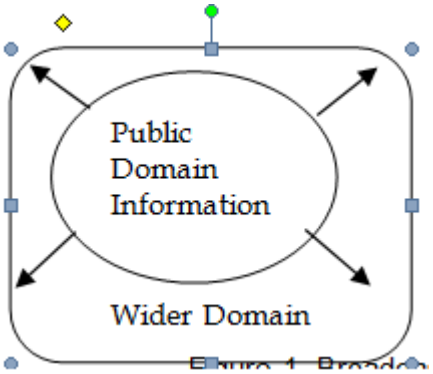

Figure 1. *Broadcasting model*

The broadcasting model transmits the following information to the citizens that help them for having the exact information about e-governance. (1) The details of government officials are readily available such as name and other contact information, (2) The approved government plans, financials details such as budget, expenditure and report of performance, (3) Putting the major judicial decision which is of value to the citizens and can have a significant impact on their future decision. This model of e-governance has very high potential. This model is basically applicable in the case were comparison is done between bad governance and good governance. This comparison helps in identifying the exact aspect of bad governance, reason and the people involved in it and also to improve the situation. The essence of this model is that it continuously integrates practices and using these benchmarking for evaluating other practices of e-governance. This models strength lies in the digital network that has an infinite capacity to store a variety of information and recover and diffuse it rapidly across all barriers both hierarchical and geographical as mentioned in Figure 2 Nath, 2000 [14].

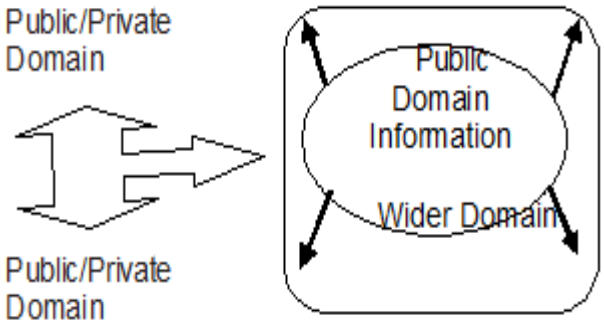

Figure 2. *Comparative analysis model*

The target audience for this critical model includes media, both affected and opposition parties, judicial matters or the public as depicted in Figure 3 Nath, 2000 [14]. This model is more evolved and informative as compared with other models. This model can be used by the different organization based on the requirement of the information.

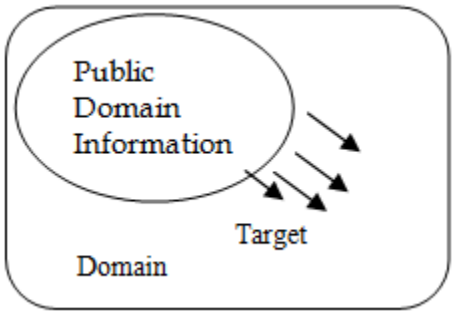

Figure 3. *Critical Flow Model*

The E-Advocacy model deals with forming virtual communities based on interconnectivity between them by sharing similar values and concerns, and these communities play a vital role in forming a linkage that supports real-life groups for related issues as displayed in Figure.4 Nath, 2000 [14].

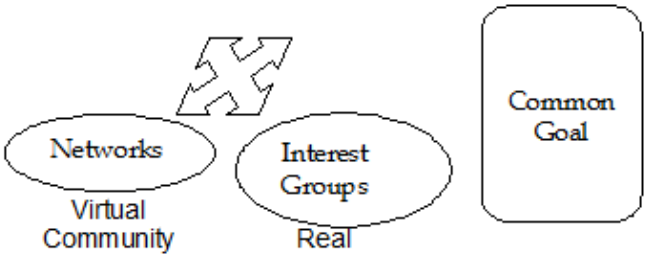

Figure 4*. Mobilization Model*

This model is helpful in building a global alliance by providing a public platform to individuals and communities A community shall develop a sense of belongingness and may find a supporter for activating effective actions through this model. This model of e-governance is considered to be the consolidation of all the above- discussed models and provides a path for one-to-one and participation of individuals in the process of governance. This model utilizes the potentiality of ICTs and it is fully leveraged. It can be used to begin a collaborative model of the communication channel with eminent policymakers and other individuals belonging to the planning commission. Figure.5 shows the process (Nath, 2000) Dwivedi.

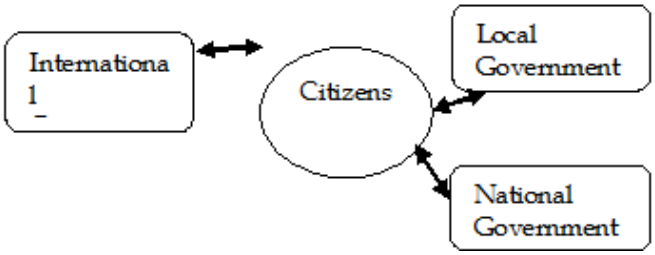

Figure 5. *Interactive service model*

3 DISCUSSION AND RESULT

With forming rule and regulation for governing the data and information available to the public and regulating it by e-governance. It also essential to manage the risk attached with information and this can be typically done by implementing assurance activities. The definition of assurance that has been coined by National Institute of Standard and Technology (NIST) as being ground for confidence focusing on four security goal that consists of integrity, accessibility, privacy, accountability for implementation (NIST, 2013a). In addition to this cybersecurity has been defined by NIST as a method designed for shielding information from being detected, averted, and reacting to attacks. The intricacy of cybersecurity basically caused by the people and very less from the device used for accessing information (Kumarwad, 2016) [13]. The definition of cybersecurity as per National Initiative for Cyber Security Careers and Studies states that it an activity or progression, skill or capability of protecting information and the communication system against the unauthorized use, modification or mistreatment. Due to the unending publication of the various high-profile security fissures, organizations are focusing more and looking for different techniques for improvising their assurance to secure their brand and reputation, also emphasize on the financial security of the organization. The major types of threats in the cyber world are mentioned in Table 1, Dwivedi, 2017 and Katzan,2016 [7] [12].

TABLE 1

MAJOR TYPES OF THREATS

Threat	Description
Cyber Stalking	The act of harassing, stalking and threating individuals through online or computer or internet as a medium of communication. It may be a threat, accusation, sexual harassment.
Child Pornography	The act of developing image or videos of a minor under the age of under-18 involved in sexual conduct through the internet. Internet is the appropriate platform for learning and fun but still accessing illegal sites creates risk for children.
Forgery and Counterfeiting	The process of forgery and counterfeiting using a computer which appears as an original document. It is possible through advanced software and hardware.
Software Piracy and Crime related to IPRs	The act of illegal reproduction and distribution of software for individual use or business piracy treated as IPR infringement crime.
Cyber Terrorism	The act of large-scale disruption of computer networks through various ways like computer viruses on the Internet. In other words the use of the public network to destroy one's objective.
Phishing	The act of capturing personal and sensitive information of anyone else through e-mail. The information may include username, password, debit card, credit card, etc. Phishing may have several forms like Vishing, Smishing.
Computer Vandalism	The act of destruction graffiti and defacement directed towards any property un-authorized. Destruction of computer resources using physical force or through malicious code.
Computer Hacking	The act of modifying software as well as hardware to fulfil the requirement of the intruder. They are classified into various types like a white hat, black hat, grey hat and blue hat.
Creating and distributing viruses over the internet	The act of creating program intentionally and inserting into the user's system without the knowledge of the user to affect files, boot sector and/or replicate itself.
Spamming	The act of passing commercial and unsolicited bulk message through the internet. An e-mail is treated as spam if it is mass-mailing, anonymity and unsolicited. These are only waste mailbox memory space.
Cross-Site Scripting	The act of injecting malicious script (Client-Side) into a trusted website. Afterwards, the malicious script gets access to the sensitive information to fulfil the personal interest.

With the recent progress in cybersecurity dealing with the issues is a major challenge for the organizations [15] [16] [17]. Therefore, organization broadly follow four major approaches for providing reasonable assurance against these cybersecurity issues:

a. Multidimensional Approach: The emphasis on the use of this multidimensional approach for legislation of cyber-crime is a vital facet. In other words, a multidimensional approach is needed to prevent the malevolent use of the cyberspace, comprising of initiatives to harmonize legislation related to cyber-crime and to stimulate penalties for criminal activities and to progress globally in the improvisation of e-governance legislation.

b. The approach of Securing Information: One of the preventive approaches for securing an information system is an effective prevention mechanism. As per the definition of Committee of Sponsoring Organizations of the Tread way Commission (COSO, 2015) information system is defined as a set of activities that involves people, data, processes and technology that enables organizations to communicate globally. It is vital to create a security system that protects the information of both public and private sector including the promotion of advance security mechanism and technological advancement.

c. The approach of Cooperative Policy Making: The mechanism of cooperative policy mechanism and timely warning of spasms are considered for the revealing. Multidimensional initiatives to the use of cyberspace in a malicious manner include the development of a mechanism of cooperative policy and warning in the early stage of cyber-attack by exchanging information between the public and private sector.

d.Program for Crisis Management: This is basically needed for designing of a stronger infrastructure for information, management of the crisis, and efforts for policy-making and justice. The concern for cybersecurity cannot be dealt with easy due to rapid market forces or by regulations but requires a solution that resolves the issues of cybersecurity with assurance.

4 CONCLUSION

The technique of handling the future risk in information technology and refuting the present and past manifestations through cybersecurity is the main focus in this research paper. The future risk management needs to have an insight of all the vulnerabilities that have occurred in the past and the finding ways to provide a solution to it with a reasonable cost attached with it. This research paper has highlighted the various security threats and the techniques used for defending it. The security of e-governance should be done both internally and externally by forming policies. The cybersecurity controlled by the companies through appointing internal auditors who collaborate with the IT department and try to understand the difficulties and issues faced by companies. The tool to accomplish good governance is considered to be e-governance. The improvement in the field of service delivery, broadcasting of information, accountability is needed for sustainable e-governance.

5 REFERENCES

[1] S.M.Alhomod, M.M. Shafi , M.N. Kousarrizi, , F.Seiti ., M. Teshnehlab, H. Susanto, Batawi, Y. A. (2012). Best Practices in E-government: A review of Some Innovative Models Proposed in Different Countries. International Journal of Electrical & Computer Sciences, 12(01), 1–6.

[2] M. Anandakrishnan, (2003), "E-Governance for Improved Services: Choices Made by Tamilnadu", in Vayunandan, E. and Mathew, Dolly (ed), Good Governance Initiatives in India, Prentice- Hall India, pp 121-126

[3] B. Bisoyi , B. Das (2016) Necessitate Green Environment for Sustainable Computing. In: S. Satapathy , K. Raju , J. Mandal , V. Bhateja (eds) Proceedings of the Second International Conference on Computer and Communication Technologies. Advances in Intelligent Systems and Computing, vol 380. Springer, New Delhi.

[4] B. Bisoyi , B. Das (2018) An Approach to En Route Environmentally Sustainable Future Through Green Computing. In: S. Satapathy , V. Bhateja, S. Das (eds) Smart Computing and Informatics. Smart Innovation, Systems and Technologies, vol 77. Springer, Singapore.

[5] E. Çayırcı, and L. Özçakır (2016). Modelling and simulation support to the defence planning process. The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology, 14(2), pp.171-180.

[6] J. Condit Fagan, and B. Fagan, (2001). Citizens' access to on-line state legislative documents. Government Information Quarterly, 18(2), pp.105-121.

[7] S. Dwivedi, (2017). "E-governance transforming rural India: An analysis of major projects and initiatives". SOCRATES, 5(1), p.74.

[8] T. Halder, S. Karforma, and R. Mandal (2014). E-governance Data Security using Steganography, Concepts, Algorithms and Analysis. International Journal of Applied Science and Engineering, 2(1), p.41.

[9] S. Jaju, , (2003), "Information Technology and Governance", in Vayunandan, E. and Mathew, Dolly (ed), Good Governance Initiatives in India, Prentice-Hall India, pp 70-85

[10] B. A Juillet Allen, L. Paquet and J. Roy (2001), E-governance & Government On-line in Canada: Partnerships, People & Prospects, Government Information Quarterly, Volume 18 .Issue 2.Pages 293-307

[11] K . Tayene, L. Jung woo (2001), "Development Fully Functional E-government: A Four-Stage Model", Government Information Quarterly. 18.

[12] H. Katzan, (2016). Contemporary Issues in Cybersecurity. Journal of Cybersecurity Research (JCR), 1(1), pp.1-6.

[13] L. Kumarwad, and R. Kumbhar, (2016). E-Governance Initiatives in Maharashtra (India): Problems and Challenges. International Journal of Information Engineering and Electronic Business, 8(5), pp.18-25.

[14] V. Nath, "ICT enabled Knowledge Societies for Human Development", Information Technology in Developing Countries. Volume 10, No. 2, August 2000.

[15] P. Barman and B. iSaha, "E-Governance Security using Public Key Cryptography special focus on ECC", Volume 2, August 2013.

[16] M. Singh and G. Sahu, (2018). Study of e-governance implementation: a literature review using the classification approach. International Journal of Electronic Governance, 10(3), p.237.

[17] P. Suri and N. Sushil (2011). Multi-perspective analysis of e-governance performance: a study of select agriculture related projects in India. International Journal of Electronic Governance, 4(3), p.259.

[18] D. Tobey, P. Pusey, and D. Burley (2014). Engaging learners in cybersecurity careers. ACM Inroads, 5(1), pp.53-56.