IMPACT OF SECURITY ISSUES IN E-GOVERNANCE OF DIGITAL INDIA

A-REVIEW

PRATIKSHA KAUSHIK[1] , DR RAJEEV KUMAR[2,] ,NAMIT GUPTA[3]

[1] BCA CCSIT, TEERTAHANKER MAHAVEER UNIVERSITY , MORADABAD 244001

[2] ASSISTANT PROFESSOR CCSIT, TEERTAHANKER MAHAVEER UNIVERSITY , MORADABAD 244001

[1]pratikshakaushik66@gmail.com

***Abstract*—** In this paper we provide a careful analysis of ICT (Information Communication and Technology) how it has made everything flexible and transparent. E-governance is the application of information and communication technology (ICT) for delivering government services, exchange of information communication transactions, integration of various stand-alone systems and services. There are many security issues among this process.

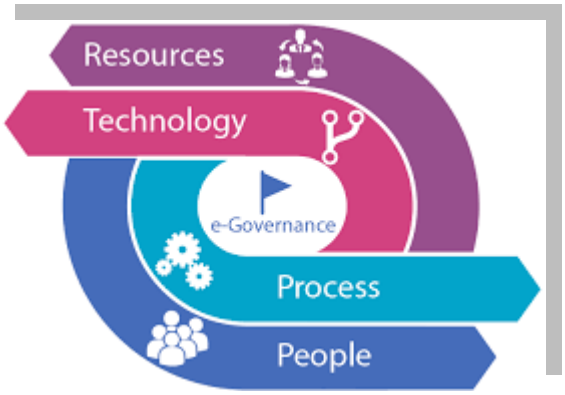
Basically its a review on the information security threats ,benifits of e-governance & the aim which governments planeed by e governance for transparent system.

Keyword s- ICT, applications ,Security threads ,malware ,packet sniffer, cryptography ,benefits,aim of e governace

Introduction

Information Communication and Technology (ICT) has made all most everything Electronic like E-Commerce, EServices, E-Voting, E-Villages, E-Learning, E- Governance, etc. Now Indian Government is in the bandwagon of institution attempting to harness ICT in their activities.“E”, in the E-Government basically denotes digital or digitalization. E-Government is dependent on ICT Services in order to achieve objective Anytime and Anywhere and it eliminates the necessity of physical travel by citizens to government agents, sitting behind desks and windows to get their job done.Major objective of E-Governance is to support and simplify governance for all government parties, citizens and businesses. E-Governance implies E-democracy where in all forms of interactions between the electorate (general public) and the elected government is performed electronically. The ultimate aim of E-Governance is to increase the citizen’s participation through mail and improve governance working .E-Governance allows common man to participate in the government’s policy making by directly communicating with government without any middleman.[1]

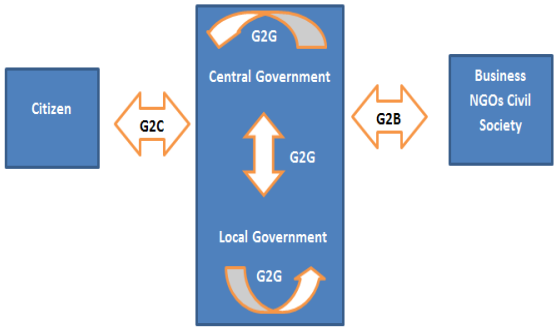
E-government (short for electronic government) is the use of electronic communications devices, computers and the Internet to provide public services to citizens and other persons in a country or region. According to Jeong, 2007 the term consists of the digital interactions between a citizen and his or her government (C2G), between governments and other government agencies (G2G), between government and citizens (G2C), between government and employees (G2E), and between government and businesses/commerces (G2B). [2]



2.Applications of e-governance

G2G: Government to Government
G2C: Government to Citizen
G2B: Government to Business
G2E: Government to Employee

- G2G (Government to Government): In this interaction, Information and Communications Technology is used to reorganize the governmental processes involved in the functioning of government entities as well as to increase the flow of information and services within and between different entities
- G2C (Government to Citizens): it maintains the relationship between government and citizens. It allows citizens to access government information and services promptly, conveniently, from everywhere, by use of multiple channels.
- G2B (Government to Business): In this type of interaction, e-Governance tools are used to help the business organizations that provide goods and services to seamlessly interact with the government. G2B can bring significant efficiencies to both governments and businesses.
- G2E (Government to Employees): G2E denotes to the relationship between government and its employees only. The aim of this relationship is to serve **employees and offer some online** services such as applying online for an annual leave, checking the balance of leave, and reviewing salary payment records.[3]



3. INFORMATION SECURITY THREATS

Incidents come in all shapes and sizes. They can come from anywhere on the Internet, although some attacks must be launched from specific systems or networks and some require access to special accounts. A cyber attack may be a comparatively minor event involving a single site or a major event in which tens of thousands of sites are compromised. [4]

e-Government security requirements can be studied by examining the overall process, beginning with the consumer and ending with the e-Gov server. The assets that must be protected to ensure secure e-Gov include client computers, the messages traveling on the communication channel, and the Web and egov servers – including any hardware attached to the servers[5].

The networks providing data to the end users of the e-Government remain vulnerable to variety

of threats such as packet sniffing, probing etc.

- **MALWARE:**

Malware, short for malicious software, consists of programming (code, scripts, active content, and other software) designed to disrupt or deny operation, gather information that leads to loss of privacy or exploitation, gain unauthorized access to system resources, and other abusive behavior

India Facing Increasing Malware Attacks

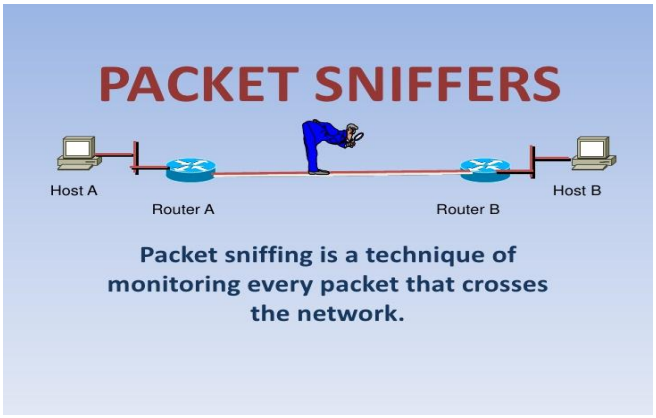
According to Perry4Law, a leading Techno-Legal ICT company in India that recently conducted a research, attacks with malicious software are on the rise in the country. Also said the company this problem is sure to escalate even further as there is neither the political will nor a National ICT Policy to counter against it.[6]

- **User to root (U2R) attack :**

User to root (U2R) attacks are a class of attacks where an attacker starts with access to a normal user account on the system and is able to exploit vulnerability to gain root access to the system e.g. loadmodule, perl, buffer_overflow, rootkit. A root compromise is similar to an account compromise, except that the account that has been compromised has special privileges on the system. The term root is derived from an account on UNIX systems that typically has unlimited, or privileges..

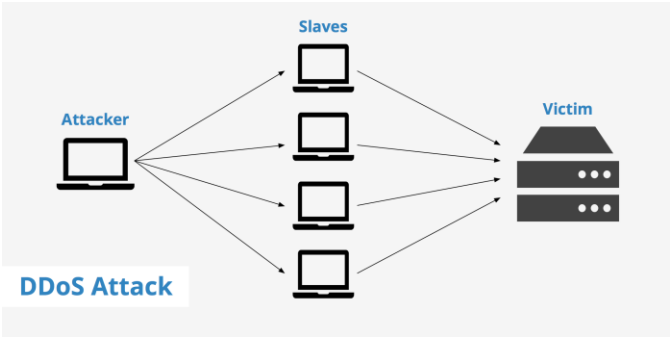
- Packet Sniffer-

A packet sniffer, sometimes referred to as a network monitor or network analyzer, can be used legitimately by a network or system administrator to monitor and troubleshoot network traffic.
Using the information captured by the packet sniffer an administrator can identify erroneous packets and use the data to pinpoint bottlenecks and help maintain efficient network data transmission. An unauthorized packet sniffing, however, can lead to serious breaches in electronic business and secured transmission.



- **Denial of Service (DOS) attack**:

A denial of service attack is a class of attacks where an attacker makes a computing or memory resource too busy or too full to handle legitimate requests, thus denying legitimate user access to a machine e.g. neptune, teardrop, smurf, pod, back, land. Attackers may "flood" a network with large volumes of data or deliberately consume a scarce or limited resource, such as process control blocks or pending network connections. They may also disrupt physical components of the network or manipulate data in transit, including encrypted data. Exploitation of Trust Computers on networks often has trust relationships with one another

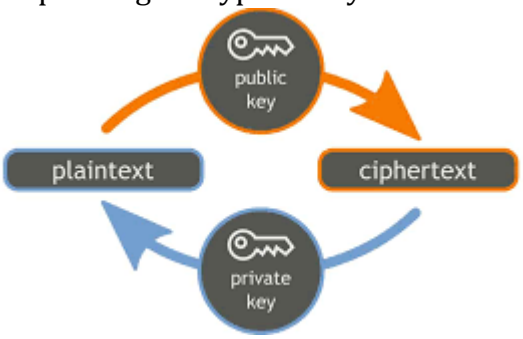


Security technologies

- **One-Time Passwords** Intruders often install packet sniffers to capture passwords as they traverse networks during remote log in processes. Therefore, all passwords should at least be encrypted as they traverse networks. A better solution is to use one-time passwords because there are times when a password is required to initiate a connection before confidentiality can be protected. One common example occurs in remote dial-up connections. Remote users, such as those traveling on business, dial in to their organization's modem pool to access network and data resources. To identify and authenticate themselves to the dial-up server, they must enter a user ID and password. Because this initial exchange between the user and server may be monitored by intruders, it is essential that the passwords arc not reusable. In other words, intruders should not be able to gain access by masquerading as a legitimate user using a password they have captured.

- **Cryptography** :

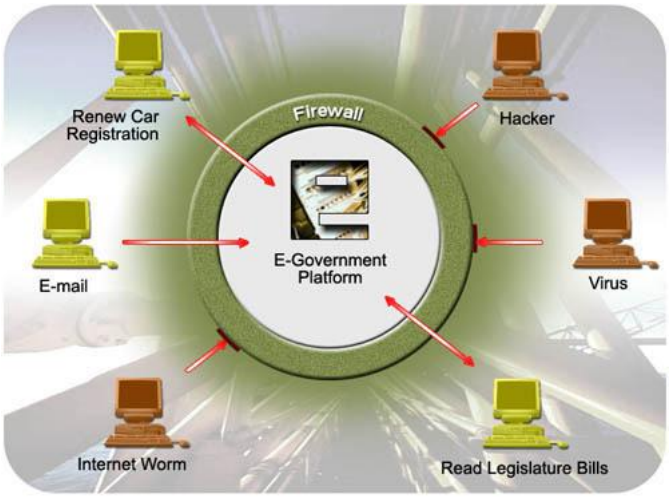
Sometimes it becomes necessary to encrypt the message sent, with the goal of preventing any one who is eavesdropping on the channel from being able to read the contents of the messages. One solution to this problem is, through the use of cryptography, to prevent intruders from being able to use the information that they capture. Encryption is the process of translating information from its original form (called plain text) into an encoded, incomprehensible form (called cipher text). Decryption refers to the process of taking cipher text and translating it back into plaintext. Any type of data may be encrypted, including digitized images and sounds. The authenticity of data can be protected in a similar way. For example, to transmit information to a colleague by E-mail, the sender first encrypts the information to protect its confidentiality and then attaches an encrypted digital signature to the message. When the colleague receives the message, he or she checks the origin of the message by using a key to verify the sender's digital signature and decrypts the information using the corresponding decryption key.



- **Firewall**

A firewall is a network security system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Network firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines

each message and blocks those that do not meet the specified security criteria.[7]



Aim of e-governance

The complete transformation of the processes of Governance using the implementation of

Information & Communication Technology is called E-Governance.

It brings in SMART Governance viz.:

S - Simple: Simplification of rules and procedures of Government making it user-friendly.

M-Moral: Infusing ethics and morals into officers again since anti-corruption and vigilance

agencies improving.

A- Accountable: ICT helps set standards of performance and efficiently measures it.

R- Responsive: Efficient service delivery and government that is in tune with the people.

T- Transparent: Information confined to secrecy is out in the public domain bringing equity

and rule of law in public agencies.

SMART Governance enables:

1. People participation
2. Accountability and efficiency
3. Transparency
4. User friendly government processes
5. Better service delivery

BENEFITS OF E-GOVERNANCE

- **Better access to information and quality services for citizens**: ICT would make available timely and reliable information on various aspects of governance. In the initial phase, information would be made available with respect to simple aspects of governance such as forms, laws, rules, procedures etc later extending to detailed information including reports (including performance reports), public database, decision making processes etc.
- **Simplicity, efficiency and accountability in the government**: Application of ICT to governance combined with detailed business process reengineering would lead to simplification of complicated processes, weeding out of redundant processes, simplification in structures and changes in statutes and regulations.[6]
- **Speed in excessing** – Technology makes communication speedier. Internet, Phones, Cell Phones have reduced the time taken in normal communication.
- **Cost Reduction** – Most of the Government expenditure is appropriated towards the cost of stationary. Paper-based communication needs lots of stationary, printers, computers, etc. which calls for continuous heavy expenditure. Internet and Phones makes communication cheaper saving valuable money for the Government.
- **Transparency in the system** – Use of ICT makes governing profess transparent. All the information of the Government would be made available on the internet. The citizens can see the information whenever they want to see. But this is only possible when every piece of information of the Government is uploaded on the internet and is available for the public to peruse. Current governing process leaves many ways to conceal the information from all the people. ICT helps make the information available online eliminating all the possibilities of concealing of information.

- **Accountability** – Once the governing process is made transparent the Government is automatically made accountable. Accountability is answerability of the Government to the people. It is the answerability for the deeds of the Government. An accountable Government is a responsible Government.[7]

CONCLUSION :

WEBSITE SECURITY IS IMPORTANT AND NECESSARY. IT IS EVIDENT FROM ABOVE DISCUSSION THAT FOR E-GOVERNANCE TO

BE SUCCESSFUL, IT REQUIRES PEOPLE, PROCESS AND TECHNOLOGY. IN INDIAN E-GOVERNANCE SCENARIO, HOWEVER, THE

SECURITY ASPECTS ARE NOT BEING TAKEN AS SERIOUSLY. IN 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. DIGITAL SECURITY IS CRITICAL IN E-GOVERNANCE INITIATIVES. CONFIDENTIALITY OF ANY TRANSACTION OR INFORMATION AVAILABLE ON THE NETWORK IS CRUCIAL. THE GOVERNMENT DOCUMENT AND OTHER IMPORTANT MATERIAL HAVE TO BE PROTECTED FROM UNAUTHORIZED USERS IN CASE OF E-GOVERNANCE PROJECTS. HENCE,SECURITY IS CRITICAL FOR SUCCESSFUL IMPLEMENTATION OF SUCH **PROJECTS. E-GOVERNANCE COUPLED WITH SECURITY SYSTEMS PROVIDING ADEQUATE PROTECTION IS THE REQUIREMENT OF ANY SYSTEM DESIGN EFFORT TO BEAT THE INERTIA.WE ALSO INVESTIGATE VULNERABILITY AND PROPOSE SOME SOLUTION TO ACHIEVE SECURITY[5]**

REFERENCES

[1] Guncha Hashmi, Pooja Khanna2
Department of Computer Science, Amity University, Lucknow, India. International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Vol. 4, Issue 5, May 2016 .

[2] https://en.wikipedia.org/wiki/E-government

.

[3 http://www.civilserviceindia.com/subject/General-Studies/notes/e-governance.html

[4] Shailendra Singh Member, IEEE; D. Singh Karaulia
E-Governance: Information Security Issues International Conference on Computer Science and Information Technology (ICCSIT'2011) Pattaya Dec. 2011

[5] Mamatha.T1 and Md.Zair Hussain2
Department of Computer Science & Engineering
Maulana Azad College of Engineering & Technology
Patna, Bihar India NETWORK SECURITY SOLUTIONS AND VULNERABILITIES IN E-GOVERNMENT.

[6http://www.spamfighter.com/News-12563-India-Facing-Increasing-Malware-Attacks.htm

[7] http://www.webopedia.com/TERM/F/firewall.html

[8]http://indiaegovernance.blogspot.in/2008/03/advantages-of-e-governance.html

.