- Scalability.

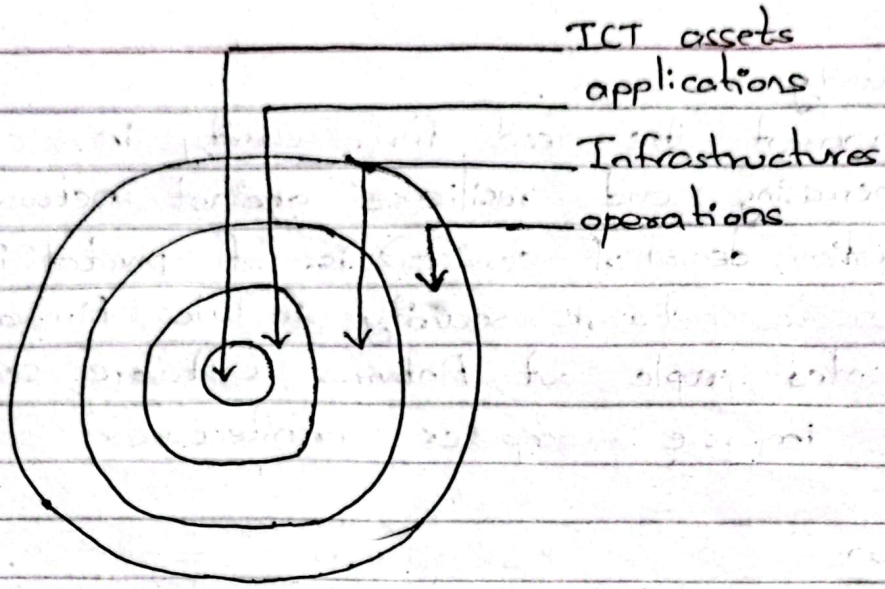
* Benefits of cloud governance

Unit-4

Security for E-government

Security is one of the important issues of e-government. Today the users or programmers are very smart and intelligent and they can attack in several forms and so the defence level has to be sufficiently strong and comprehensive. Deployment of strong security mechanisms help the government to carryout its activities efficiently and systematically.

Inorder to make the e-government effective, the most importants feature that it must implement is its e-government security. Security is all about protecting the information and communication technology (ICT) assets of an organization. The ICT assets include data, information, knowledge resource, programs, hardwares and networks. These assets are very important so it is very important responsibility of e-governance administrators to protect these assets.



There are various threats to security of our ICT system and we can't define and declare them exactly, it may come from various sources and in various forms. So, it is very necessary for E-governance adminstrators to identify these threats. Basically, there are two sources of threats;

(i) Internal threats
(ii) External threats

Internal source of threats include, the employee who works on E-governance project, customers of E-governance project may attempts to access the database for their personal financial profit.

External sources includes professional hackers, criminal organizations, etc..

#. Challenges and approach of E-government security

The key security challenges of E-gaverment are as follows :-

(1) Network security

↳ With E-government, the need for security in communication network is increasing and resilience against network attack (access, modification, denial of service) is of pivotal importance. Measure to ensure network security includes Firewalls and proxy to keep unwanted people out, Antivirus software, security fencing as well as improve computer architecture.

(2) Identification

↳ The issue of identification arises several important question related to our case. In E-procurement, the issue of verifying the identity of a business is important not only for making sure that the business is dealing with instantly but also it focuses in long term vision. The identification helps to identify the authenticate user who can access the required data, modify the data if needed and correct the data if error arises.

(3) Useability

↳ Useability focuses on making application and services easy for the people to use. The issue of useability is linked to security concerns since attempts to increase data security may decrease their useability. Useability also addresses how data is going to be used and who is using the data. Useability entails a strong focuse on issues of trust in E-government invoke by the intractions amo ators that control, deliever or benefit from the service.

(4) Access control

↳ All electronic system that contains sensitive information. will

be of interest to the people who might want to use this information for nefarious purpose. As a result, access control to these system is needed in order to prevent unwanted use of the information stored. Access control in general has a very wide defination, since it can be any thing from your carlock to the pincode to your credit card. But, the basic function is to denied unwanted access. So, in the area of E-government the access control will mainly be electronic or physical and the system can be anything from database of citizen information, bank accounts, health records, etc.

#. Security management

Security management is very much important in E-governance system which helps in carring out different level activities systematically. The security of E-governance system has to be managed systematically in three different levels.

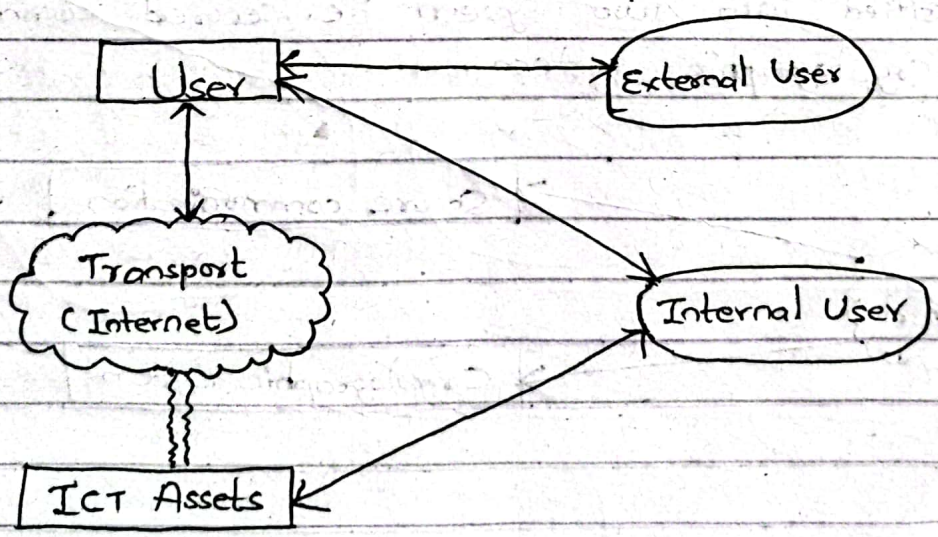
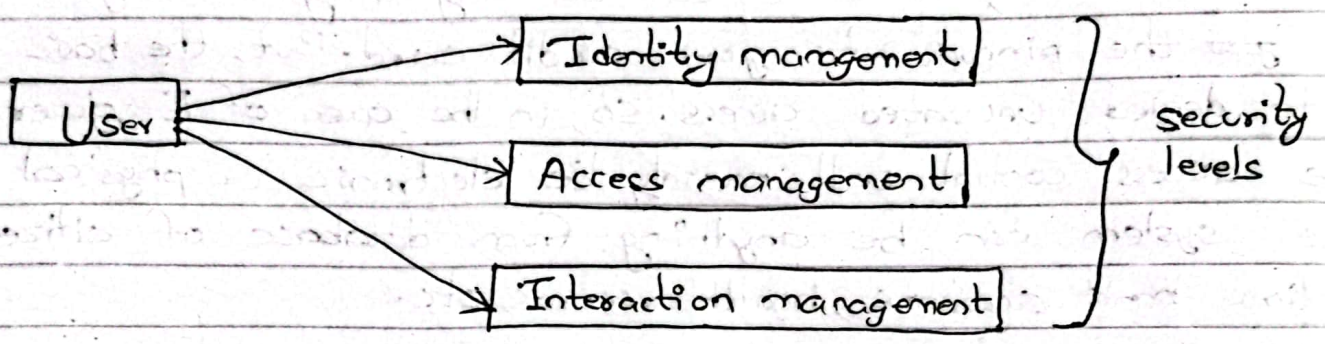


fig:- E-governance security Environment

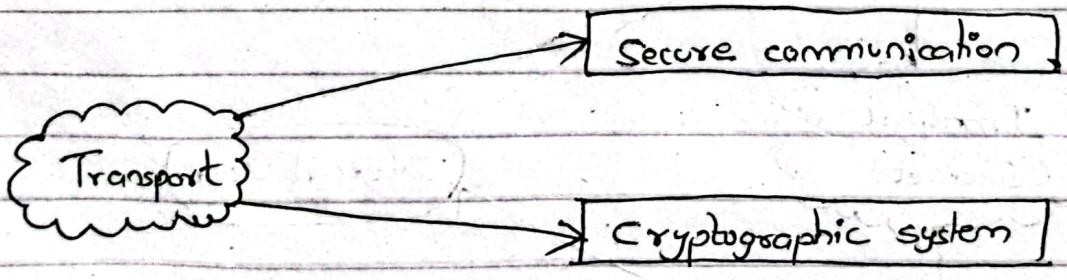
(i) Security at User level

Security at User level is very important issue. We can classify the user level security management into three parts namely; identity management, access management, and interaction manageme



(ii) Security at Transport level

In this level we considered about E-governance security into two acpects which are security within LAN and WAN and the second one is security over the internet. This security level is classified into two system i.e. secured communication system and cryptographic system.



(iii) Security at ICT Assets level

ICT assets are most precious for any organizations or institution, so to secure this level we have two broad categories of security treatment i.e. physical security and electronic security.

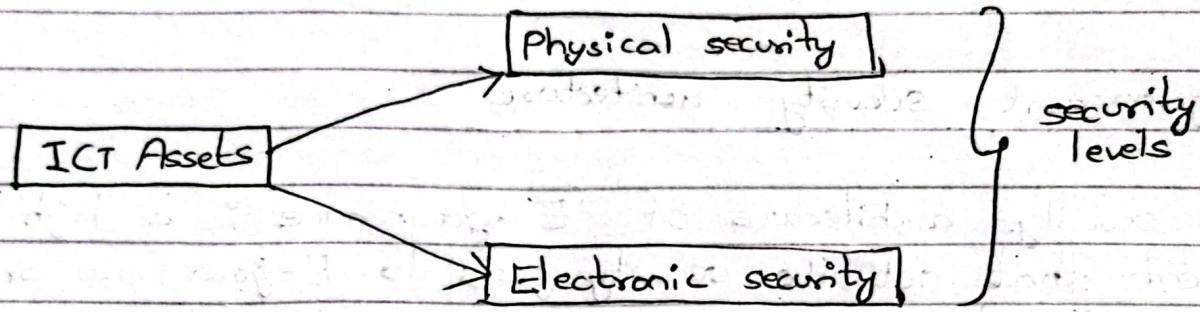


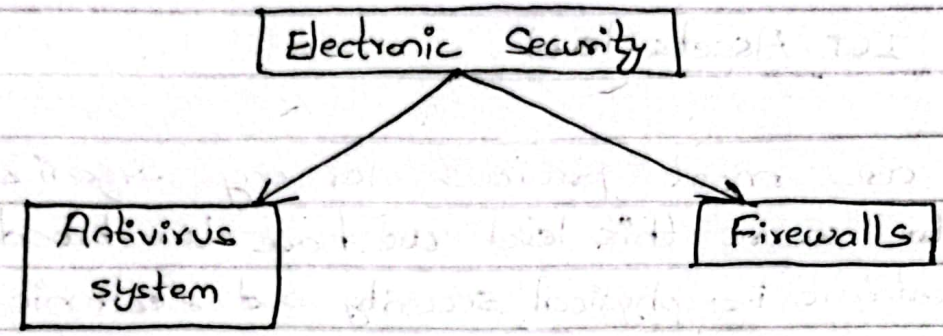
fig :- Security for ICT Assets

(a) Physical security

It is used to protect the data against physical damage or losses like natural dicasters, etc. To protect data in this level we take some steps to maintain security by implementing dust proof environment, fire protection system, CCTV monitoring, security Alaram's, Automated backup system, etc.

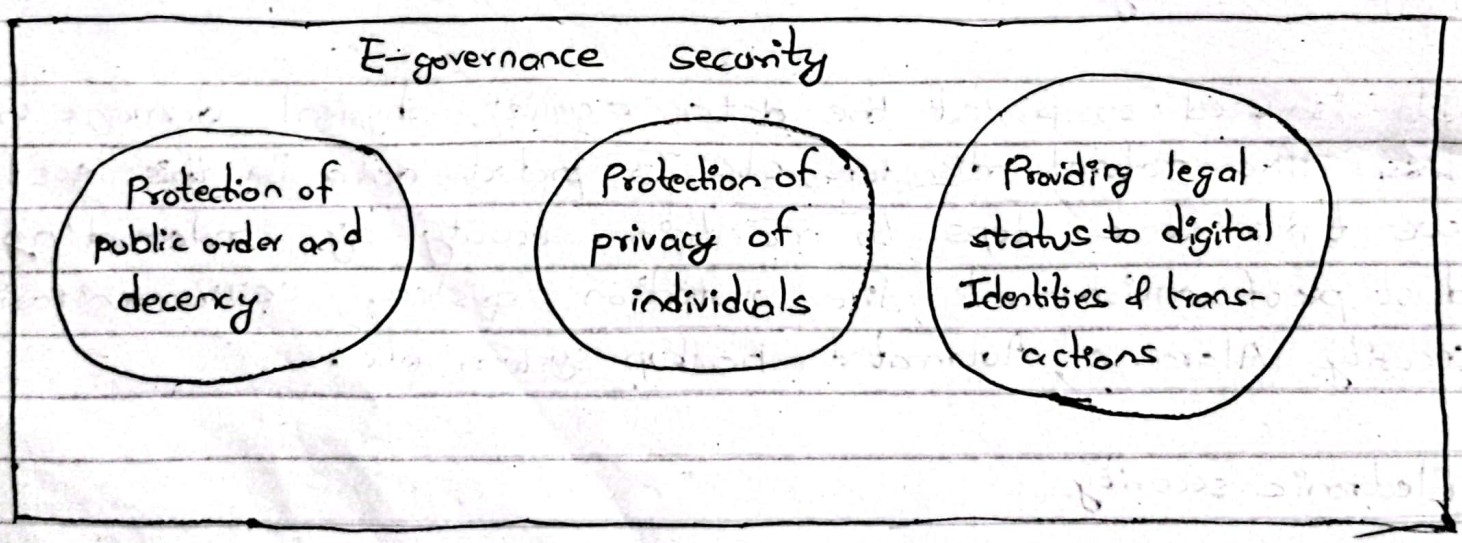
(b) Electronic security

To give the protection against digital threats we used electronic security. We can manage electronic security in two ways i.e. Antivirus system and Firewalls.



E-government security Architecture

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



Security Standards

The standard for information security was set by BS 7799 (British standards), being its popularity, it was adopted by ISO as ISO 17799 and its sequel BS 7799-2 that describes the specification for information security management. The ISO 27001 was published in october 2005, replacing the old BS 7799-2 standard. It is the specification for information security management system. ISO 17799 defines 127 security controls structured under 10 major headings to enable the information security manager to identify the particular safeguards that are appropriate to their specific area of responsibility.

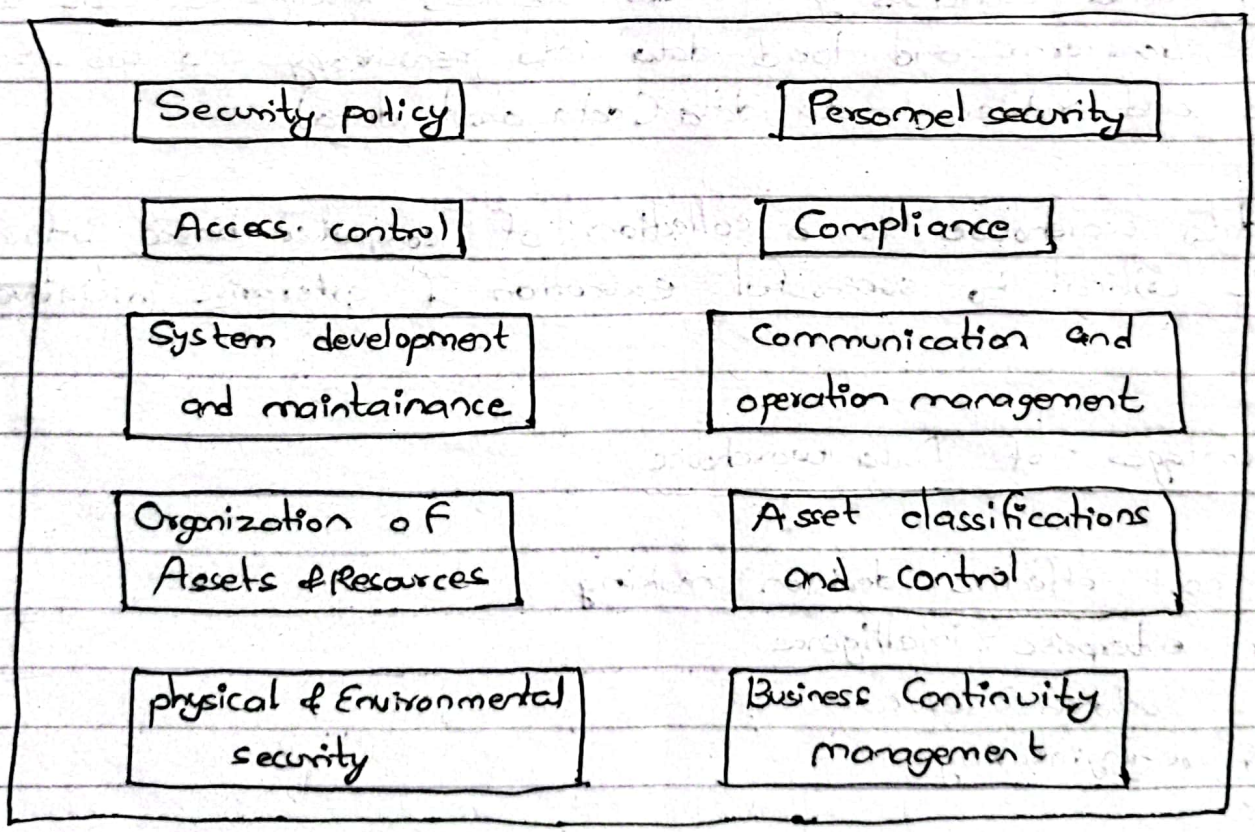


fig:- Major security areas