E-Governance

(Elective II)

EG3204CT

Sixth Semester

Notes

Prepared by

Laxmi Yadav & Sushant Sharma

Diploma in Computer Engineering

Unit 1 Introduction

E-Governance refers to the utilization of information and communication technology for providing government services, disseminating information, communication operations with the general public. It encompasses the digital transformation of government operation to ensure transparency, accountability and accessibility.

E-Government refers to the use of information system and technology by government agencies to provide public services and administration at different levels, enhancing efficiency, productivity, and citizen management. It aims at making government digitally interactive with citizen (G2C), with other government agencies (G2G), with employees (G2E), with business (G2B). The development of e-government capabilities is an important undertaking because it is not only rapidly changing the way that government supply information, deliver services, and deal with public, but they are also becoming an integral part of government strategies.

History of e-Governance development.

E-Governance :- the use of digital technology in government processes, began in the 1990s with the internets rise. The initial stage involved simple information distribution on government websites. The 2000s saw the second phase which included interactive services like online forms and payments. The focus shifted to improving transparency, efficiency and citizen participation in governance. The 2010s introduced mobile governance (m-governance), cloud computing and data analytics, enhancing public service delivery and decision making. The latest stage emphasizes integrating AI and block chain to secure data, streamline services and make governance more responsive and personalized.

How e-Governance works.

E-Governance works by integrating information and communication technology (ICT) into government functions to enhance the delivery of services. It uses digital platforms like

websites, apps, and portals to offer services such as tax payment, licence renewals, and grievance (गुनासो) redressal (निराकरण). These system operate on secure network, database, and software to manage information and automates processes. E-Governance also employs electronic communication and digital records to improve transparency, reduce corruption and make decision-making more efficient.

Categories of e-Governance.

There are several types based on its scope and functionality:

(i) Goverment to Citizen (G2C)
(ii) Goverment - to - Busmess (G2B)
(iii) Goverment to Goverment (G2G)
(iv) Goverment - to Employee (G2E).

* Goverment - to - citizen (G2C):

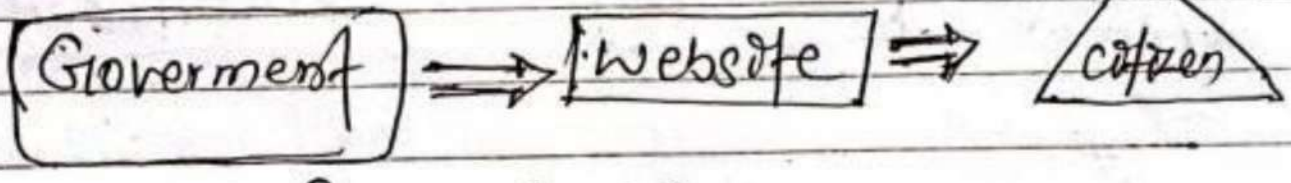


fig: G2C

G2C refers as a category of e-governance

where goverment services are provided directly to citizens through digital means. By using websites, mobile apps and online portals, G2C services reduce the need for in person visits to goverment offices, streamline processes, and improve the overall efficiency of service delivery. This includes online activities such as filing taxes, applying for social security, renewing passports and accessing public records. Its goal is to make interaction with the goverment easier and more convenient.

* Goverment-to-Business (G2B).

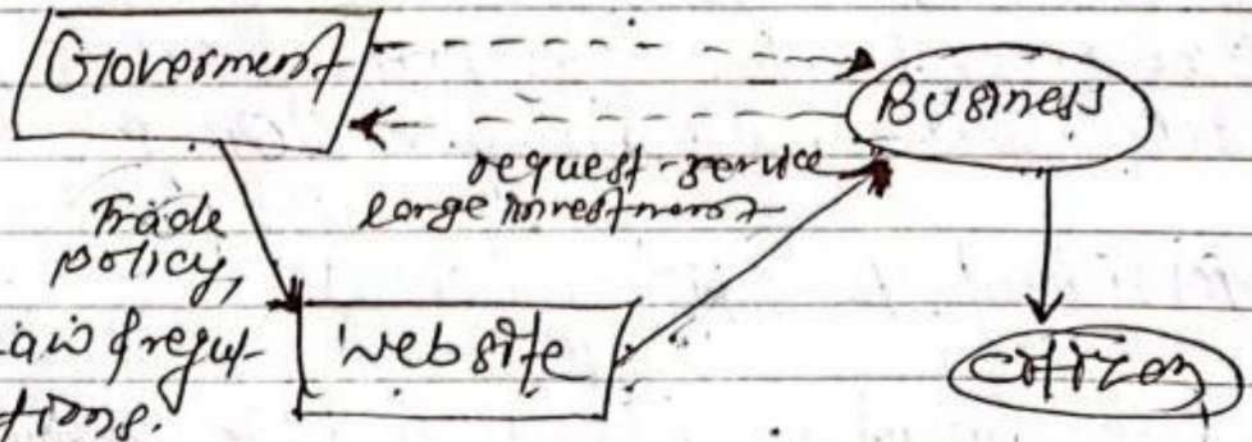
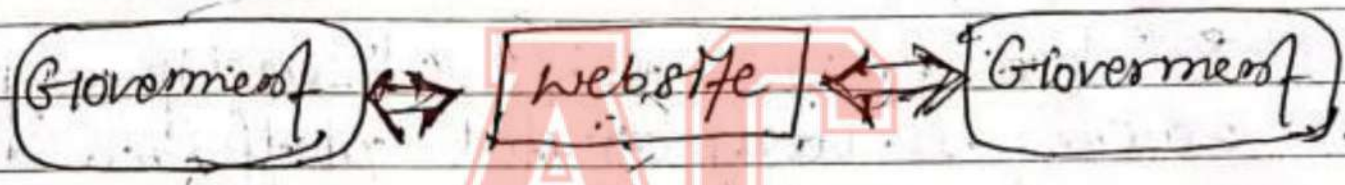


Fig: G2B

G2B refers to business specific transactions (such as payments,

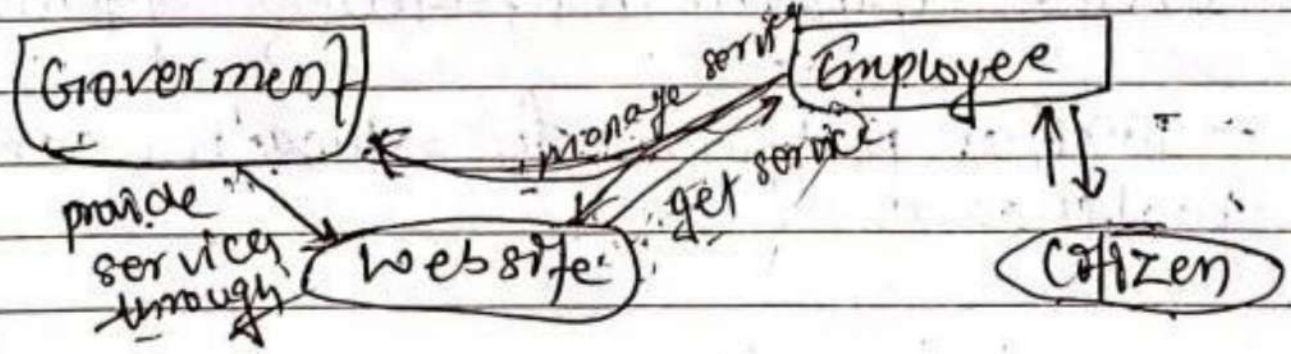
selling of goods and services) and the provision of business-focused services online. By using online systems; businesses can access necessary service more quickly and manage their regulatory requirement more effectively. It helps to reduce administrative burdens and improve efficiency of transaction between the governments and businesses.

* G2G (Government-to-Government).



G2G refers to the digital communication and data sharing between different government departments and agencies. The main purpose of government to government is to increase efficiency and boost performance to improve the outcome.

* G2E (Government to Employees)



Government to Employee, generally refers to how the government as an employer manages and interacts with its employee who are called civil servants or public employee. It also includes hiring, paying salaries, giving promotion, providing benefits and setting rules and responsibilities for their employees.

Applications of E-Governance

- It encourages digital citizenship engagement through digital platform.
- It includes data management tools for government agencies.
- Secure digital storage of government records
- Access to government service online
- Online complaint and feedback systems.
- Digital platform for education and healthcare.

Global Trading Environment:

Generally, it refers to the international context in which trade occurs. It includes the global market dynamics, trade policies, regulations, and economic conditions that influence how countries and businesses conduct trade with each other. It encompasses factor like trade agreements, tariffs and trade barriers that affect international trade. Due to the global trading environment, the whole has become a global village.

Adoption of e-commerce governance:

This refers to governments using digital technologies to manage their operation and services. It makes services more convenient for citizen, improves data management, strengthens security and encourages greater public participation. Efficient e-governance system make a country more attractive for global business and investment. It helps to reduce corruption and save money by cutting down on paper work and increase transparency to the next level.

Benefits of E-Government.

- Easy implementation of Right to Information.
- Makes government services more convenient and accessible.
- Reduces administrative and paper work costs
- Improved interaction with different groups and citizen.
- Increases communication between various government agencies.
- It helps in improving the quality of public services.
- Organize and analyze data more effectively.

[E-Government Life Cycle]

The e-Government life cycle is the series of stages involved in the creation, deployment and manageme of digital government services.

It includes :

(a)

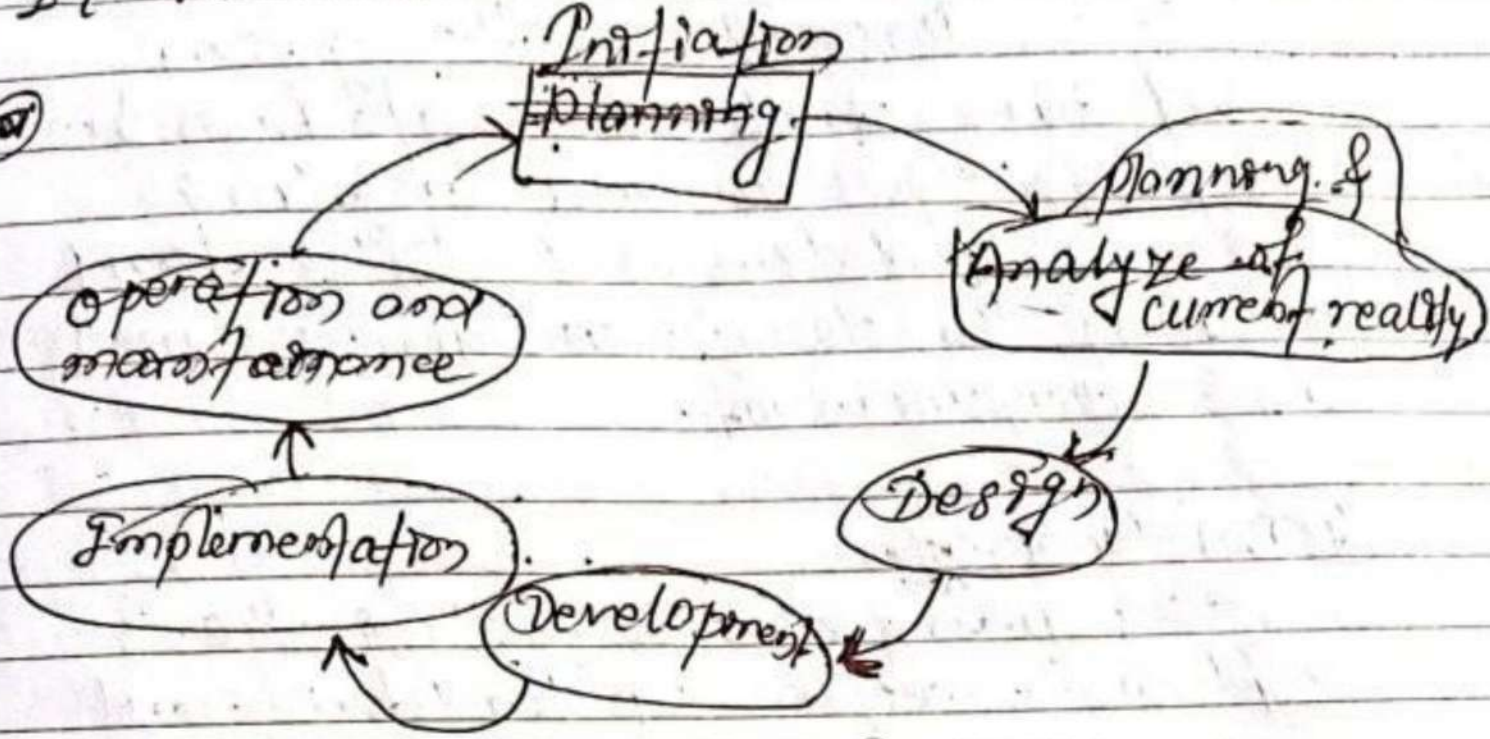


Fig: E-Government Life Cycle

* Initiation (शुरुवात): This step involves recognizing the need for digital government services and setting clear objectives. It includes gathering support and securing funds for the project.

eg Planning & Analyze of current reality. In this stage, a comprehensive plan is created to guide the project through its lifecycle. Analysis is also done to overcome from those problem of daily lifes in reality.

③ Design:
In this phase, the system architecture and user interface are designed. This includes creating mockups, defining workflow and ensuring the design meets user need and requirement.

④ Development:
This phase involves coding the software; setting up hardware and integrating various component to build the complete system.

⑤ Implementation:
The system is deployed and put into operation. This phase includes installing the system, configuring it for use, and training users on how to interact with the new system.

⑥ Operation & maintenance:
Once the system is live, it is continuously managed and maintained. This involves monitoring performance, providing user support and making updates based on feedback and changing need.

Difference between traditional government and e-governance.

Traditional Government	E-Governance
• It is a traditional concept in which services are provided to public involving face-to-face meeting.	It is a modern concept on which services are provided to public through online platforms
• It is an ancient and still in usage where the digital network is not reachable.	It is used to save the valuable time of the citizens.
• It can be only available during a limited time duration.	It is available round the clock.
• It can be in any form which is non-electronic or manual form.	It can be only in electronic of digital mode only.
• It can be slow due to manual processes and paperwork. • Information might be harder to access.	It speeds up processes through automation and digital tools. • provides more accessible information online

Advantages of e-Governance

- Makes goverment operation quicker and more efficient.
- Better Access to the services
- More citizen engagement
- Quick response
- Environmental benefits by saving paper.
- Store data in an organized way.

Disadvantages

- Unequal access to technology
- Cyber security risks
- Expensive setup and maintenance
- Difficult to navigate for some users
- Concerns about data misuse
- Need for training user and staff.
- Some prefer traditional method.
- Problems occurs if technology fails.

Online service delivery

Online service delivery is an effective way to build closer relationship with customers, partners and the public while simultaneously cutting costs and reducing delays.

pros

→ It is fast and reliable.
→ Can access services anytime from anywhere.
→ We can pay when we get our order.
→ It saves your time in visiting the store.
→ Reduce operational and administrative cost.

cons

→ It only can be done online.
→ Sometimes, we don't get our desired product.
→ It could be more expensive than self visiting the store.
→ It is totally dependent on technology.
→ Not every one has internet access.

Electronic Service delivery:

Electronic service Delivery (e-services) is a type of service delivery which are provided to citizens or businesses through electronic means, typically via the

internet. It may include e-commerce and also non-commercial services provided by the government.

Advantages
- Can be accessed anytime.
- Reduces operational costs.
- Less physical documentation.
- Improved tracking
- User-friendly interface

Disadvantage:
- Privacy concern
- High set up costs.
- Risk of hacking or data breaches
- Fully dependent on technology.
- User face difficulty to navigate.
- Some prefer traditional methods

Maturity and adoption model

Maturity model

A maturity model is a framework that helps organization evaluate and improve their processes over time. This model shows how

and organization can progress from having ad-hoc processes to having well-managed and optimized processes. It consists of several levels for stages that represent increasing levels of maturity. Each level describes how what an organizations processes look like at that stage and provide guidelines for moving to the next level.

Advantage

→ Provides a clear path for growth.
→ Allows comparison with industry standards.
→ Aligns stakeholders around common goals.
→ Offer specific guidance for advancement.
→ Identifies and reduce potential risks.

Disadvantage

→ Require significant time and effort
→ May be to prescriptive
→ Potential for misuse
→ Not easily adaptable to all context.
→ May neglect flexibility and innovation.

Adoption Model:

Adoption model is a framework that helps to understand how new ideas, products or technologies are accepted and used by people or organizations. It breaks down the process into different stages and identifies the factors that influence how quickly and widely something is adopted.

Advantage

→ Helps to estimate how quickly people will accept and use something new
→ Improve strategy planning
→ Enable targeted efforts.
→ Facilitate smoother implementation.

Disadvantage

→ Not always adaptable to all context
→ Assumes a linear adoption process.
→ May oversimplify.
→ Can overlook cultural difference.

Unit-2 Models of e-Governance.

In Nepal, various models of e governance have been implemented to improve goverment services and enhance trasparency, accountability and efficiency. Some models of egovernance are;

Models of e-Governance

(1) G2C (Goverment to citizen)
→ To deliver services directly to the public through digital platform.
→ Saves time and reduce the need of people to visit goverment offices.
→ For example: Online application for passport & driving license.

(2) G2B (Goverment to Business)
→ Make interaction between goverment & business.
→ Easily operate business by reducing paper work and processing time.
→ Online business registration, tax filing and permits.

(3) (G2G) (Goverment to Goverment)
→ Improved communication and data sharing between different goverment departments.
→ Enhance coordination and efficiency within the goverment.

(iv) G2E / Government to Employees.

→ To provide online services for goverment employees.

→ Automates routine tasks and ensures timely access to employee information.

→ Payroll management, pension processing and HR management system.

E-procurement

The public procurement monitoring office (PPMO) has implemented an e-procurement system to handle goverment purchase and tenders. This model allows supplier to participate in goverment tenders online.

→ promotes transparency, reduces corruption and ensures fair competition among suppliers.

Major challenges of G2G

→ Data security issues.
→ Vulnerability to cyber attack
→ Intellectual property
→ Lack of knowledge and awareness.
→ Resistance to change
→ poor internet and old devices.
→ Maintaining day to day backup

Development of G2B Governance

In Nepal, The government has been working to improved the business environment and fostering economic growth. The government is also focusing on digital tools like the Electronic Single window (ESW) to simplify trade and business process. They have also introduced reforms to make things like company registration, taxes and investment more straightforward. There's an emphasis on public-private partnership, to improve infrastructure and services Efforts are also being made to cut down on red tape and make regulation clearer. There are programs and incentives to support small and medium business, which are important for the economic growth of the country.

Overall, these aim to create a better environment for businesses to thrive.

Different between G2C and G2B e-gov

G2C	G2B
• It targets citizens.	It targets Business & companies.
• It provides services directly to individuals.	It facilitates government-business interaction.
• It focuses on making government service more accessible.	It focuses on streamlining regulatory and business processes.
• It aims to enhance citizen satisfaction.	It aims to reduce hurdles for businesses.
• For example: online tax filing and e-passport.	Examples include online business registration and e-procurement.
• It simplify interaction between citizen and government	It encourage more business by friendly environment.

(4) G1 2 G1 and G1 2 E

G1 2 G1	G1 2 E
① It targets different govermen agencies and departments.	It targets different govermen agencies employees.
② Facilitate communication and data sharing between govermen entities	provides tools and services to help employees with their work.
③ Helps to improve collaboration among govt bodies.	Focus on making work easier and efficient for emp.
④ It aims to reduce redandancy.	It aims to satisfy employee needs.
⑤ Ensure cohesive and effective functioning of govermen as whole.	Create a more effective and motivated govermen work-force.
Example: inter agency data sharing platform, joint decision-making system.	Examples Online payroll system, employees portal, training programs.

Unit 3 E-Governance Infrastructure

E-Governance infrastructure is the foundational framework that enables the effective delivery of government services and information through digital channels. It includes the technological, legal and organisational components required to implement and manage e-Governance. Here's the overall infrastructure given

(1) Application architecture

It refers to the structured design of software applications, focusing on how various components interact and are organized. It ensures that applications are scalable, secure and integrated effectively

(2) Support system

It refers to the mechanism and services that ensure the continuous and efficient operation of e-governance applications and services. It provide technical assistance and maintenance. They include help desks, technical support team that help to ensure the smooth operation of e-governance system.

(iv) Data center
→ A facility used to house critical servers and storage systems that manage and protect government data. It provide the physical infrastructure necessary for data storage, processing and backup.

(v) Government Gateway
→ A centralized platforms that provide access to various government services and systems. It acts as a bridge between different government departments and the public, facilitating interactions and transactions.

(vi) Open source software
→ Software with source code that is freely available for modification and distribution. In e-governance, open source software can be used for various applications, promoting cost-effectiveness and flexibility.

(vii) Free software
→ Software that is not only free of cost but also allows users to run, modify and distribute it. Similar to open source software, free software supports transparency and

community driven development.

EDI (Electronic Data Interchange)

→ A technology that allows the exchange of business documents between organization in a standardized electronic format. It facilitates seamless communication and transaction between government agencies, businesses, and other external partners. It relies on predefined standards to format data so that it can be understood and processed by different systems. These standards ensure that data is consistent and can be easily interpreted across various platforms. The standards are:

ANSI X12:

The American National Standards Institute (ANSI) developed the X12 standard of electronic data interchange. It defines a set of transaction sets, data elements and control structure for various business documents.

(iv) EDIFACT:

The Electronic Data Interchange for Administration commerce and transport is an international standard developed by the united nation. It provides a common syntax and structure for electronic messages. EDIFACT supports a wide array of messages such as orders, invoice and custom declaration. Its messages are made up of segments that include data elements, similar to ANSI X12. However, It uses a different syntax and set of delimiters, making it distinct from ANSI X12.

(v) TRADACOMS:

TRADACOMS is an older system used for exchanging business documents electronically, mainly in the UK's retail industry. It was developed in the 1980s to help businesses like stores and suppliers communicate more efficiently, without using paper. It works by organizing information into sections, such as the product ordered, prices and delivery details. Order, Invoice, Delivery Note, Receipt confirmation and Credit Note are the types of document used in TRADACOMS

④ GST EDI (Goods and Services Tax EDI)
↳ GST EDI refers to the electronic system used for filing and processing of GST related documents and transactions. GST EDI system in Nepal is an essential step towards modernizing tax administration, making compliance easier for businesses, and improving the overall efficiency of government services. It facilitates the electronic submission of tax returns, invoices and other relevant document to the Inland Revenue Department (IRD).

Protocols of EDI

↳ It is defined as the method and standards for transmitting EDI message between trading partners. There are the protocols used in EDI,

(i) AS2 (Applicability Statement 2).
(ii) FTP / SFTP.
(iii) VAN
(iv) HTTP / HTTPS.

(i) AS2

AS2 is a popular protocol used to securely send and receive business documents over the internet. It encrypts data using digital signatures to ensure that the information is safe and authentic. It works with various systems and file types, making it easy for different businesses to connect.

(iv) FTP/SFTP

FTP is used to transfer files between a client and server. It is less secure because it transmits data in plain text.

SFTP is a secure version that uses SSH (Secure Shell) to encrypt the data being transferred, providing a higher level of security.

(v) VAN

It is a private network provider that facilitates the exchange of EDI documents between businesses. It typically charges service fees, which can vary based on the volume of data exchanged and specific services provided.

(8) HTTP / HTTPS.

HTTP

protocol for transferring data over the web. Transmit data in plain text, making it less secure. Commonly used for general web browsing.

HTTPS

Secure version of HTTP using SSL/TLS. Encrypts data for confidentiality and integrity. Essential for secure transactions like online banking.

* (Components of EDI)

It typically consists of several components. Some are:

(1) Standard format:
→ EDI uses standardized format for structuring data, ensuring consistency across different systems.

(2) Communication protocol:
→ AS2 and FTP are popular for transmitting

EDI document security.

(iii) EDI software:
→ Applications like ERP systems or dedicated EDI solution for creating and managing EDI transactions.

(iv) Mapping Tools.
→ Software that translate data between internal formats and EDI standards.

(v) Trading partner agreement:
→ Essentials for defining the rules and expectations for EDI transaction between businesses.

Electronic Fund Transfer
→ EFT refer to the process of moving money electronically between bank accounts. It includes various method like direct deposits, wire transfer, and online bill payment, allowing individuals and business to transfer funds quickly and securely without the need for physical checks or cash.

Unit - 4

Mobile Governance

Mobile Governance : also known as m-governance. It involves using wireless handheld devices like cellphones and tablets to enhance the effectiveness and efficiency of government operation and services. It focuses on empowering citizens by making government services more accessible via mobile devices.

Application of M-Governance.

(1) E-government services :
- Access to services like tax payment and license renewals.

(2) Emergency services :
→ Real time alert for emergencies.

(3) Health services.
→ Telemedicine and health information access.

(4) Education.
- Online resources and communication tools.

⑤ Voting:
- Voter registration and information.

⑥ Transport Management:
- Public transport schedules and traffic updates

Advantages of M-Governance

- Immediate updates from goverment agencies.
- It enhances emergency management through timely alerts.
- Service can be personalized based on user prefences.

⇒ Allow citizen to access services anytime; anywhere
→ It reduces Administrative cost by minimizing paperworks.
⇒ Enhances efficiency by reducing time & cost.
⇒ It encourage citizen engagement and feedback.
⇒ It helps to collect data for better decision making.

Wireless application protocol

WAP stands for Wireless Application Protocol. It is a protocols designed for micro-browsers and it enables the access of the internet in mobile devices. It enables creating web applications for mobile devices. WAP was important for early mobile browsing but has mostly been replaced by newer technologies. It includes a gateway that connects phones to the web. It simple language called WML for creating mobile-friendly pages and a feature that sends content directly to users

WAP Browsers

A wireless access protocol (WAP) browsers allows mobile device such as older cellular phones to access compatible web content. The mini-browser can use multiple internet protocols to

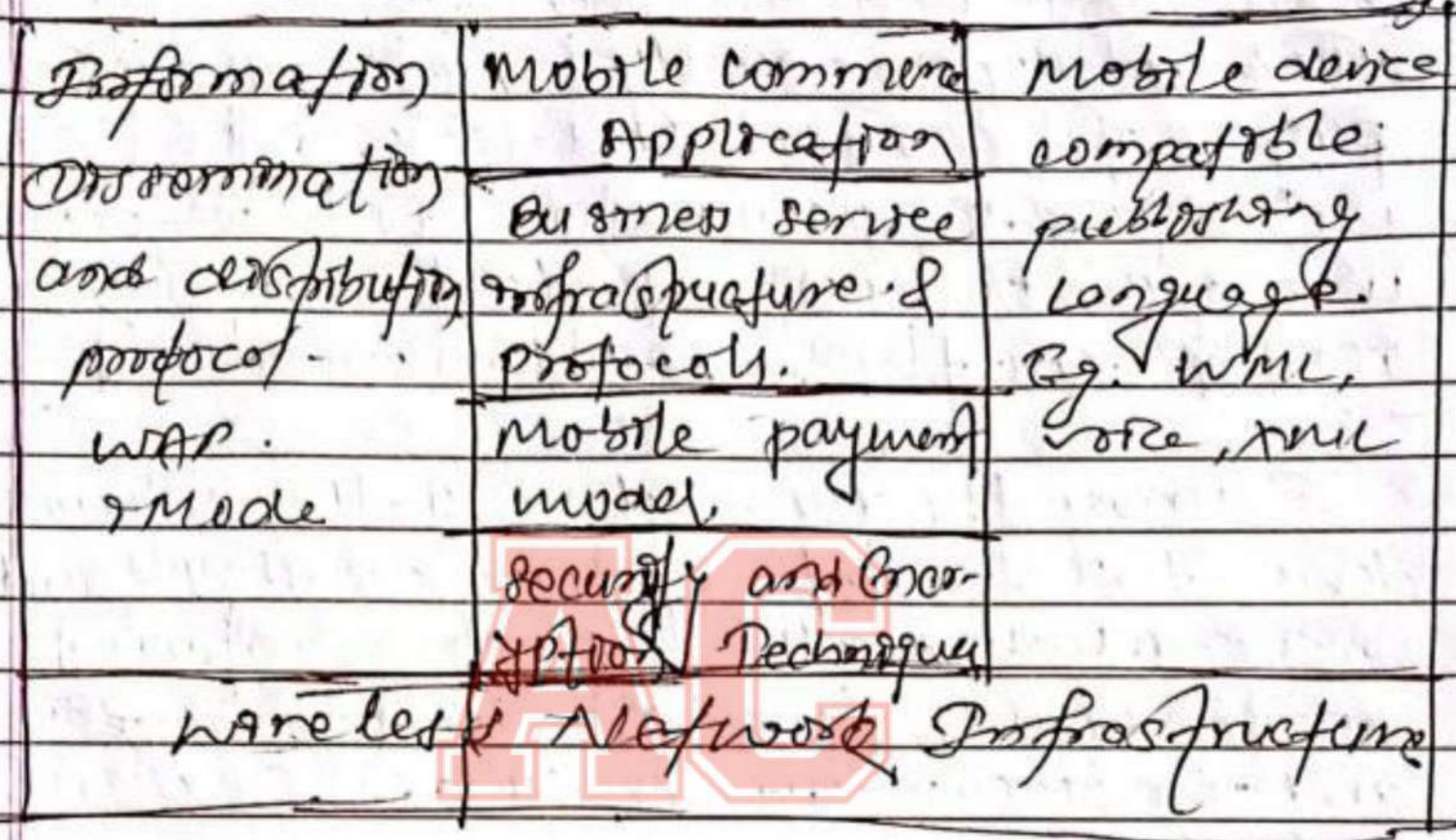
render web pages into plain text or simplified versions of the original web pages. In order for a WAP browser to be effective, web developers usually create seperate WAP pages for mobile devices. Otherwise, without WAP optimization, web content will usually take longer to load and may not render correctly in older mobile devices.

During the early days of the internet, mobile devices had limited system resources and screen size; which made loading internet based content such as email, instant messaging and newsgroups as challenge.

Mobile Commerce Architecture

Mobile commerce Architecture refers to the structure and design of system that facilitate services through mobile devices. It includes various components like mobile application, payment gateway, user interfaces, and back-end system that work together. It need a reliable wireless network, different protocols for business services, mobile payment models and security and encryption tech.

ariques: The architecture of mobile commerce is drawn below:



Wireless Network Infrastructure.

→ For successful m-commerce there must be strong wireless network infrastructure. Wireless network have evolved from voice-only radio based analog transmission to digital voice and data transmission.

Security and Encryption.

→ Mobile commerce can be made secure by using different kinds of

security protocols. Encryption and decryption take place algorithm can be adapted for extra security. SSL and TLS security measures can be adapted.

Mobile payment Models

→ Online payment is a fundamental necessity of mobile commerce. Some examples of mobile payment are mobile wallet, debit card, credit card, paypal. There are three main mobile payment model.

(i) Acquire centric Model.
(ii) Issuer centric Model.
(iii) Mobile Network operator.

Unit 5 Technology for Online Business

IT Infrastructure.

IT infrastructure refers to the combined set of hardware, software, network facilities and services that are needed to develop, test, deliver, monitor, control or support IT services. It forms the foundation on which all IT services and solutions are built and operated.

key Component of IT infrastructure.

(1) Hardware
- physical devices like servers, computers, storage devices, routers and switches.

(2) Software:
- Application, operating system and enterprise software solution that run on the hardware

(3) Networking
- Connectivity component, including internet connections, intranets and network infrastructure. (eg. LAN, WAN)

(4) Data Storage:
Systems for storing, managing and backing up data; such as databases, storage area networks

and cloud storage.

(5) Facilities
physical spaces like data centers where hardware is housed and maintained.

(6) Security
Measures and tools to protect IT infrastructure, including firewalls, antivirus software and encryption.

Internet
Internet is a world wide, publicly accessible computer network of inter-connected computer network that transmitted data using the standard internet protocol. The largest internet network in the world is internet.
The internet forms a well known component of the global information distribution network. It targets a wide range of e-governance application such as information publishing, information retrieval, video conferencing and many more. It also includes search engine that help users to find information on almost any topic

It also provide access to a range of services, including browsing websites, sending emails, sharing files and using communication tools like chat and video calls.

Intranet

An intranet is a private network used within a company or organization to share information and resources securely among its members. Unlike the public internet, an intranet is only accessible to people inside the organization. It helps with internal communication, file sharing and hosting important application like HR system and project tools. It is protected by security measures to ensure that only authorized users can access it, making it a secure way to manage and share information within an organization. It is also a useful tool for managing internal operations and improving teamwork.

Extranet

The extranet is the private network that use the internet that allows people outside business. Internet protocol network connectivity and public communication

system to secretly share part of business information or operation with supplier. An extranet can be viewed as part of a company's intranet that is extended to users outside the company. It is similar to an intranet but is accessible to authorized external users. This helps the organization to collaborate, share information and communicate more effectively with these external parties, all while keeping the rest of the internal network secure.

VPN

A virtual private network (VPN) extends a private network across a public network and enable user to send or receive data across shared or public network. A VPN is created by establishing a virtual point-to-point connection through the use of dedicated circuits or with tunneling protocols over existing network. A VPN available from the public network internet can provide

some of the benefits of a wide area network (WAN) from a user perspective, the resource available within the private network can be accessed remotely. This connection helps protect your online activity from being seen by others, such as hacker or your internet service provider.

Firewall

A firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established policies. It is an essential barrier that sits between a private internal network and the public internet. It allow non-threatening in and keep dangerous traffic out.

Types of Firewall

- Packet filtering:
  data is analyzed and distributed through filter standard

- Proxy service
  protects message at application layer.

- Stateful inspection.

Dynamic packet filtering that monitors active connections to determine which network packet to allow through the firewall.

- Next Generation Firewall (NGFW)
Deep packet inspection firewall with an application level inspection.

Cryptography

A cryptography refers to a method or algorithm used to secure information by transforming it into an unreadable format known as cipher text, that can only be read by someone with the correct decryption key. It ensures the protection of data during storage and transmission against unauthorized access and tampering (छेड़छाड़).

Types of cryptography

Symmetric key cryptography

It is an encryption system where the sender and receiver of a message

use a single common key to encrypt or decrypt messages. The most popular symmetric key cryptography is Data Encryption System (DES).

Asymmetric key Cryptography

A pair of keys is used to encrypt or decrypt information. A public key is used for encryption and a private key is used for decryption. The both public key and private key are different.

Hash function

There is no use of any key in this algorithm. A hash value with a fixed length is calculated as per the plain text which makes it impossible for the content of plain text to be recovered. Many operating system use hash function to encrypt passwords.

Private key

A private key is typically a long, randomly, or pseudo-randomly generated sequence of bits that cannot be

easily guessed. It is also known as a secret key. It is a variable in cryptography that is used with an algorithm to encrypt and decrypt data.

Public key.

A public key is a large numerical value that is used to encrypt data. The key can be generated by software but often provided by a trusted, designated authority and made available to everyone.

Digital signature

A digital signature is a unique cryptographic code that is attached to the documents, email, software, and digital certificate. It can be used to prove ownership of the certificate. When a digital signed file is present it can use key pair linked with that signature to verify it. There is also a hash function. The hash function performs while signing that serves as a checksum. The digital signature is that let the clients know that the entity is trusted and that what is

signed as authentic.

Digital certificate

A digital certificate is a cryptographic file that binds key pairs to validate an entity. When digital is issued, it is signed by a certificate authority (CA) that is issuing it. When the client is digitally certified by a certificate authority, this means that the client can be trusted. SSL certificate is an example of a digital certificate.

Certificate Authority

A certificate authority (CA), also sometimes referred to as a certification authority is a company or organization that acts to validate the identities of entities and bind them to cryptographic keys through the issuance of electronic document known as digital certificate.

Hypertext

Hypertext is a text based system that allows user to navigate between pieces of information by clicking on links

It is commonly used on the internet where web pages are interconnected via hyper links, enabling users to jump from one page to another pages

Hypermedia expands upon the concept of hypertext by incorporating various media types such as images, audio, video and interactive elements alongside text. This richer form of communication enhance the user experience by providing more engaging and diverse content; Web pages, multimedia presentation and interactive application are example of hypermedia

HTTP

HTTP stands for Hyper Text Transfer protocol. It is the foundation of the world wide web, and is used to load webpages using hypertext links. HTTP is an application layer protocol designed to transfer information between networked devices and runs on top of other layers of the network protocol stack. In HTTP, the error can be reported without closing the connection.

It allows HTTP pipelining of requests or responses. Since there are few TCP connections. Hence network congestion is less.

Characteristic of HTTP:

- Any type of content can be exchanged as long as the server and client are compatible with HTTP.

- It includes caching, connection management and content negotiation.

- It is human readable, uses method like GET and POST.

2. Client send request to server and server responds with resource like HTML pages.

=> Its design principle have shaped much of how the modern web operates

Unit-6

Electronic payment system (EPS)

An electronic payment system (EPS) refers to a digital system or platforms that facilitates financial transaction over the internet or other electronic network. It allows consumers and businesses to exchange money electronically by passing traditional paper-based methods like cheque or cash.

Online Banking

Online banking allows a user to conduct financial transaction via the internet. Online banking is also known as internet banking or web banking. Online banking offers customers almost every service traditionally available through a local branch including deposits, transfer and online bill payment. It requires a computer or other device, an internet connection and a bank or debit card. In order to access the service, clients need to register for their bank's online banking service. In order to register they need to create a

password. Once that's done, they can use the service to do all their banking.

EPS

An electronic payment system is a way of making financial transaction or paying for goods and services through electronic medium without the use of cheque or cash. It is also known as online payment system.

Types of EPS

* Credit payment system.

① Credit Card:
→ A form of electronic payment system which requires the use of a credit card issued by a financial institution to the card without the use of cash.

② E-wallet:
It is the form of prepaid account that stores user financial information like debit and credit card information for make an online transaction easier.

④ Smart card.
A plastic card with a microprocessor that can be loaded with funds to make transactions. They are also named as chip card.

* Cash payment system.

① Direct debit.
→ A financial transaction in which the account holder instructs the bank to collect a specific amount of money from his account electronically to pay for goods or services.

② E-cheque
→ It is a digital version of an old paper cheque. It is an electronic transfer of money from a bank account, usually a checking account without the use of paper cheque. It uses digital signatures.

③ E-cash:
A form of electronic payment system where a certain amount of money

is stored in a client device and is available for online transactions

Security requirements of EPS

1. Authentication
   → Implement multifactor authentication for users and systems

2. Encryption:
   → Different mathematical algorithms are used for encryption and decryption of messages

3. Integrity
   → Ensure data is not altered and maintain secure logs.

4. Non-repudiation:
   → Use digital signatures and audit trails to confirm transaction authenticity.

5. Authorization:
   → Implement role-based access control and transaction limits

6. Privacy :- Follow data protection laws and protect user information.

SSL (Secure Socket Layer)

SSL is a protocol for general purpose secure message exchange. It was developed by Netscape for the secure online transaction. It uses a combination of public-key and symmetric key encryption to safeguard data transaction. The techniques of hash function is used for this purpose. SSL protocol use a digital certificate but there is no payment gateway.

SET (Secure Electronic Transaction)

Secure electon transaction or SET is a system which ensures security and integrity of electronic transaction. It was developed by MasterCard and visa to secure web browses for a bank card transaction. The dual signature mechanism is deployed by SET to safeguard a transaction. The technique of digital signatures is used for this purpose. SET

protocols hides the customer credit card info from the merchant and hides the info to the bank. to protect privacy.

Payment System

A payment system is an electronic payment technology that contains several procedures including a payment processor which can be divided into two parts.

① Front End processors:
→ They have connections to various card association and supply the merchant bank.

② Backend processors:
→ These processors accept settlement from front end processors.

Payment Gateway

A payment gateway is a merchant service provided by an e-commerce application for service providers that authorizes credit card or direct payment processing for e-commerce. A payment gateway facilitates payment transaction by the

transfer of information between a payment transaction by the transfer of information between a payment protocol like chrome, website and front end processor for acquiring a bank.

Online payment processing

Online payment processing refers to the digital systems and services that facilitate the transfer of funds between a buyer and seller over the internet. These system enables businesses to accept payment from customers using various payment methods such as credit cards, digital wallets, and bank transfer.

Payment processing Network

For the payment system, it is important to handle the transaction between a merchant and the customer. There can be a series of inter connections to the payment

processing network. The payment network sets the interchange fees charged during payment processing. It helps the electronic that the transactions are processed correctly including set guidelines and qualifications requirements for member institutions.

Digital wallet

Digital wallets is a software based system that securely stores user payment information such as credit/debit cards, debit or bank account info and allow them to make payment online or in person without the need to use a physical card. It can also stores other personal information like loyalty cards, coupons, and tickets. By using a digital wallet, users can complete purchases easily and quickly with near-field communications technology.

Unit-7

Security Issues in e-Governance

1.1 Security issues in e-Governance refer to the challenges and vulnerabilities related with safeguarding digital platform used by governments for public service delivery. These platform can handle large amount of data. It also protects from cyber threats and unauthorized access. Security issues arises due to weak authentication mechanisms, data breaches, inadequate encryption, phishing attacks and insider threats.

Here are the security issues of e-governance.

(1) Data privacy and protection.
→ protecting sensitive information from breaches

(2) Cyber attack.
→ Threats like phishing, and DOS.

(3) Network security.
→ Securing communication between users and government server

① Insider Threat:
→ Risks from employees misusing access.

② Authentication and Authorization.
→ Ensuring only authorized user's access system

[Risks Involved in E-Governance.]

→ Online Security Breaches.
→ Privacy Issues
→ Intellectual Property Infringement
→ Product Liability Issues.
→ Human Error.
→ Platform Downtime
→ Property and Inventory Damage

[e-Governance Security Tools]

Security Tools in e-governance are system and technologies designed to protect integrity, confidentiality and availability of digital government services. Key Types includes

Firewalls

- Protects network from unauthorized access and cyber threats by filtering incoming and outgoing traffic.
At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public network. A main purpose is to allow non-threatening traffic in and to keep dangerous out.

Types of firewalls

- Packet Filtering:
A small amount of data is analyzed and distributed according to the filter standards
- Proxy service.
Network security system that protects while filtering messages at the application layer.
- Stateful inspection.
Dynamic packet filtering that monitors active connections to determine which network packet to allow through the firewall

- Next Generation Firewall (NGFW).
Deep packet inspection firewall with an application level inspection.

(8) Cryptography:
Cryptography is the method of protecting information and communication through the use of codes so that only those for whom the information is intended can read and process. A plaintext or messages is converted to an unreadable text known as cipher text using a mathematical algorithm this is known as encryption. At the receiver, the ciphertext is converted back to the original message which is known as decryption.

Types of Cryptography.

Symmetric key Cryptography:
Symmetric key systems are faster and simpler but the problem is that sender and receiver have to somehow exchanges keys in a secure manner. It use same key to encrypt and decrypt message.

Asymmetric key Cryptography:
A pair of keys is used to encrypt and decrypt information. A public key is used for encryption and a private key is used for decryption. The public and private keys are different. A public key is a large numerical value that can be generated by software program to encrypt data. A private key is typically a long, randomly or pseudo randomly generated sequences of bits that cannot be easily guessed.

Hash Function:
There is no usage of any key in this algorithm. A hash value of both a fixed length is calculated as per the plain text which makes it impossible for the contents of plain text to be recovered. Many operating system use hash function to encrypt passwords.

③ Antivirus :

Antivirus is a kind of software used to prevent, scan, detect and delete viruses from a computer. Most antivirus software runs automatically in the background to provide real-time protection against virus attacks. Comprehensive virus protection program helps to protect your files and hardware from malware such as worms, Trojan horses, and spyware, and may also offer additional protection such as customizable firewalls and website blocking.

④ VPN

A VPN extends a private network across a public network and enables users to send and receive data across shared or public network as if their computing devices were directly connected to the private network. A VPN is created by establishing a virtual point-to-point connection through the use of dedicated circuit or with tunneling protocols over existing networks. It provides access to resource that are inaccessible on the public network and is typically used for remote workers.

Protecting e-Governance System:

→ Use firewalls and intrusion detection sys.

→ Secure sensitive information in transit and storage.

→ Implement strong user authentication method.

→ Regularly back up data and have recovery plans.

→ Inform citizen about online safety.

→ Educate staff and users on cybersecurity practices.

→ Work with security experts to stay ahead of threats.

Biometric:

Biometric technology refers to the use of unique physical or behavioral characteristics for identification and authentication. The use of biometric system is increasing day-to-day due to their high accuracy and difficulty to replicate.

Common biometric method includes:

① Fingerprint Recognition:
- Analyzing the unique patterns of ridges and verify identity.

② Facial Recognition:
→ Using algorithms to identify person's identity based on facial features.

③ Iris Recognition.
- Scanning the unique pattern in the colored part of the eye.

④ Voice Recognition.
→ Analyzing vocal characteristics and pattern to identify a speaker.

⑤ Palm Recognition.
Using the unique patterns of a person's palms for identification.

⑥ Signature Recognition:
↳ Analyzing the unique aspects of person's signature, including speed and pressure

Client server network security: It refers to the measures and protocol implemented to protect data and resources in a network where client request services from a central server. It involves safeguarding the communication between clients and servers to prevent unauthorized access, data breaches, and cyber threats. key aspects include firewall, encryption, regular update and security policies. These elements work together to ensure the integrity, and availability within the network.

Data and message security: It refers to the practices and technologies used to protect information from unauthorized access, alteration or destruction during storage and transmission. It includes measures such as encryption to secure data confidentiality, authentication to verify user identities. Overall, data and message security aim to safeguard sensitive information from various threats.

Unit 8 Legal and Ethical Issues

Issues related to e-Governance

1. Lack of coordination
   Coordination between various government departments and agencies can be difficult, leading to delays in implementation.

2. Training Gaps:
   Government employees more training to efficiently manage e-gov- platforms.

3. Interoperability problems:
   Difficulty in integrating different systems.

4. Resistance to change:
   Cultural and trust issues among users

5. Cost and Maintenance
   - High initial cost and ongoing expenses.

Legal Issues:

Legal Issues in e-governance involve challenges related to the creation, interpretation and enforcement of laws

- that governs digital interaction between government and citizen. key legal issues are given below,

(i) Intellectual properties:
- Managing right related to software and digital content.

(ii) Data privacy:
- Ensuring personal information is protected and handled according to privacy laws.

(iii) Compliance
- Following existing laws and regulations

(iv) International Issues
- Handling legal matter related to cross-boarder data and services

(v) Copyright:
An exclusive groot from the government that allow the owner to reproduce partial or whole part to display it to the public.

(vi) Transperency
- Maintaining openness and accountability in digital processes

Ethical Issues:

Ethical issue are problems about what is right or wrong in certain situations. They involve making decision based on moral principle, such as fairness, honesty and respect for others. These values often come up when values or interests conflict. Some ethical issues related to egov given

① Privacy:
protecting citizen's personal data and preventing misuse

② Security:
Safeguarding system against breaches and attacks.

③ Fairness:
Ensuring equal access and treatment for everyone

④ Accountability:
- Holding people and system responsible for error or misuse.

⑤ Digital Inclusion.

- Addressing the needs of those without access or digital skills

(iv) Integrity.
Conducting e-governance with honesty and in the public best interest.

(Taxation)

Taxation is defined as the process by which governments collect financial contribution (tax) from individual and businesses to fund public services and infrastructure. Taxes can be imposed on various sources, such as income, property, sales and profits.

The primary purpose of taxation is to provide governments with the financial resources needed to deliver public service and maintain infrastructure. These services include healthcare, education, transportation and public safety, which are essential for the functioning of society. Without taxes government would struggle to fund these services, potentially leading to a decline in quality of life and economic growth.

However, taxation can also have negative

effects. High tax rates may discourage investment and economic activity. Complex tax system can create administrative burdens for both individuals and businesses.

Types of taxes.

① Income Tax
It is a tax on the earning of individual and businesses.

② Property Tax
This type of tax is imposed on property of owners based on the value of their property.

③ Sales Tax
- Applied on the purchase of good and services.

④ Corporate Tax
- This tax is applied on the profit of business corporation.

⑤ Excise Tax:
→ Government use excise tax to raise money and to discourage the use of products harmful to us.

Unit 9

Cyber law.

Concept of Cyber law

Modern says Internet technologies are vulnerable. The attacker are easily influenced by the system in order to protect the internet from there possibilities cyber law is made.

Cyber law is the area of law that deals with the internet relationship to technological and electronic element including computer, software, hardware and information system. It is also known as cyber law or internet law. It prevents or reduce large scale damage from cyber criminal activities by protecting information action, privacy, communication, intellectual properties, freedom of speech and so on related to the use of Internet, website email, software, hardware, etc. The increase in the internet traffic has yet to have a higher proportion of legal issues world wide.

Some emerging trends of cyber laws are listed below:

① First laws for protecting personal data

(v) Enhanced requirements for securing systems.
(vi) New laws for emerging cyber threats.
(vii) Rules for international data transfer.
(viii) Regulation for blockchain tech and digital currencies.
(ix) Standards for secure online activities.

Aims of cyber law:

(i) To promote growth of cyber security & law.
(ii) To create effective cyber crime laws.

→ Promote fair use of digital resources.
→ Ensure data privacy and security.
→ Regulate online behaviour & transaction.
→ Encourage international cooperation on cyber security issues.
→ Provide legal framework for emerging technologies.
→ Protect individuals from identity theft and cyber stalking.

Salient provisions for cyber law,

Cyber law provisions includes rules for data protection to ensure personal and sensitive information is secure, definitions and penalties for cyber crime. like hacking and identity theft, and regulation for valid electronic contracts and signatures. It also cover privacy protection for online communication.

As an example, The Government of Nepal has approved the Electronic Transaction Act-2006 on 4th Dec-2006. This law doesn't only legalize all sorts of electronic transaction and digital signatures but also has computer based mechanism and penalties cyber crime. Apart from the act there are the terms of controller of certification authority which are further divided into 12-sections and 80-clauses. According to cyber law of Nepal, If any individual is found in cyber crimes like hacking the intellectual properties of others, he/she will be punished for minimum of 6month to 3 years of prison and has to pay minimum pay up to Rs 50000 to 3 lakh.

Contracting and contract enforcement.

Contracting.

In cyber law, contracting means creating and signing agreements online that are legally valid. This involves making sure that digital contracts and signatures are recognized by the law. Just like traditional paper contracts.

Contract enforcement.

Contract enforcement in the digital world means making sure that online agreements are followed. If someone fails to meet the term of an online contract, the law provide ways to address and resolve disputes. This including taking legal action to ensure that the agreed-upon terms are carried out and that any breaches are dealt with properly.