UNIT-3

E-Government Infrastructure Development

⊛ Network Infrastructure:

Network infrastructure is the hardware and software resources of an entire network that enable network connectivity, communication, operations and management of an enterprise network and establish the connectivity to all the entities of digital governance. It provides the communication path and services between users, processes, applications, services and the internet. Network infrastructure is typically part of the IT infrastructure found in most enterprise IT environments.

The entire network infrastructure is interconnected, and can be used for internal communications, external communications or both. A typical network infrastructure includes:

Networking Hardware:

→ Routers
→ Switches
→ LAN Cards
→ Cables

Described at last of this chapter

Networking Software:

→ Network operations and management.
→ Operating systems
→ Firewall
→ Network security applications

Network Services:

→ T-1 Line
→ Satellite
→ Wireless protocols
→ IP addressing

⊛ Computing Infrastructure:

Infrastructure is the foundation or framework that supports a system of government or organization. Computing Infrastructure provides management and support for end-user computers, servers, storage systems, operating systems, databases, middleware and ERP (Enterprise resource planning) systems. There are three groups that make up the Computing Infrastructure team:

i) **Database and ERP Administration:** It manages and supports the main database infrastructure for core applications used by staff, faculty and students, based on Oracle Database software. It also manages and supports Oracle and MySQL databases for variety of administrative and academic needs.

ii) **End-User Computing:** The End-User Computing group consists of two teams that provide personal computer management, support and assistance to faculty and staff. The End-User Computing infrastructure team provides back-end management and support for a number of key applications. End-User Computing group, as a unit, works very closely with other groups within CCS and other departments, to ensure that the best solutions and services are delivered in a secure and manageable way.

iii) **Server and Storage Services:** The Server and Storage Services group is responsible for the CCS managed data centers, servers. and storage systems that provide infrastructure resources to applications and services used by staff, faculty and students. The Server and Storage Services group is also responsible for establishing standard server and storage platforms and for the management of the hardware and software required to integrate these platforms to deliver an efficient, scalable and cost-effective infrastructure.

⊛. Data Centers:

Data centers are simply centralized locations where computing and networking equipment is concentrated for the purpose of collecting, storing, processing, distributing or allowing access to large amounts of data.

Need of Data Center: Despite the fact that hardware is constantly getting smaller, faster and more powerful, we are an increasingly data-hungry species, and the demand for processing power, storage space and information in general is growing and constantly threatening to leave behind companies abilities to deliver.

Any entity that generates or uses data has need for data centers on some level, including government agencies, educational bodies, telecommunications companies, etc. Lack of fast and reliable access to data can mean an inability to provide vital services or loss of customer satisfaction and revenue.

What are the core components of a data center?

Data center design includes routers, switches, firewalls, storage systems, servers and application delivery controllers. Together they provide: Network infrastructure, Storage infrastructure and Computing resources.

How do data centers operate?

Data center services are typically deployed to protect the performance and integrity of the core data center components. Network security appliances include firewall and intrusion protection to safeguard the data center. Application delivery assurance maintains application performance, these mechanisms provide application flexibility and availability.

⊛. E-Government Architecture:

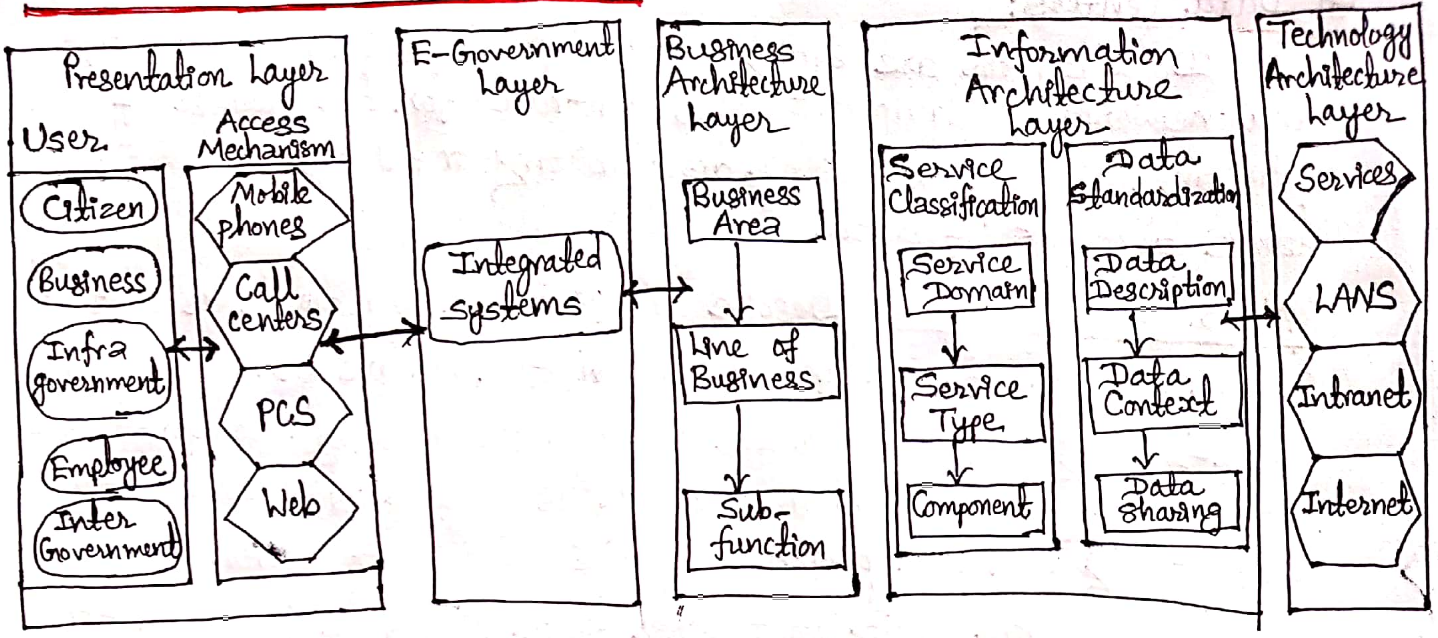

Fig: Overall E-Government architecture structure.

Presentation Layer: The presentation layer identifies and describes the system users, who require access to government information at different capacities, and the channels through which information can be accessed. It manages the user's interface with the system.

E-Government Layer: The main goal of e-government layer is to achieve a government that;
- ↳ does not ask for information it already has.
- ↳ is focused on better services
- ↳ will not allow it's facilities to be misused
- ↳ is well informed.

Business Architecture Layer: It provides a functional rather than organizational view. of the government's lines of business including it's internal operations and services for citizens. It describes government around common business, thus promotes agency collaboration.

Information Architecture Layer: It can be divided into two; Service classification and Data standardization. Service classification include Service Domain, Service type, and component & Data standardization include data description, data context and, data sharing.

Technology Architecture Layer: It categorizes the standards and technologies that support and enable the delivery of service components and capabilities. It also unifies existing agency technologies and e-government guidance by providing a foundation to advance the reuse and standardization of technology and service components from a government wide perspective.

⊛ Interoperability Framework:

Interoperability framework is Set of standards and guidelines which describe the way in which organizations have agreed, or should agree, to interact with each other. Set of standards and guidelines should be followed by public sector information systems and processes, in order to achieve technical, organizational and semantic interoperability during service provision. An IEFG (Interoperability Framework for E-Governance) involves a common structure which comprises a set of standards and guidelines.

Levels of Interoperability:

→ Organizational Interoperability (like process-re-engineering including Government-Orders, Process Changes, Organizational Structures).

→ Semantic Interoperability (Enabling data to be interpreted & processed with the same meaning)

→ Technical Interoperability (like technical issues in interconnecting ICT systems and services, information storage, security etc.)

The Multilateral mechanism for IFEG is influenced by following key sub-areas:

i) Political: For strategy related issues.

ii) Legal: For issues like IPR / Copy Right, privacy etc.

iii) Managerial: For issues like training, motivation.

iv) Economic: For funding related issues.

v) Social / Cultural: For social cultural factors like differences in culture, working practices, issues of trust, timings etc.

⊛. Cloud Governance:

Cloud Governance is a framework to govern the use of cloud services, not block them from using these services. A cloud framework includes people, processes and technology while ensuring security, cost management, and deployment acceleration. It helps in regulating and controlling the use of cloud services by defining process, standards, and policies to be followed in planning, operating and managing cloud services.

Key Benefits of Cloud governance framework:

i) **Controlled Access:** By selecting who owns each area of asset and software management, our cloud governance plan will build necessary limits on who can access and impact our cloud ecosystem. Controlling access to critical assets is vital and will enhance the reliability of our cloud processes.

ii) **Reduced Security Risks:** Our cloud governance plan will help us to identify vulnerabilities in our system, and establish metrics to measure the impact of security measures.

iii) **Enhanced Compliance Readiness:** Developing a cloud governance program allows us to build compliance review and standards into our processes and architecture.

iv) **Lowered Costs:** Cloud governance shifts workflows from analog to automated. Automated workflows reduces manpower, and reduced manpower means reduced costs.

Risk of Poor Cloud Governance:

→ Cloud Security Risks
→ Cloud Integration.
→ Cloud Portability and Interoperability
→ Cloud Vendor Lock-In
→ Cloud Applications Governance
→ Lack of Incentives for Consumers.
→ Shadow IT and Hidden Clouds.

Elements of Cloud Governance:

i) Cloud Business Office (CBO): It ensures alignment of cloud vision with business vision and ensures that governance is enforced across the enterprise. CBO is also responsible for demand management, cost optimization, and prioritization.

ii) Cloud CoE (Center of Excellence): It defines processes, regulates and standardize cloud adoption, migration and operation across the enterprise.

iii) Cloud governance organization structure and roles and responsibilities.

iv) Cloud governance processes around the cloud service lifecycle.

v) Cloud foundational components like cloud refrence architecture, standards, templates, guidelines etc.

⊛. E-readiness:

E-readiness (electronic readiness) is defined as a degree to which a country's economy may be ready, willing or prepared to obtain benefits which arise from information and communication technologies. It is the ability to use information and communication technologies (ICT) to develop one's economy and to foster one's welfare. E-Readiness is one of the important factor for the digitizing Society. The calculation of e-readiness deals with many kinds of social aspects related with Economical matters, Cultural matters, Literacy rate, Poverty etc. E-readiness, means the infrastructual pre-requisites for taking up any e-governance project. These infrastructural pre-requisites or preconditions may be identified as:

1. Data system infrastructural preparedness
2. Legal infrastructural preparedness.
3. Human infrastructural preparedness.
4. Institutional infrastructural preparedness.
5. Technological infrastructural preparedness.

1) Data Systems Infrastructure:

The core of e-governance is e-MIS, the electronic Management Information System. The data that were managed manually need to be computerized or bought into electronic form which means that the preparedness of computerized database or data warehouse is required. Data quality and data security are of prime concern here as most of the government infrastructures are not up to the mark in developing countries. This is the core computerization activity of any government process which may take several years to reach this stage.

2) Legal Infrastructure Preparedness:

They lack necessary laws and legal infrastructure to enable reengineering of the existing business practices, rules and regulations within the government at various levels. This seems to be highlighted in developing countries while developed countries have been significantly successful in administrative reforms and business reengineering. The fundamental question that arises here is "Are the laws and regulations required to permit and support the move towards e-governance initiatives in place?

E.g. Digital Signature Act.

3) Institutional Infrastructure Preparedness:

For any government to implement a successful e-governance project, the required institutional infrastructure must be in place which most of the government lack. The government body has to establish a separate IT department which basically coordinates with e-government projects within the nation. The IT department works out for the hardware selection and acquirement, network or software development and implementation and also the training of staff at various levels of government. Many countries still lack the institutional infrastructure.

4) Human Infrastructural Preparedness:

Human resource development by training is an essential requirement which comes from well trained manpower both technical and non-technical. The technical manpower resources are essential for all the phases of e-governance and related information system life cycle comprising systems analysis, design, programming, implementation, operation and documentation. Both private and government institutions should play a major role in this regard. Apart from technical human infrastructure, there is a need for training and orientation of user personnel. Such training will make them capable of handling e-governance projects.

5) Technological Infrastructural Preparedness:

Technology is fast changing in ICT domain and there is a requirement of great financial support time for software and hardware. Government organizations encounter this situation especially as their procedures. The technological infrastructure in developing countries including computing ~~tool~~ and telecommunication is absent. As a result software and hardware may not be compatible.

⊛ Need of E-Readiness:

The concept of e-readiness is important because it's level can be a strong predictor of how well a country can perform in the new economy. An e-readiness judgement would provide policy makers with a detailed score card of their economy's competitiveness relative to it's international counterparts. Further, a breakdown of indicators allows policy analysts to pinpoint areas of strengths and weaknesses, thus providing a balanced perspective in guiding a country through the digital transformation.

⊛MIS: A management information system (MIS) is a computer system consisting of hardware and software that serves as the backbone of an organizations operations. An MIS gathers data from multiple online systems, analyzes the information, and reports data to aid in management decision-making.

MIS is the study of people, technology, organizations, and the relationships among them. MIS professionals help firms realize maximum benefit from investment in personnel, equipment, and business processes. MIS is a people-oriented field with an emphasis on service through technology.

⊛ Networking Hardware:

Networking hardware are electronic devices which are required for communication and interaction between devices on a computer network. Specially, they mediate data transmission in computer network.

1). **Routers:** The router is a physical or virtual internetworking device that is designed to receive, analyze, and forward data packets between computer networks.

2) **Switches:** A switch is a hardware device that connects multiple devices on a computer network. The switch contains the updated table that decides whether the data is transmitted or not. Switch delivers the message to the correct destination based on physical address present in incomming message.

3) **LAN cards:** A LAN card connects a computer to a network. LAN cards are typically built in our computer.

4) **Hub:** A Hub is like switch that divides the network connection among multiple devices. When computer requests for some information from a network, it first sends the request to the Hub through cable.

5) **Cables:** Network cables are used to connect and transfer data and information between computers, routers, switches, and storage area networks.

⊛. Networking Software:

Networking software is a foundational element of any network. It helps administrators deploy, manage and monitor network.

1) Network operations and management: Network operations management Manage, Automate, and Ensure Compliance for physical, virtual, and Software-Defined Networks.

2) Operating Systems: An operating system is the most important software that runs on a computer. It manages the computer's memory and processes, as well as all of it's software and hardware.

3) Firewall: A firewall is a system designed to prevent unauthorized access to or from a private network. We can implement a firewall in either hardware or software form, or a combination of both.

⊛. Network Services:

A networking service is a low-level application that enables the network to perform more than basic functions.

1) T-1 Line: It is a communication transmission service that uses 2 twisted pair copper wires to transmit and receive data or voice traffic. A T-1 line can transmit data at a speed of 1.544Mbps.

2) DSL: It stands for "Digital Subscriber Line". It is a communications medium used to transfer digital signals over standard telephone lines.

3) Satellite: A satellite is an object in space that transmits data.

4) Wireless protocols: They are used to connect computers, laptops and smartphones. The more widespread and standardized protocols are Wireless LAN or Bluetooth.

5) IP Addressing: IP address is a numerical label assigned to each device connected to a computer network that uses Internet Protocol for communication.