Security Metrics and E-Governance Portals

Subhash Chander
Govt. P.G. College
Sector – 14, Karnal Haryana (India)

Ashwani Kush
University College, Kurukshetra University,
Kurukshetra

ABSTRACT

The major problem of modern Indian society is corruption, bureaucracy and security of information systems. Government is trying to provide many basic services online to its citizens. But major success has not been achieved on this side because success rate in implementation of e-governance projects is very low. There are so many security breach cases one can listen and see through various media in the modern society. In this paper certain challenges in implementation of e-governance systems in Indian democratic setup has been discussed. Certain solutions regarding the challenges are also highlighted. Particular security related metrics must be kept in mind while handling e-governance matters. Various Privacy, security and users in e-Governance related issues have been taken into consideration.

Keywords

Security, ICT, metrics, e-governance, threats, vulnerability

1. INTRODUCTION

In the modern age of Information and Communication Technology (ICT) newer services are being made available online to the citizens. The term e-governance focuses on the use of ICTs by governments for its various governance related functions. The potential of networking, Internet and related technologies has transformed government structures and operations.

E- Governance is related positively to rapport government citizen relationship and corruption reduction. Information technology (IT) has the potential to transform government structures and improve the quality of government services. Technology provides two main opportunities for government: (1) improved operational efficiency by reducing costs and increasing productivity; and (2) better quality services provided by government agencies [1]. Every state government is providing certain basic services like driving license, domicile certificate and caste certificate and others online to its citizens. E-government is to enable users to transact business throughout on 24×7 basis and saving the cost and improves government effectiveness [2]. Privacy and security of the these e-governance portals is necessary. Data available on the e-governance portals must be secure and managed properly for its effective use by users of the portal. Privacy and security include the features like privacy policies, authentication, encryption and data management [3]. For security measurements we apply certain metrics. Generally metric is used with respect to time but security metrics is used in different contexts. Two terms namely measurements and metrics are used interchangeably but there is difference between the two terms. Measurements are objective raw data whereas metrics are objective or subjective human interpretations of those data. Measurements are instantaneous snap shots of particular measurable parameters, whereas metrics are more complete pictures, and typically comprised of several measurements, baselines and other supporting information that provide the context for interpreting the measurements [4]. For information system security, the measurements are concerned with aspects of the system that contribute to its security. That is, security metrics involve the application of a method of measurement to one or more entities of a system [4]. There is a need to develop a broad assessment framework model which could give a direction to the assessment and learning's which can go back into the project. At the same time it is very important to develop self-assessment models, which could be used at the conceptualization level itself, of e-governance project [5]. The rest of the paper is organized here as follows. Section 2 presents Challenges & solutions to e-governance implementation, Section 3 gives security metrics in e-governance, Section 4 gives security, privacy and users in e-governance and section 5 presents conclusion of the paper.

2. CHALLENGES TO E-GOVERNANCE AND SOLUTIONS

There are various challenges to the e-governance in every country. But these obstacles become more prominent in case of developing countries. Because instead of having problems related with governance of the society there are certain other major hurdles like education, environment, infrastructure and social problems. India being largest democracy, and second largest in terms of population and having diversified geography itself poses great challenges in e-governance implementation. Mainly such hurdles and problems are divided in to technical, political, cultural and legal problems [6]. These challenges have been categorized into many ways namely technical, political, cultural, social and economical.

2.1 Technical

In case of technical level hindrances infrastructure is stressed that work as a backbone of E-Governance. Technical challenges include interoperability, standardization, privacy and security [7]. Interoperability with existing software and hardware platforms is a key success factor. It is unlikely that available resources can support a full replacement of existing application. Hardware should be fully compatible with future technologies [7]. If it is not feasible to work on the existing infrastructure then one has to think of the procurement of the new hardware or software. Unnecessarily procurement of hardware and software is not possible for developing countries. Infrastructure must provide secure and safe transactions for all the citizens whether illiterate or literate, rich or poor, young or aged. In various applications of e-governance there is requirement of online transactions. All these transactions must be performed in a secured manner which is only possible in case of good and secure infrastructure including hardware and software installations at the sites.

2.2 Political

Political will is necessary in case of secured e-governance in Indian culture. It can be seen that various southern states namely Gujarat, Maharastra, Karnatka, Andhra Pradesh have done well in e-Governance field as compared to various other northern states including Punjab, Haryana, Himachal Pradesh etc. One of the important reasons in making such a progress is political will of the head of the states. This is only possible in case of

transparent, strong and powerful political system and politicians. E-government projects can easily be put at risk if projects lack government support, if a solid information infrastructure is not developed [8].

2.3 Cultural

In case of Cultural barriers the responsibility lies on the users themselves. Users may lack in confidence, they may be facing threat regarding their important data and there may be obstacles to use IT equipments. In Indian scenario there is lack of proper law in case of breach of security. Present offensive morphed images and videos loaded on various major social networking sites have conformed this. Government has ordered to block such sites [10] that have tried to increase communal tension in India. When new infrastructures are interconnected, vulnerabilities might arise from the common links, failures might propagate through the different systems, intrusion and disruption in one infrastructure might provoke unexpected threats to others. Framework for cyber security and critical information infrastructure protection would entail a national strategy and creation of legal frameworks to curb cyber crime [11]. Security and privacy of personal and financial data is a great challenge in itself. United States have sector based data protection and privacy laws at federal and state levels whereas United Kingdom has a single law covering all departments. At Indian level there are an Indian IT ACT 2000, Indian copyright act, Indian Penal code and Indian Contract act 1872 to deal with data protection and privacy in India [12]. But these laws are not sufficient and staff is not trained for implementing these rules and laws properly. There is a need to have clear cut laws mentioning clearly what type of punishment one will get if he tries to breach the security of the system.

2.4 Social

Social challenges may include accessibility, usability and acceptance. All these attributes depend on the environment prevailed in the country. Certain applications may not be accessible, usable and acceptable by the society in a country. There are various societal differences among various countries. Freedom or censorship on the Internet and its material is such an issue which may or may not be acceptable to society in a particular country. Various social disparities are also one of the major barriers of e-governance. Disparities in Indian society exist at many levels may be caste, creed, religion, human and geographical. Hence there is a need to have policies that concentrate on the social status of citizens utilizing e-governance services. Illiteracy is also one of the biggest barriers in the implementation of e-governance.

2.5 Economical

Economical challenges include costs, reusability, maintainability and portability. Other challenges which can be taken into account are leadership, lack in strengthening and improving coordination, public private partnership (PPP), skilled human resource, monitoring and evaluation [8]. Out of all these challenges security and privacy is major challenge for various rolled out and upcoming e-governance projects in India. E-governance itself is great challenge and poses big opportunities to the general public. The major characteristics which need to be taken care of while implementing e-Governance are quality, accessibility, cost, time, authenticity, confidentiality and security.

3. SECURITY METRICS IN E-GOVERNANCE

In daily life one makes so many security arrangements for assets like home, bike, cars etc. Here idea is to secure assets from outsiders only whereas in case of e-governance one is to secure assets from external as well as from internal sources. Here assets may include data, information, knowledge resources, wisdom, programs and networks. There is need of security from internal or external entities in the system of e-governance. There is need of security against government employees, service operators, commercial organizations, professional hackers and terrorist organizations. Various types of threats may be defacing of the web sites, hacking into servers, Damage to critical databases & applications, Denial of Service attacks and virus attacks. Security metrics can be used to indicate how severe an attack can be when a particular security function fails [12]. Security must be provided in such a manner that basic characteristics are not compromised. Such basic characteristics are Confidentiality, integrity and usability of the information. Every government has its legal and compliance standards to which any e-governance security or information security must comply with. In India Standardization Testing & Quality Certification (STQC) Directorate, Department of IT, Government of India (GOI) is responsible for the STQC services of the IT sector. These services are information security, standards formulation, quality management in IT industry, software Quality evaluation, ITes Quality and IT service management. Information security is mainly divided into three parts namely Management, operational and technical control. Management control includes risk assessment and treatment, security policy, organization of information security, asset management and information system acquisition. Operational control includes human resource, physical and environmental controls, communication and operations management and business continuity planning. Technical control means identification and authentication, cryptographic control, access control and audit and accountability [13]. For e-governance certain certification schemes exist for quality assurance which are five in number and are here as follows.

(1) Smart Card Certification (along NIC)
(2) Bio-metrics Device Certification (along UIDAI)
(3) Website Certification
(4) Information Security Management Systems Certification
(5) IT Service Management Certification [13].

E-government is a tool for fundamental transformation of the way government works, enabling faster, cheaper, more personalized and more efficient service delivery to citizens and businesses anytime and anywhere [14]. Corporate Information Security Working Group reports on the best practices and metrics team subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census suggested thirteen security metrics as follows.

1. Malware protection, including worms and viruses
2. Change management, including patch management
3. Identity and access management, including privilege assignment and authentication
4. Firewalls including workstation, host, sub-network, and perimeter as required
5. Configuration management
6. Basic identity management mechanisms, (authentication, authorization, access control) for access to both physical and electronic assets, are implemented and regularly reviewed.
7. Information security policies are in force for acceptable use, incident Response /reporting, and each of the baseline areas included in this document.
8. Regular monitoring and review is conducted for alert mechanisms, system logs for critical systems, firewall logs, incident reports, configuration violations;

vulnerability assessment results and overall security program.

9. A business continuity plan is implemented and regularly tested. All critical assets are routinely backed up. Ability to selectively restore from backups is tested regularly
10. All users are required to attend security awareness training prior to being granted access to the organization's networks and periodically as condition of continued access.
11. All information security management, technical, and user roles and responsibilities are explicitly assigned and assignments are acknowledged.
12. Compliance with external (legal, regulatory) requirements is regularly demonstrated via internal and external audit. Audit findings are resolved in a timely manner.
13. The practices noted above are required in all third party service level agreements for those parties having access to organizational networks [15].

Out of these thirteen first five are considered as minimum and essentials for Small and Medium Enterprises (SMEs). It is must to concentrate on these first five security metrics for Indian e-governance system and other online information system. According to first one there is need to have one virus or malware protection system. Users also need to be alert for this metrics otherwise one end server may be having full security provisions and on the user side not even antivirus program is available. The tendency behind not having an antivirus is let system first be compromised then one will be alert to remove the virus from the system. Certain patches are available with each antivirus program and rather for each software application since it is not feasible to prepare complete application in one go because of certain limitations and constraints at the time of designing new software. Constraints may be in the form of time, money, features, size etc. Such patches must be utilized to by various e-governance applications and information systems. All patches are available for genuine soft wares that are purchased. Burt in most of the cases this condition of genuine software is not fulfilled. Various authentication mechanisms and privilege assignments must be taken into consideration. Poor authentication may promote unauthorized users to enter into the secured portion of the portal. More privileges given to users may also lead them to those activities which may be utilized by hackers in future for compromising the portals and websites. Firewalls that are used to control the incoming and outgoing network traffic, by analyzing the data packets on the basis of certain predefined rules. Firewall may allow or not certain data packets on the basis of these rules. Hence firewalls, may be hardware or software, are must for each e-governance projects but certain projects lack on this part. Configuration Management (CM) is the technique for improving performance, reliability and maintainability and reducing costs, risks and liability. CM process facilitates orderly management of system information and changes for better results.

4. PRIVACY, SECURITY AND USERS IN E-GOVERNANCE

Certain issues related with the website and web portal are inconsistent Home/ Web pages, missing/ broken links - Site links not working, accessibility requirements as per W3C hardly met, incorrect/ obsolete contents, important buttons/ keys disabled, site map not available, search function not available/ not working [13]. Citizens' concern on privacy of their life and confidentiality of the personal data is an important and serious issue. Privacy and confidentiality has to be highly valued in establishing and maintaining websites. Hence there is need of good cyber /IT policy and that policy must be adhered to which can work as a backbone to get support of citizens. In e-governance applications there is a great demand of security for many important and financial transactions which take place as a routine matter. Each financial transaction requires transactional security. The security and safety of various ICT platforms and critical infrastructures in India must be considered on a priority basis before any e-governance base is made fully functional. Interface of e-governance platform should be usable by all kinds of people may be rich or poor, disabled or elderly people, understandable by non native language people and illiterate people etc. certain security related issues for e-governance are weak application security, missing/ ineffective security policy (E.g., Password policy), mis-configured/ vulnerable systems such as servers, firewalls, etc., improper authentication & access control (access rights & authorizations), inadequate confidentiality/ integrity (credentials transmitted in clear text), risk assessment, inappropriate data backup & archival for disaster recovery and inadequate physical security. The major work on e-governance has been done in the developed countries. Even among developing countries certain democratic scenario is also to be taken into account while developing new e-governance projects for its people. Before developing any e-governance projects, it is must to check affective rate of a particular project. It requires a complete procedure to be adopted for this kind of job. Affective rate here means to know how many people will be affected after implementation of such an e-governance project. It must not happen that certain e-governance project is being developed for handful of users and to sort their problems. Before developing any online system it must have an approximate idea about the number of users. Many online systems in India failed because of the lack of number of users of particular portals. Normally it happened that system fails on the last date of applying online forms. Firstly check the number of affected person and then provide the required bandwidth so that system may not fail on the last dates. Secondly one can have idea from the successful e-governance projects in India. Certain key success factors of e-governance are use of citizen-centric approach in case of services delivery, development of the personalized services and creation of the integrated government portals. Society survey may be done to know which services are mostly desired by people living in rural areas. Rural areas must be the taken into consideration in case of Indian e-governance systems. An agriculture related e-governance project will be best suited for northern India as compared to hilly and eastern areas. Now a day's government and its bureaucratic structure is so much strong that no care is taken for the user. Hence citizen centricity is must and must be kept in mind throughout the stages of the development of e-governance projects. Failure to do this may cause a loss of crores of rupees, which ultimately is the public money. If one knows the target users' then application may be built accordingly and there will more chances of success of such projects. It can be easily determined that what is to be presented and in what form is to be presented. Conclusively user is the centre of all e-governance applications as shown in fig. 1 below.

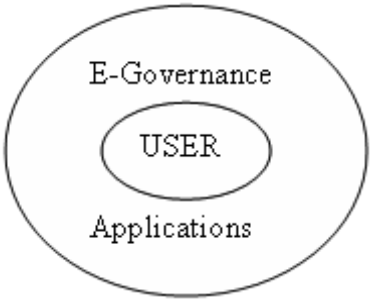

Fig. 1: User and E-Governance applications

4.1 Issues related with e-governance

There are number of issues involved in e-government implementation. The first and the foremost issue to select area, ensure involvement of users, commitment from government authorities at various levels in the hierarchical bureaucratic structure. Moreover after implementation website or portal maintenance of websites for having reliable and up to date information, security and privacy issues as well as the adoption of supporting laws and regulations. Success of the e-government projects depends not only on the good hardware and software but also on the citizens' perceptions of security and privacy issues while performing online transactions. Various positive impacts of the implementation of e-governance on a process can be measured in terms of quality, time, cost and flexibility. Major Goals of implementation of such projects is to improve quality, reduce costs, reduce service time or production time, improve productivity, increase revenue, improve customer service, use IT capabilities and improve competitiveness [2]. Successful implementation of the E-governance requires a change in the mindset of one and all – citizen, executives or the government. With the help of Internet, the government processes can be made efficient, effective, and citizen friendly. There is need for the government to stress in areas like process re-engineering, capacity building, training, assessment and awareness among users. An assessment exercise involves a tedious process, in terms of capacity, time, and resources; if the intention is to assess an e-governance project thoroughly. E-governance projects involve a number of stakeholders, whose expectations from the project needs to be addressed [5]. The beneficial impact of ICT and e-governance on the rural economy and quality of life is very well recognized by one and all. There is a need to maintain a proper database of all the citizens and this job is done by the Unique identity Authority of India (UIDAI) by preparing UID cards of every citizen. That will also help in tackling certain security issues in connection with e-governance. Not only this, users must also accept such systems by heart [8]. Since users are the base of such projects and ultimately projects are to be utilized by them. As soon as ICT infrastructure is increasing the chances of external and internal attacks are increasing. So to keep our data and infrastructure safe there is need to have coordination among various agencies like Fire Brigade, Police, Media and medical services to curb any natural or external attacks by terrorists. There is a need to have sight on the security policies of the e-governance applications.

5. CONCLUSION

Various e-governance applications are being implemented at national and state levels. There is need to have certain minimal security metrics that can be imposed before implementation of any e-governance application. If those are fulfilled then it maybe allowed to work otherwise it must be made compatible regarding these minimal metrics. In various countries many programs, plans, election mandates seems to be very good in the election days. Lack of good leadership, no motivation for doing new work, poor education system and socio economic conditions are some general barriers in the implementation of such plans and programs. Certain technical and other barriers in e-governance implementation have already been discussed in the paper. Certain issues related with e-governance need to be kept in mind for getting success in this area of e-governance. Since E-governance is totally user centered projects hence their feeling, ideas about such projects must be given due weight age throughout the course of action. Also there is a large gap on planning and action and until and unless this gap is not diminished such projects cannot be implemented effectively and country will not be able to make much progress.

6. REFERENCES

[1] Alam S B, Bulbul R,"GSM and ICT Framed E-Governance Incorporated with Network Protection", International Journal of Mobile & Adhoc Network (IJMAN) ,Volume 1, issue 2 (2011)

[2] Guo Liping," Study on Path Evolution and Strategy of E-government in China", IEEE transactions 2011

[3] Chander Subhash, Kush Ashwani," Web Portal Analysis of Asian Region Countries", International Journal of Information Engineering and Electronic Business (IJIEEB), Singapore, Volume 4, Issue 4, Pp 25-32, August 2012.

[4] Okereke G. E., Osuagwu C. C.," A metric model for ranking the security strength of a web page" International Journal of Enterprise Computing and Business Systems (IJECBS) , Vol. 2 Issue 1 January (2012).

[5] Gupta Piyush, "Challenges and Issues in e-Government Project Assessment", Pp 259-262, ICEGOV2007, Macao, China, ACM Press, 2007.

[6] Hwang Min-Shiang, Li Chun-Ta, Shen Jau-Ji and Chu Yen-Ping, "challenges in e-Government and security of information", Information & security : An International Journal, Vol. 15 No.1, Pp9-20 (2004).

[7] Suresh P., "Understanding Challenges in e-Governance", SETLabs Briefings a journal published by Infosys labs, Business innovation through technology, e-governance, Vol. 9 No. 2 (2011).

[8] Mrinalini Shah," E-Governance in India: Dream or reality? ", International Journal of Education and Development using Information and Communication Technology (IJEDICT), Vol. 3, Issue 2, pp. 125-137, (2007).

[9] Mansar Selma Limam," E-Government Implementation: Impact on Business Processes", Innovations in Information Technology, Dubai conference Publications, Pp 1-5, IEEE transactions (2006).

[10] Bannerji Ajay, " India to share Net proof with Pak, over 250 websites blocked", Pp1,Vol 132 No.231, The Tribune , Haryana Edition 21st August, 2012.

[11] Chaturvedi M M, Gupta MP, and Bhattacharya J.," Cyber Security Infrastructure in India: A Study", CSI Publication, Emerging Technologies in E-Government, Pp 70-84, (2008).

[12] Chaula Job Asheri, Yngström Louise, and Kowalski Stewart," Security metrics and Evaluation of Information systems security", downloaded on 31-7-2012.

[13] "E-Governance STQC Role & Responsibilities", a document of, department of IT, Govt. of India

[14] Golubeva A., Merkuryeva I., "Evaluation of Demand for e-Government: the case of Saint-Petersburg"

[15] Information Technology Security Metrics, IT services department, July (2009).