E-Governance: Information/Data Security

Hiren Harshadbhai Darji

Abstract----As internet supported in e-governance, digital communities involve, in an e-government project, a substantial amount of documentation is done like government recruitment records, police records and so on. Each department is thoughtful so that only authorized people get into the network and access the information. An understanding of the information security technology and the need for its implementation is key for harmless, secured and smooth functioning of e-governance undertaking.

Keywords: E-Government, Information Security, Security Framework, Data Security.

I. Definition Of E-Governance

E-governance is the application of information & communication technologies to transform the efficiency, effectiveness, transparency and accountability of informational & transactional exchanges with in government, between govt. & govt. agencies of National, State, Municipal & Local levels, citizen & businesses, and to empower citizens through access & use of information. [6]

A. E-government concept:

The concept of an e-government system is to provide access to government services anywhere at any time over open networks. This leads to issues of security and privacy in the management of the information systems. Managing such issues in the public sector has different weights than in the private sector. The broader e-government approach is socio-technical by nature, involving people and processes as well as technologies; hence, particularly in transitional countries, the social culture and characteristics of the country are factors in successful e government development. [5]

B. The Basic Structure of E-Governance:

Layne in 2001 described a four-stage growth model to develop a fully functional e-government. Based on technical, organizational and managerial feasibilities, the four stages of a growth model for e-governance are:

- Cataloguing (Information)
- Transaction
- Vertical integration (Interactive)
- Horizontal integration (Strategic, interactive) or transformation.

The first stage is "cataloguing" or "Information" because efforts are focused on cataloguing government information and presenting it on the web. The first stage is focused on establishing an on-line presence for the government.

The second stage "Transaction", where e-government initiatives are focused on connecting the internal government system to on-line interfaces and allows citizens to perform with government systems to on-line interfaces and electronically, is referred as "transaction-based" e-government. This stage is a link between the live database and the on-line transaction.

Any citizen can contact one point of government to complete any level of governmental transaction, which can be referred as "one stops shopping" concept. This integration may happen in two ways: vertical and horizontal. Vertical integration refers to local and central administration connected for any functions or services of government, while horizontal integration refers integration across different functions and services.

Vertical or intra- departmental integration is must before implementing the horizontal or interdepartmental integration because of different level of complexities associated. It is expected that

vertical integration across different levels of government should happen first, because the gap between the levels of government is much less comparatively than the difference between different functions. Mostly administrators interact more closely with their central or local counterparts than with other departments in the same level of government. The vertically and horizontally integrated e-government represents an ideal situation, in which citizens have on-line access to ubiquitous government services, with a transparent system. [6]

II. Information Security For E Governance

E Governance involves Information Technology enabled initiatives that are used for improving the interaction between Government and citizens or Government and business as well as the internal Government operations. To provide "trusted" services, e Governance needs to focus on Effectiveness, Efficiency, and Flexibility & Transparency.

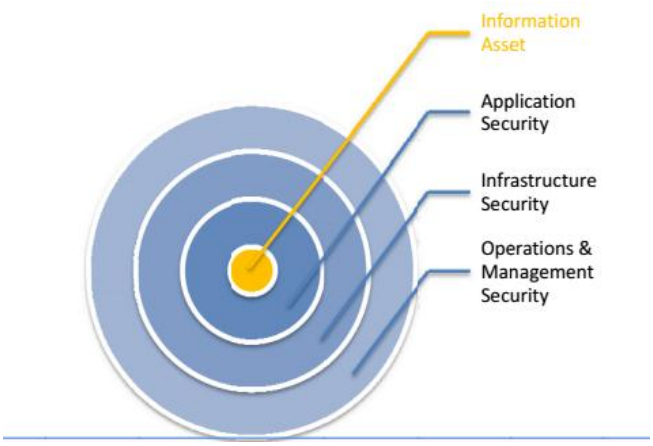
Information security is intended to safeguard the information assets and is determined in terms of confidentiality, integrity and availability.

Confidentiality: Protecting sensitive information from unauthorized disclosure or intelligible interception.

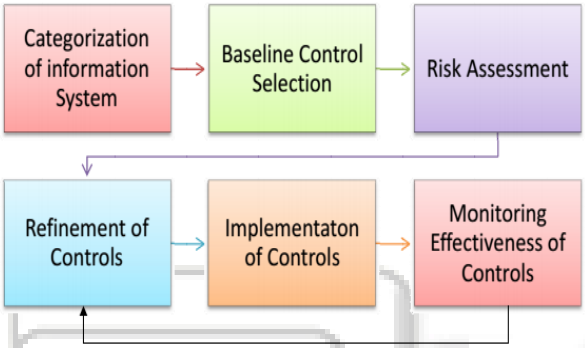
Integrity: Safeguarding the accuracy and completeness of information and software; protecting data from unauthorized, unanticipated or unintentional modification.

Availability: Ensuring that information and vital IT services are available when required.

In fact security of any information on system is essentially an amalgamated output o of Application Security, Infrastructure Security, and Secure Operation & Management. Enforcement of security at all levels is essential to achieve a fairly secure environment. [9]



– *Information Security Assurance Framework:*



III. Data Security

Data security limits access to data objects to specific individuals. Different levels of data security include read-only, edit, insert, and delete. Data security can be set at the application or object level.

Data security for e-Governance systems may be enforced through business logic or at the database layer. In most cases the business logic authenticates users and provides them with specific rights to data objects. This means that authenticated users gain access to objects based on specific capabilities assigned by the system. For example, a person may have read-only access to government related information so he cannot change the values associated with the application. A person or user may have access to citizen records that he manages, but not have access to citizen records managed by others. To simplify e-Governance, systems offer role-based security so administrators can assign broad security policies to specific individuals. By assigning roles, administrators can change security for many people at once without the responsibility of changing individual records.

Most data security is limited to data access. Once a user gains access to specific information, screens, or reports, the information can be downloaded and shared with others. Digital rights management goes one step farther by "wrapping" data objects with rights that follow the object no matter where it goes. In this case, users can forward the encrypted data, but that data cannot be viewed or changed unless the recipient can be verified. [3]

IV. Information Security Threats For E Governance

- *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.

- *Probe :*

Probe is a class of attacks where an attacker scans a network to gather information or find known vulnerabilities.

- *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.

- *Internet infrastructure attacks* **:**

These rare but serious attacks involve key components of the Internet infrastructure rather than specific systems on the Internet.

- *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.

- *Remote to Local (R2L) attack :*

A remote to local attack is class of attacks where an attacker sends packets to a machine over network, then exploits the machine's vulnerability to illegally gain local access to a machine.

- *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. [2]

Improving Security in E-Governence:

- *Security policy:*

A policy is a documented high-level plan for organization-wide computer and information security. It provides a framework for making specific decisions, such as which defense mechanisms to use and how to configure services, and is the basis for developing secure programming guidelines and procedures for users and system administrators to follow. [2]

- *Security Practices:*

System administration practices play a key role in network security. Checklists and general advice on good security practices are readily available. [2]

- *Security Procedures:*

Procedures are specific steps to follow that are based on the computer security policy. Procedures address such topics as retrieving programs from the network, connecting to the site's system from home or while traveling, using encryption, authentication for issuing accounts, configuration, and monitoring. [2].

V. Conclusion

Security is an essential part of e-government, however in our country the security aspects are not considered seriously. 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. This paper provides brief idea about e-government and its security aspects.

REFERENCES

[1] Yen-Ping Chu, "Challenges In E-Government and Security of Information ".
[2] Shailendra Singh Member, IEEE; D. Singh Karaulia, "E-Governance: Information Security Issues" Dec-2011.
[3] Rajan Manro, Dr. Rajneesh Randhawa, Dr. A S Joshi, "Security Issues in Cloud Based E-Governance Model" June-2012.
[4] "Information Security Management in E-Governance".
[5] Salahuddin Alfawaz, Lauren May, Kavoos Mohanak, "A Managerial Conceptual Framework"
[6] Mrinalini Shah, "E-Governance in India: Dream or Reality? 2007.
[7] "Frame / Methodology for the Information Security Management in an E-Government Environment".
[8] Gopala Krishna Behara, Vishnu Vardhan Varre, Madhusudhana Rao, "Service Oriented Architecture for E-Governance", Oct-2009.
[9] An Approach Paper, "Egovernance Security Standards Framework".
[10] Vinayak Godse, "Data Security in E-Governance Projects In India ".
[11] Sharif N As-Saber, Aashish Srivastava, Khalid Hossain, "Information Technology Law And E-Government: A Developing Country Perspective"
[12] Ankush Joshi, Haripriya Tiwari, "Security for E-Governance".

.

