International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 9, September - 2013

Enhance security system of E-governance

Govind Singh Tanwar
Research Scholar
Dept. of Computer Science & Engineering
Suresh Gyan Vihar University
Jaipur (Rajasthan), India

Chitresh Banerjee
Dept. of Master of Computer Application
Suresh Gyan Vihar University
Jaipur (Rajasthan), India

***Abstract* – E-Governance is nothing but use of internet technology as a platform for exchanging information, providing services and transacting with citizens, businesses, and other arms of government. E-Governance provides a sound strategy to strengthen overall governance. It can not only improve accountability, transparency and efficiency of government processes, but also facilitate sustainable and inclusive growth. E-Governance also provides a mechanism of direct delivery of public services to the marginal segments of the society in the remotest corners, without having to deal with intermediaries. This paper deals with the problems and challenges of E-Governance, reasons of E-Government Project Failures, current status of E-Governance related initiatives in India and future prospects of E-Governance in India.**

Keywords: e-governance, security service authentication, one-time password (OTP)

I. Introduction

The concept of e-government started with the advent of government websites in the early 1990s. The system of government is fixed, static hierarchical regulated, whereas web is dynamic, flat and unregulated. Government's function is liked mammoth, where one hand does not know what the right hand is doing [1]. With the development of Information Technology and increased dependence on the internet as a transaction medium and the development of adequate infrastructure and regulations, government websites soon developed into a highly potential channel for supporting a frontend and back end applications [2].

In India there is uneven progress. Many government departments and states have planned or implemented some form of e-government initiatives. For example, in Andhra Pradesh and Karnataka there are three to four departments that have computerized extensively with online delivery of services at all their offices in the state[3]. In five to six departments, electronic delivery of services is at a pilot stage of implementation. In most of the remaining 50 departments websites have been created but there is no move to offer online services. Although the few departments that have gone online have demonstrated remarkable improvements in service delivery, most of these projects remain relatively isolated success stories without structure for scale-up and replication. A recent study on e-government readiness classified Indian states into four groups, indicating that 18 out of 26 states have made very little progress on e-government [4].

There is a useful discussion found throughout the reviews that examine the current framework of e-governance of India. Current framework has been developed either by traditional framework or by technologists focusing on encrypted data. The major limitation of existing framework is that no any physical authentication is done or no any backup and easy discovery is use in. The existing framework does not cover all aspects of secure login or authorization; they are not general enough to describe fully the secure and backup process in a way which will assist the development of new framework techniques [5].

Current status of e-Governance in India

II. e-Governance Present Security System

In the e-governance security system is also work as on the old system of security. Here which only prescribed the advanced security system but that is not presently in working. If the e-governance is want to upgrade the our security system with high level of security system, high level of security system implemented with the help of biometric scanning. If the e-governance is used the biometric system of the UID then the e-governance system is going to secure. But presently two different stages is that

a. Registration or Login

b. One-time Password (OTP)

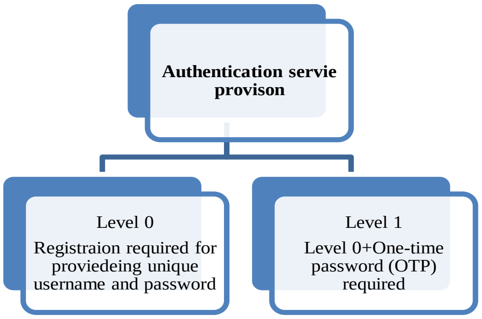
Authentication servie provison
Level 0
Registraion required for proviedeing unique username and password
Level 1
Level 0+One-time password (OTP) required

Figure 1: Govermental Authentication service provision [1]

1. **Registration or Login** – In this process, if the user is login at first time then they will required to registrated him/her self with the help of registration form and give the some basic details like name, address, mobile no etc. this information is not verified by the system and user will easy going to registred on the web portal and access all the information. if user is already registered on this web portal then his/her required the fill the user name and password that is given at the time of registration and after that he/she will be able to access all the government information directly.

2. **One-time Password** – At present the e-governance is made a different web portal with the name of e-parmaan. In the e-parmaan portal firstly the user will

required to registered him/her self with the basic information and also a another option is One-time password. It's meaning that after fill all the information, one tempary password is send on the user's mobile no that is entered at time of registraion. This password is alive only for 3-5 mint. After that this is automatically dead. This is just a system generated password with 4-5 digit. Each in every time the password is changed. After receiving the password the user will be able to work with our login. The beniftit of this process at-leat the user's mobile is verified by the system.

III. Different Security Technology

Security technology should provided the system and information protection against attackers for the organizations. Each technology provided the help to protect system/information against hackers/attacks and also find the unusual/suspicious activities. Here we are critical analysis to various security technologies and find the best technology for our system. Presently we all are know the biometric technology is one of the best option for protect our information to the attacker. Several of security technologies are shown in figure 4.2 here it is.

1. **Operational Technology -** Burglars actively seek ways to right to use networks and hosts. Armed with knowledge about precise errors/bugs, social engineering techniques and methods to take the information from system automatically penetration, burglars can often put on entry into systems with disturbing ease. System administrators face the problem not only how maximum valid user use the system services but also minimize the number of unauthorized users and complexity of network and protect the network form attacker. Data resources and assessed should be defended and unauthorized user's activities should be detected and assessed and suitable reply can be made when the security episode as they develop or occur.
2. **One-Time Passwords -** One-Time passwords is the another solution of authenticate a user. In one time password is time based password, just like for 5 to 15 mints as dependent of the authentication level. One time password will give them another power of user to valid his/her self or monitoring our login. For example that Gmail providing the 2-step verification process in which when the user will logon at any system the server will send the OTP on his/her mobile phone, that is entered in his/her account, that OTP is only valid for 5 mint, after that they expired automatically. If administrator is want to improve the more security in OTP they encrypted when they traverse in the network so that the attacker will not identify them. If they capture OTP using the packet sniffers during the traverse networks not to read them.

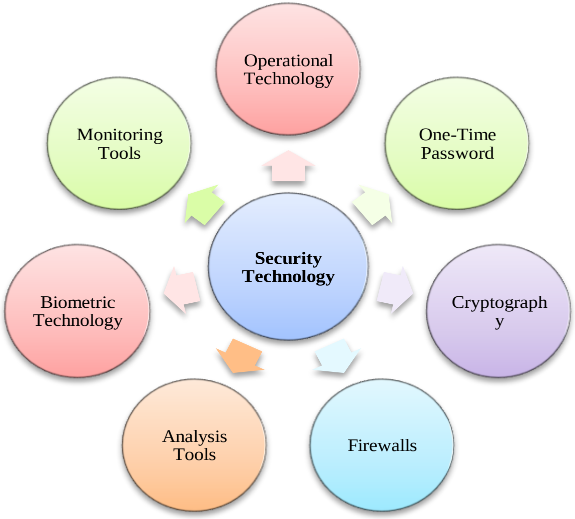

Figure 2: Different Security Technologies

3. **Cryptography** – Cryptography is another best method in security. They give the power to hidden the information during the network traverse or stored. In which many methods has to purpose like 16-bit, 32-bit, 128-bit, 256-bit encryption or many algorithms like DES, AES, Message Digest, RSA, Quantum encryption etc. In these methods the original message (called plain text) is converted in non-readable form. For example that if plain text is 100 bit long and want to send this information to another person through network then we will add the extra bit in the plain text like 28-bit if we are using the 128-bit encryption method using the public/private key according to the algorithm after that is message is converted into non-readable (called cipher text) from and send it into a network or stored. Information is received by receiver, they firstly decrypt the information again using the public/private key, and decryption is the just reverse process of the encryption.
4. **Firewalls** – Firewalls placed at a network gateway server which is provided the security to our private network and resources form the other networks attackers. It seems like a group of program. Firewall is also a program and hardware both. Firewall mainly works on the internet and also installed at the network. It allows workers access to the internet, it's provided the security form the outsider's user and also control the user who is used our data resources. The main purpose of firewall installation in the network is that it brooks all the requests and queries that are achieved the criteria of security that is established by the organization's network administrator. If a simple firewall is installed in the network the work is that they only filtering the router mean that they only discard those packets that are coming form the unauthorized addresses or seems to connect to unauthorized ports for service.
5. **Analysis tools** – There is strong need for analysis tool because of the increasing sophistication of attacker rules and the bugs/errors/loopholes present in the used applications/system, it is very important to review periodically network loopholes to compromise. A multiple range of loopholes/bugs identification tools are present, which give the command and take the

advantage to analysis the network. Analysis tools are freely available to the internet they give the advantage to analysis the network and find the threat and misused the treat for attack on the network.

6. **Monitoring tools** – Regular monitoring of network activity is essential if a web portal is to maintain a highly confidential data on the network. Network monitoring tools should be installed at appropriate location for collecting and regularly monitor the network and examine the data traveled in the network for any suspicious activity from the attackers. Presently it's possible in various monitoring tools providing the automatic alert system means when they found any suspicious activity in network than the issue a notification to network administrator. Most of attacker used the denial-of-service attack because the administrator is busy to solve this problem and they hack all the confidential information/data form the network or place a malicious code in the network they give regularly information to the attacker and send a copy of all the data or information automatically without knowledge to the administrator.
7. **Biometric technology -** Biometric technology is process of verifying or identifying an person with two different approaches is 1) physiological characteristic, in which examine the fingerprint, IRIS examine or face detection, 2) behavioral characteristic, in which check the keystroke, dynamic signature or voice verifications. They both are included in the biometric technology. Biometric technology is one of the best security mechanism for secure our private or confidential data from the attacker or various malicious activities.

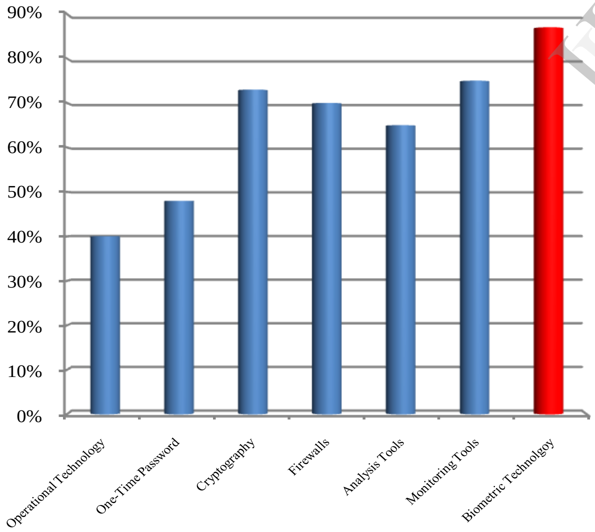

Figure 3: Statically review of security technology [8]

IV. Enhancement of security system of E-governance

Registration and Authentication

Registration is the process for access restricted services/document. Registration and authentication process is both are implemented parallel at the same time. Actually the major differences between the both the process is that the registration process the user is give the personal information like name & password for login, E-mail id, address, mobile no etc. But in the authentication process verify that this information is correct and the information is not used by another person. When these processes is implementing on internet it's called "Electronic authentication (e-authentication)". Electronic authentication is achieved by the following factors:

- **Knowledge -** something the user knows (e.g. user name, password, PIN, secret questions and answers, etc.);
- **Possession -** something the user has (e.g. Digital signature, smart card, etc.);
- **Be -** something the user is (e.g. biometric fingerprint, iris pattern, face recognition etc.); or - A combination of the above.

E-authentication service is implemented in different level. Here we give the different level of authentication service is that?

Authentication Service Provision

Level 0: This is the basic authentication mechanism using username and password. The user could be provided the capability of self-registration by which he/she can generate a username/password. He/she fill the self-registration form with the basic information also including the authenticated information like Aadhaar, PAN, Driving License, Rashan Card no etc. all this information helpful, if the user will forgot your username/password.

Level 1: At Level 1, a user will be able to prove her identity using OTP token along with his/her Unique Identification Card number (UID) credentials. The OTP will provide on his/her mobile phone no, this is entered at the time of registration of UID [6].

Level 2: At Level 2, the user would need to prove his/her identity through a hardware or software token (along with PIN). For this purpose, token would be a digital certificate/digital signature or a smart card or personal identification number (PIN) issued by the higher authority that would be required from the login.

Level 3: At Level 3, the user will prove his/her identity using biometrics authentication. This is the highest level of authentication security that would be available to a user. Biometrics based verification would be done in accordance with the Aadhaar authentication process.

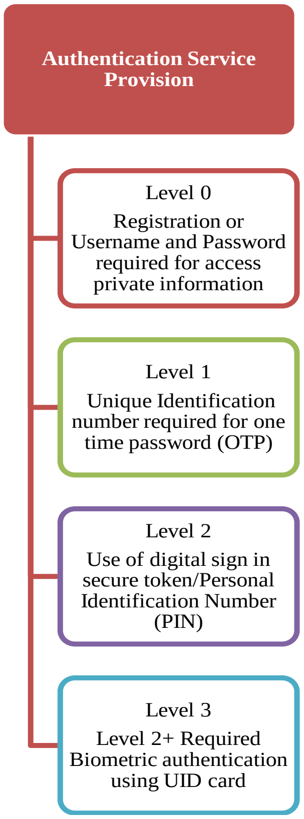
Authentication Service Provision
Level 0
Registration or Username and Password required for access private information
Level 1
Unique Identification number required for one time password (OTP)
Level 2
Use of digital sign in secure token/Personal Identification Number (PIN)
Level 3
Level 2+ Required Biometric authentication using UID card

Figure 4: Authentication Service Provision

Conclusion

During the last few years, many initiatives have been taken by different state governments in India for using IT as a tool in the functioning of Government so as to provide better services to citizens. In this paper we have made an attempt to summaries key areas which should be focused upon when a country wishes to position itself to be seriously moving towards E-Governance in a comprehensive way. This is a change, a transition that cannot be stopped since it is part of a global movement. Cooperation from government officials and staff will contribute to a smoother transition. Given the current high level of political commitment and largely adequate sources of funding, India is likely to soon emerge as a leader in E-Governance.

References

[1] National e-Governance Plan: http://www.negp.gov.in/

[2] National Portal of India: http://india.gov.in/

[3] Open Government Platform: http//ogpl.gov.in

[4] e-Governance Policy for Mordernising government through digital democracy in India, Journal of Information Policy 2 (2012): 183-203.

[5] Department of Electronic and information technology: http://deity.gov.in/content/e-governance#

[6] Unique identification card project: http://www.UIDAI.gov.in

[7] Aggerwal S. "UID - Challenges, Applicability and Opportunity". pp-1-8.

[8] MIT Report.