UNIT-4

Security for e-Government

E-government has become a popular focus of government efforts in many countries around the world. To provide trusted services, e-governance needs to focus on effectiveness, efficiency and flexibility. If the citizen is to derive maximum benefit from the provision of e-services through e-governance, the e-service must possess following attributes:

→ The users must know the information about the available e-services.
→ The users must be aware of the benefits of these services.
→ The user should be able to locate the e-services easily.
→ The e-services must be accessible to all members of the intended target groups.

Information security is determined in terms of confidentiality, integrity and availability.

Confidentiality: Protecting sensitive information from unauthorized disclosure.

Integrity: Safeguarding the accuracy and completeness of information and software.

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

In context of Security, services provided by e-government program are categorized with respect to functional processes as:

i) Publishing: Publishing involves simply posting information on a publicly accessible Website.

ii) Interactive processing: It involves citizens reading instructions published on Websites and following those instructions to submit reports, applications etc.

iii) Transaction processing: It involves processing of information submitted via interactive e-government Websites.

iv) Service delivery: It involves actual execution of actions approved on the basis of e-government interactions.

⊛. Challenges and approach of E-Government Security:

Threats to the security of information in an e-government environment can include natural and accidental events (e.g. flooding, fire, storms, human error etc.) and deliberate threats (e.g. fraud, information theft, hacking, viruses etc.). Confidentiality, Integrity and Availability, also known as the CIA triad, is a model designed to guide policies for security.

1) Availability: Availability is the process of ensuring that information and vital IT services are available when required. Availability concerns affect: publishing, interactive processing, transaction processing and service delivery e-government activities. Following are some availability concerns:

i) Fault-related availability concerns: It includes hardware faults, changes in program or data structures, and failures in other system facilities that are not computer based.

ii) Intrinsic availability concerns: It includes unuse of storage and recovery mechanisms, failure of magnetic media, and loss of facilities due to physical damage.

iii) Denial of service concerns: Government services are attractive targets for malicious activities. Denial of service attacks can be launched from a variety of sources and can take a number of forms.

iv) Individual or informally organized hackers: Most denial of service attacks against e-government services have been launched by individual or informally organized hackers. Some of these have resulted in significant disruption and expense to the taxpayer.

2) Integrity: Integrity is the process of safeguarding the accuracy and completeness of information and software. Integrity concerns affect: publishing, interactive processing, transaction processing,

and service delivery e-government activities. Following are some integrity concerns or issues:

1) Data Content Integrity Issues: Data content integrity issues are associated with unauthorized modification or destruction of e-government information content. This can involve modification or destruction of
   → information electronically published by the government;
   → information associated with reports, applications or other service requests.

2) Intentional modification of data: Data may be modified or destroyed within e-government processors (e.g. Web Servers). Penetration may be accomplished by defeating identification and authentication mechanisms.

3) Connection integrity issues: Successful implementation of e-government services requires some degree of confidence on the part of private citizens or other user entities that information being read originated only with the assumed government source and that information being provided goes only to the appropriate government destination(s).

3) Confidentiality: It is the process of protecting sensitive information from unauthorized disclosure.

1) Impacts or consequences of unauthorized exposure: The consequences of unauthorized exposure of information via e-government resources depend in large part on the specific information that is exposed.

2) Loss of confidence in institutions and service delivery mechanisms: Public disclosure of e-government confidentiality breaches can result in loss of public confidence in e-government mechanisms and in the institutions they serve.

⊛. Security Approaches for E-Government:

1) **Cryptographic Mechanisms:** Cryptography is one of the best method in security. They give the power to hide the information during network traverse or stored. There are many methods like 16-bit, 32-bit, 128-bit, 256-bit encryption or many algorithms like AES, DES, RSA etc. In these methods the original message is converted into non-readable form called ciphertext.

2) **Database Design:** Some e-government services include provision of data that are derived from aggregation or analysis of information that is subject by law to privacy protection. A number of database design and management approaches have been developed to address this problem.

3) **Anti-virus system:** There are many types of viruses that occupy disk space, corrupt our valuable data or storage medium. So to protect a system from virus anti-virus system can be kept.

4) **Firewalls:** Firewall is a system designed to prevent unauthorized access to or from a private network. Firewall is a security device which can be hardware or software or both. We have several firewall techniques such as Packet filter, Application gateway, Proxy server etc.

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 used application/system.

6) **Monitoring tools:** Regular monitoring of network activity is essential if a web portal is to maintain a highly confidential data on network. If monitoring tools find any suspicious activity in network then automatic alert system alerts the system.

7) **Biometric technology:** Biometric technology is process of verifying or identifying an person with two different approaches: physical characteristics (which examine fingerprint, Iris, face etc.) and behavioural characteristics (which check keystroke, signature, voice etc).

⊛Security Management Model:

A security management model is meant to be a generic description of what an organization should do to provide a secure environment for itself. It is generic in that it describes what should be done, but not how to do it, which makes it flexible enough to be used by many kinds of organizations. We should choose a model for our organization to follow that is "flexible, scalable, robust, and sufficiently detailed".

1) **Access Control Models:** Access controls regulate the admission of users into trusted areas of organization—both the logical and physical. Access control is maintained by means of a collection of policies, programs to carry out those policies, and technologies that enfore policies. The general application of access control comprises four processes: identification, authentication, authorization, and accountability.

2) **Security Architecture Models:** It illustrates information security implementations. It can help organizations quickly make improvements through adaption. Some models are implemented into computer hardware and software, Some are policies and practices, Some are implemented in both.

3) **Bell-LaPadula Confidentiality Model:** It is a state machine-based multilevel security policy. The model was originally designed for military applications. State machine models define states with current permissions and current instances of subjects accessing the objects. The security of the system is satisfied by the fact that the system transitions from one secure state to the other with no failures.

4) **Biba Integrity Model:** It is a formal state transition system of data security policies designed to express a set of access control rules in order to ensure data integrity. Data and subjects are ordered by their levels of integrity into groups or arrangements. Like other models, this model supports the access control of both subjects and objects.

5) The Clark-Wilson Model: It is integrity model which focus to protect integrity of data. It consists of subject/program/object triples and rules about data, application programs and triples. The Clark-Wilson security policy model seeks to formalize the principles of accounting security that have collected over centuries of experimental bookkeeping.

6) The Graham-Denning access control model: This is a computer security model that shows how subjects and objects should be securely created and deleted. It also addresses how to assign specific access rights. It is mainly used in access control mechanisms for distributed systems. There are three main parts to the model:

- → A Set of Subjects,
- → A Set of Objects,
- → A Set of Eight Rules.

7) Harrison-Ruzzo-Ullman Model: The security model proposed by Harrison, Ruzzo, and Ullman (HRU) is a flexible access control model. In HRU, the current set of access rights at any given time can be represented by a matrix, with one row for each subject and one column for each subject and object. Each cell in table contains the list of access rights. The components of HRU model include:

- → A set of subjects,
- → A set of objects,
- → A set of access rights,
- → An access matrix.

8) Brewer-Nash Model: The Brewer and Nash model also known as Chinese wall, was constructed to provide information security access controls that can change dynamically. It was designed to provide controls that mitigate conflict of interest in commercial organizations, and is built upon an information flow model.

E-Government Security Architecture:

The security architecture of E-governance is a high level document that set the security goals of e-governance project and describe the procedure that need to be followed by all the e-governance hierarchy such as users, business operators etc. Appropriate legal framework is absolutely essential for the systematic and sustained growth of e-governance.

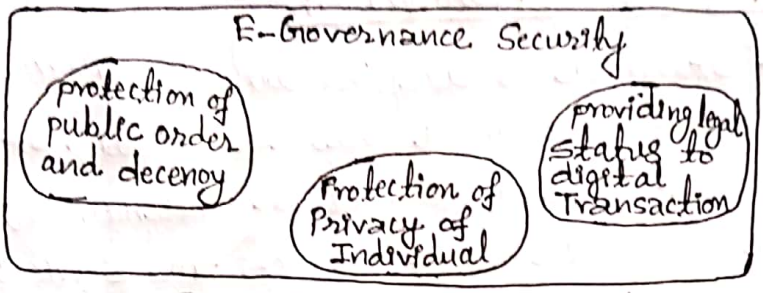

Fig: E-Governance Security

E-governance Security Architecture Reference Framework:

e-Government Security Architecture forms part of the Technical Reference Model (TRM). TRM supports and enables the delivery of ICT Security Standards Domains and capabilities and provides a foundation to advance the re-use and standardization of technology and service components. The TRM has been structured hierarchically as:

i) Service area: Each service Area aggregates the standards and technologies into a lower-level functional area. Each Service Area consists of multiple Service Categories and Service Standards.

ii) Service category: Each service category classifies lower levels of technologies and standards with respect to the business or technology function they serve. In turn each Service Category is comprised of one or more service standards.

iii) Service standards: They define the standards and technologies that support a Service Category. To support Public Institutions mapping into the TRM, many of the Service Standards provide illustrative specifications or technologies as examples.

⊛ Security Standards:

Security Standard represents a set of requirements that a product or a system must achieve. Assuming the conformity of a product or system with a certain standard demonstrates that it fulfills all the standards specifications. There are currently some primary standards in place governing information security.

Need/Importance of Security Standard:

The use of standards is accepted without any exception and gives the possibility of comparing a personal security ~~of~~ system with a given frame of reference adopted at an international level. Standards ensure desirable characteristics of products and services such as quality, safety, reliability, efficiency etc, at an economical cost. Organizations can benefit from common best practice at international level, and can prove the protection of their business processes and activities in order to satisfy business needs.

Some of Security Standards:

1) **ISO/IEC 27000 standards series:** This involves information security standards published jointly by the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). The series provides the recommendations on information security management, risk handling and controls implementation within the context of an overall Information Security Management System (ISMS).

2) **The SP800 standard series:** It is the oldest of all the information security standards. It consists of over a hundred documents covering almost every aspect of information security. The most representative among all these documents is the computer security handbook SP800-12 which provides a good idea of the NIST approach.

3) ISF Standard of Good Practice for Information Security:

The Information Security Forum (ISF) is an international, independent, non-profit organization dedicated to benchmarking and best practices in information security. The Standard of Good Practice (S.G.P) released in 1996 represents a detailed documentation of best practice for information security.

4) Control Objectives for Information and related Technology (COBIT):

COBIT is a set of best practices for information technology management created by Information Systems Audit and Control Association (ISACA), and the IT Governance Institute (ITGI) It's mission is to "research, develop, publicize and promote an authorative, up-to-date, auditors etc."