Unit-5
Internet

The Internet, sometimes called simply "the Net," is a worldwide system of computer networks -- a network of networks in which users at any one computer can, if they have permission, get information from any other computer (and sometimes talk directly to users at other computers).

It was conceived by the Advanced Research Projects Agency (ARPA) of the U.S. government in 1969 and was first known as the ARPANet. The original aim was to create a network that would allow users of a research computer at one university to "talk to" research computers at other universities. A benefit of ARPANet's design was that, because messages could be routed or rerouted in more than one direction, the network could continue to function even if parts of it were destroyed in the event of a military attack or other disaster.

Today, the Internet is a public, cooperative and self-sustaining facility accessible to hundreds of millions of people worldwide.

In order to connect to the Internet, you must have access to an Internet service provider (ISP), which acts the middleman between you and the Internet. Most ISPs offer broadband Internet access via a cable or fiber connection. When you connect to the Internet using a public Wi-Fi signal, the Wi-Fi router is still connected to an ISP that provides Internet access. Even cellular data towers must connect to an Internet service provider to provide connected devices with access to the Internet.
Some of the basic services available to Internet users are −

- **Email** − A fast, easy, and inexpensive way to communicate with other Internet users around the world.
- **Telnet** − Allows a user to log into a remote computer as though it were a local system.
- **FTP** − Allows a user to transfer virtually every kind of file that can be stored on a computer from one Internet-connected computer to another.
- **UseNet news** − A distributed bulletin board that offers a combination news and discussion service on thousands of topics.
- **World Wide Web (WWW)** − A hypertext interface to Internet information resources.

Advantages of Internet:

- **Source Of Information:**

  It is the best source of variety of information. Now even students of colleges and universities mainly depend on it to complete not only their assignments but also to keep themselves up-to-date. There is no better source of research other than internet. We can find latest trends, we can talk to specialists without actually visiting them, and we can also get professional assistance through internet.

- **Source Of Entertainment:**

  Online games, chatting, surfing, music, movies, dramas and TV shows are becoming most common sources of entertainment. Games are available free of cost, chat rooms are available to discuss on any topic, entertainment websites are accessible, online movies and other TV shows are also easily accessible just because of internet.

- **Keep Informed:**

  Internet is a source of newest news because there are hundreds and thousands of news groups and services which keep you informed with every tick of clock. People like to read news about sports, weather, politics or any other topic internet keep you well informed and up-to-date.

- **Online Shopping:**

  Internet shopping is becoming popular because of virtual shops where you can buy anything you want and need without going out of home. Virtual shops are earning much money recently. Most popular product is cloths which more women are buying it through internet. Also groceries, house hold and other electronic items are available. You only need to sit in front of computer, click mouse and product will be at your doorstep within few hours.

Disadvantages of Internet:

- **A Waste Of Time:**

  Most people argue that spending much time in using internet is bad which leads to obesity in young generation. In a contemporary world people also say that internet is not necessary for life and life would be easier without it.

- **Not Safe Place For Children:**

  If children are allowed to use internet then parent become worry if they are spending much time on internet. Pornography and unethical communities are available. So one can say that internet is not a safe place for children because there are different tools available who can bypass 'parental protection'. Also children who use internet are becoming addicted to it which is again very dangerous.

- **Privacy Exposure:**

  Because of hackers community now it's very easy to decipher someone's chat or email messages. As we know data is transmitted in the form of packets, hackers sniff that packets and easy reconstruct.

- **Money Frauds:**

  With the introduction of online business, virtual shops and credit card usage; now it becomes very easy to buy things without going into market. There are some other Social Media Advertising sites which make frauds of money, these sites tries to get your personal information, credit card details and even pin code. Once they get this information you can easily become victim of money frauds.

- **Viruses/Malwares**:
  Often our systems get infected from viruses and ultimately damage our important data which is difficult to recover. These viruses are transported via internet, and USBs. Our computer can become totally out of order.

- **Online Threatening Or Harassment**:
  If someone manage to get your personal IDs or email address then it becomes easier to harass in chat rooms, online messages and through emails.

Protocol

A protocol is a standard set of rules that allow electronic devices to communicate with each other. These rules include what type of data may be transmitted, what commands are used to send and receive data, and how data transfers are confirmed.
Protocols exist for several different applications. Examples include wired networking (e.g., Ethernet) and Internet communication (e.g., IP).
Protocols are a fundamental aspect of digital communication. In most cases, protocols operate in the background, so it is not necessary for typical users to know how each protocol works.

Types of Protocol:

1. **Transmission Control Protocol (TCP):** TCP is a popular communication protocol which is used for communicating over a network. It divides any message into series of packets that are sent from source to destination and there it gets reassembled at the destination.
2. **Internet Protocol (IP):** IP is designed explicitly as addressing protocol. It is mostly used with TCP. The IP addresses in packets help in routing them through different nodes in a network until it reaches the destination system. TCP/IP is the most popular protocol connecting the networks.
3. **User Datagram Protocol (UDP):** UDP is a substitute communication protocol to Transmission Control Protocol implemented primarily for creating loss-tolerating and low-latency linking between different applications.
4. **Post office Protocol (POP):** POP3 is designed for receiving incoming E-mails.
5. **Simple mail transport Protocol (SMTP):** SMTP is designed to send and distribute outgoing E-Mail.
6. **File Transfer Protocol (FTP):** FTP allows users to transfer files from one machine to another. Types of files may include program files, multimedia files, text files, and documents, etc.
7. **Hyper Text Transfer Protocol (HTTP):** HTTP is designed for transferring a hypertext among two or more systems. HTML tags are used for creating links. These links may be in any form like text or images. HTTP is designed on Client-server principles which allow a client system for establishing a connection with the server machine for making a request. The server acknowledges the request initiated by the client and responds accordingly.

8. **Telnet:** Telnet is a set of rules designed for connecting one system with another. The connecting process here is termed as remote login. The system which requests for connection is the local computer, and the system which accepts the connection is the remote computer.
9. **Gopher:** Gopher is a collection of rules implemented for searching, retrieving as well as displaying documents from isolated sites. Gopher also works on the client/server principle.

Uniform Resource Locator (URL)

A Uniform Resource Locator (URL), also known as a Universal Resource Locator, is the address of a resource on the Internet and the protocol used to access it.

It indicates the location of a web resource like a street address indicates where a person lives physically — because of this, an URL is often referred to as: "web address".

URL contains the following information:

- The protocol used to access the resource.
- The location of the server (whether by IP address or domain name).
- The port number on the server (optional).
- The location of the resource in the directory structure of the server.
- A fragment identifier (optional).

Parts of a URL:

Using the URL https://whatis.techtarget.com/search/query?q=URL as an example, components of a URL can include:

- The protocol or scheme. Used to access a resource on the internet. Protocols include http, https, ftps, mailto and file. The resource is reached through the domain name system (DNS) name. In this example, the protocol is https.
- Host name or domain name. The unique reference the represents a webpage. For this example, whatis.techtarget.com.
- Port name. Usually not visible in URLs, but necessary. Always following a colon, port 80 is the default port for web servers, but there are other options. For example, :port80.
- Path. A path refers to a file or location on the web server. For this example, search/query.
- Query. Found in the URL of dynamic pages. The query consists of a question mark, followed by parameters. For this example, ?.
- Parameters. Pieces of information in a query string of a URL. Multiple parameters can be separated by ampersands (&). For this example, q=URL.

Web Browser

A web browser is an interface that helps a computer user gain access to all the content that is on the Internet. It can view images, text documents, audio and video files, games, etc.
More than one web browser can also be installed on a single computer. The user can navigate through files, folders and websites with the help of a browser. When the browser is used for browsing web pages, the pages may contain certain links which can be opened in a new browser. Multiple tabs and windows of the same browser can also be opened.
On the Web, when you navigate through pages of information, this is commonly known as web browsing or web surfing
To access the Web, you need a web browser, such as Microsoft Internet Explorer or Mozilla Firefox.

Most browsers have these user interface features:

- Allow the user to open multiple pages at the same time, either in different browser windows or in different tabs of the same window.
- Back and forward buttons to go back to the previous page visited or forward to the next one.
- A refresh or reload button to reload the current page.
- A stop button to cancel loading the page. (In some browsers, the stop button is merged with the reload button.)
- A home button to return to the user's home page.
- An address bar to input the URL of a page and display it.
- A search bar to input terms into a search engine. (In some browsers, the search bar is merged with the address bar.)

Types of Web Browser:

Internet Explorer

Internet Explorer by Microsoft is the default browser for Windows operating system. Its still very popular with many internet users. This is the most commonly used browser in the universe. This was introduced in 1995 along with Windows 95 launch and it has passed Netscape popularity in 1998.There are a lot of necessary features like Active X capabilities, SmartScreen Filters, a list of recommended sites and more.

Google Chrome

This web browser is developed by Google. Today, chrome is known to be one of the most popular web browser .It Focuses on enhanced performance of web applications.
Hundreds of useful extensions can be downloaded for free from Chrome Store and can be used for personal use.
A large array of apps available at Chrome Store. These adds a considerable amount to the browsing experience of the users.

Mozilla Firefox

Firefox is a new browser derived from Mozilla. It was released in 2004 and has grown to be the second most popular browser on the Internet.

It designed for simplicity, security, extensibility yet flexibility and power. Available for Linux and android as well. There are lots of plugins and extensions with some powerful developer tools.

Firefox allows an open architecture which accepts the installation of themes and extensions. Themes give the browser a customizable new look. Developers can write extensions to make the browser perform functions as desired like check your Gmail account when you open the browser, or block all ads.

Safari

Safari is a web browser developed by Apple Inc. and included in Mac OS X. It was first released as a public beta in January 2003. Safari has very good support for technologies like XHTML, CSS2 etc.

Opera

Opera is smaller and faster than most other browsers, yet it is full- featured. Fast, user-friendly, with keyboard interface, multiple windows, zoom functions, and more. Java and non Java-enabled versions available. Ideal for newcomers to the Internet, school children, handicap and as a front-end for CD-Rom and kiosks.

Konqueror

Konqueror is an Open Source web browser with HTML 4.01 compliance, supporting Java applets, JavaScript, CSS 1, CSS 2.1, as well as Netscape plugins. This works as a file manager as well as it supports basic file management on local UNIX filesystems, from simple cut/copy and paste operations to advanced remote and local network file browsing.

Lynx

Lynx is a fully-featured World Wide Web browser for users on Unix, and other platforms running cursor-addressable, character-cell terminals or emulators.

Unit-5
World Wide Web Consortium (W3C)

The World Wide Web Consortium (W3C) is an international organization committed to improving the web. It is made up of several hundred member organizations from a variety of related IT industries. W3C sets standards for the World Wide Web (WWW) to facilitate interoperability and cooperation among all web stakeholders. It was established in 1994 by the creator of the WWW, Tim Berners-Lee.
The primary international standards organization for the web, the World Wide Web Consortium is dedicated to bringing together interested parties from different IT sectors to work on web issues.
"The objective of the W3C is to bring the web to its full potential,". Its members are key participants in web development, including commercial, educational and governmental entities, according to the W3C website.
Its mission includes "developing protocols and guidelines that ensure the long-term growth of the web."
The basis for W3C's credibility as a driver of technical standards for the web. The W3C:

- Was founded by the inventor of the web, Tim Berners-Lee
- Has a membership that includes key participants in the IT industry
- Has a track record of success

The organization is guided by its open standards principles. It calls them OpenStand, which it refers to as "The Modern Paradigm for Standards."

The five fundamental principles of standards development, per the W3C website, are:

- Due process
- Broad consensus
- Transparency
- Balance
- Openness

Standards developed by the Consortium include:

- CGI
- CSS
- DOM
- HTML
- HTTP
- XHTML
- XML

The W3C has broad support. "All stakeholders can have a voice in the development of W3C standards,"including Members large and small, as well as the public." The World Wide Web Consortium was created in cooperation with CERN in Switzerland. It has enjoyed support from government organizations DARPA and the European Commission. It is currently hosted by MIT Laboratory for Computer Science in the U.S. and INRIA in Europe.

Search Engine

Search Engine refers to a huge database of internet resources such as web pages, newsgroups, programs, images etc. It helps to locate information on World Wide Web.
User can search for any information by passing query in form of keywords or phrase. It then searches for relevant information in its database and return to the user.

Components of Search Engine:

Generally there are three basic components of a search engine.

- Web Crawler
- Database
- Search Interfaces

Web crawler

It is also known as spider or bots. It is a software component that traverses the web to gather information.

Database

All the information on the web is stored in database. It consists of huge web resources.

Search Interfaces

This component is an interface between user and the database. It helps the user to search through the database

Working of Search Engine:

Web crawler, database and the search interface are the major component of a search engine that actually makes search engine to work. Search engines make use of Boolean expression AND, OR, NOT to restrict and widen the results of a search.

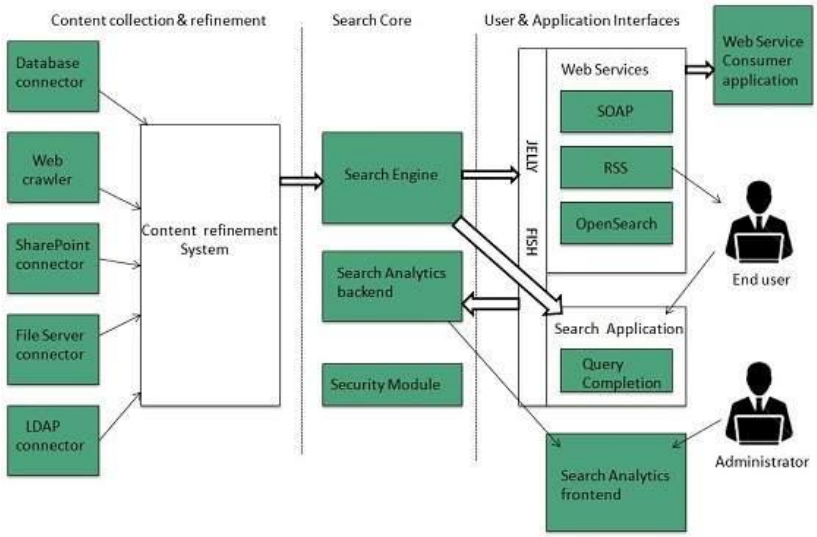
Following are the steps that are performed by the search engine:

- The search engine looks for the keyword in the index for predefined database instead of going directly to the web to search for the keyword.
- It then uses software to search for the information in the database. This software component is known as web crawler.
- Once web crawler finds the pages, the search engine then shows the relevant web pages as a result. These retrieved web pages generally include title of page, size of text portion, first several sentences etc.
- User can click on any of the search results to open it.

Architecture of Search Engine:

The search engine architecture comprises of the three basic layers.

- Content collection and refinement.
- Search core
- User and application interfaces



Search Engine Processing:

- **Indexing Process-**

Indexing process comprises of the following three tasks:

- Text Acquisition
- Text Transformation
- Index Creation

Text Acquisition

It identifies and stores documents for indexing.

Text Transformation

It transforms document into index terms or features.

Index Creation

It takes index terms created by text transformations and create data structures to suport fast searching.

- **Query Process**

Query process comprises of the following three tasks:

- User interaction
- Ranking
- Evaluation

User interaction

It supporst creation and refinement of user query and displays the results.

Ranking

It uses query and indexes to create ranked list of documents.

Evaluation

It monitors and measures the effectiveness and efficiency. It is done offline.

Examples:

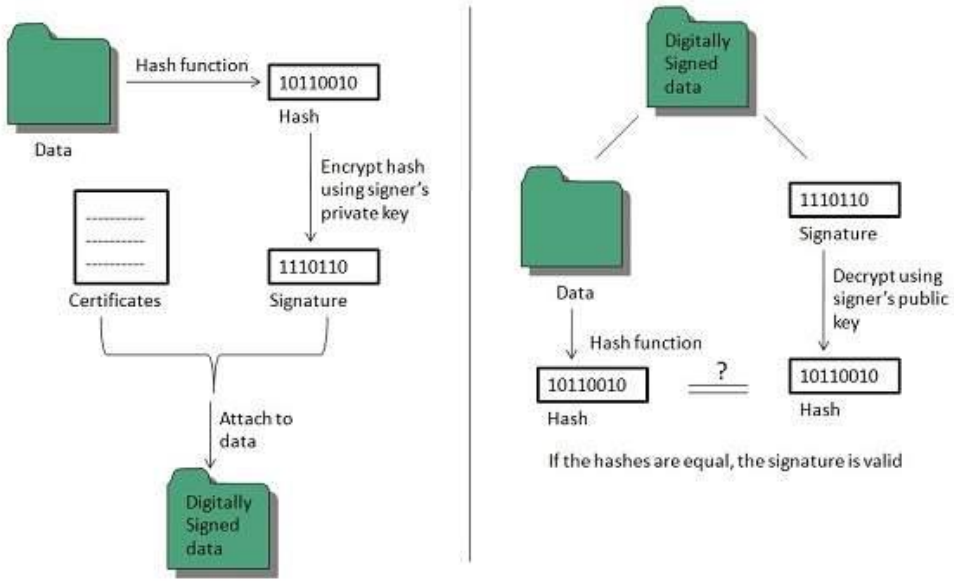
Following are the several search engines available today:

Search Engine	Description
Google	It was originally called BackRub. It is the most popular search engine globally.
Bing	It was launched in 2009 by Microsoft. It is the latest web-based search engine that also delivers Yahoo's results.
Ask	It was launched in 1996 and was originally known as Ask Jeeves. It includes support for match, dictionary, and conversation question.
AltaVista	It was launched by Digital Equipment Corporation in 1995. Since 2003, it is powered by Yahoo technology.
AOL.Search	It is powered by Google.
LYCOS	It is top 5 internet portal and 13th largest online property according to Media Matrix.
Alexa	It is subsidiary of Amazon and used for providing website traffic information.

Unit-5

Digital Signature

Digital signatures allow us to verify the author, date and time of signatures, authenticate the message contents. It also includes authentication function for additional capabilities.



A digital signature should not only be tied to the signing user, but also to the message.

Applications:

There are several reasons to implement digital signatures to communications:

- **Authentication**

  Digital signatures help to authenticate the sources of messages. For example, if a bank's branch office sends a message to central office, requesting for change in balance of an account. If the central office could not authenticate that message is sent from an authorized source, acting of such request could be a grave mistake.

- **Integrity**

  Once the message is signed, any change in the message would invalidate the signature.

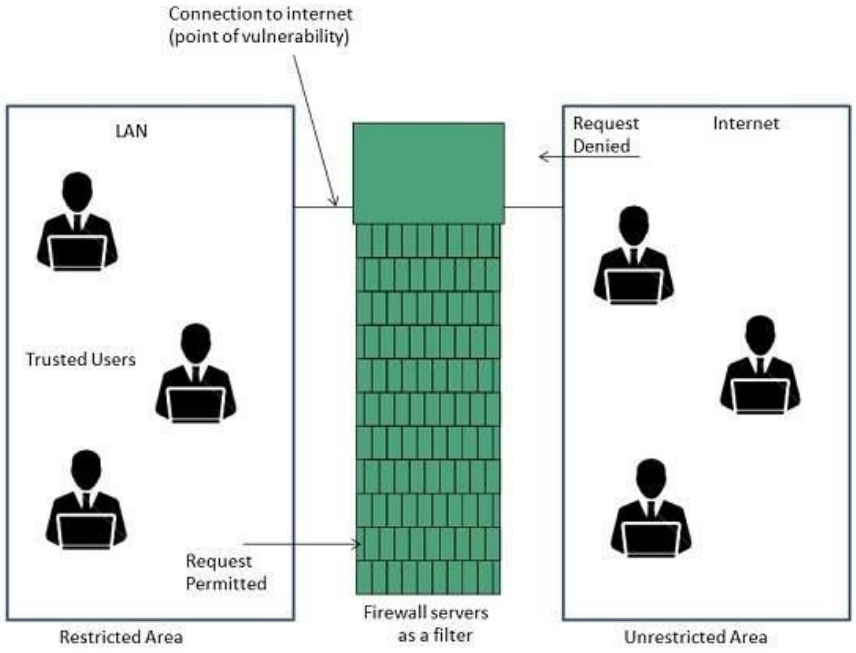
- **Non-repudiation**

  By this property, any entity that has signed some information cannot at a later time deny having signed it.

Firewall

Firewall is a barrier between Local Area Network (LAN) and the Internet. It allows keeping private resources confidential and minimizes the security risks. It controls network traffic, in both directions.

The following diagram depicts a sample firewall between LAN and the internet. The connection between the two is the point of vulnerability. Both hardware and the software can be used at this point to filter network traffic.



Types of Firewall

Firewalls are generally of two types: Host-based and Network-based.

- **Host- based Firewalls :**
  Host-based firewall is installed on each network node which controls each incoming and outgoing packet. It is a software application or suite of applications, comes as a part of the operating system. Host-based firewalls are needed because network firewalls cannot provide protection inside a trusted network. Host firewall protects each host from attacks and unauthorized access.
- **Network-based Firewalls :**
  Network firewall function on network level. In other words, these firewalls filter all incoming and outgoing traffic across the network. It protects the internal network by filtering the traffic using rules defined on the firewall. A Network firewall might have two or more network interface cards (NICs). A network-based firewall is usually a dedicated system with proprietary software installed.

Internet Security

Internet security refers to securing communication over the internet. It includes specific security protocols such as:

- Internet Security Protocol (IPSec)
- Secure Socket Layer (SSL)

Internet Security Protocol (IPSec)

It consists of a set of protocols designed by Internet Engineering Task Force (IETF). It provides security at network level and helps to create authenticated and confidential packets for IP layer.

Secure Socket Layer (SSL)

It is a security protocol developed by Netscape Communications Corporation. It provides security at transport layer. It addresses the following security issues:

- Privacy
- Integrity
- Authentication

Threats:

Internet security threats impact the network, data security and other internet connected systems. Cyber criminals have evolved several techniques to threat privacy and integrity of bank accounts, businesses, and organizations.

Following are some of the internet security threats:

- Mobile worms
- Malware
- PC and Mobile ransomware
- Large scale attacks like Stuxnet that attempts to destroy infrastructure.
- Hacking as a Service
- Spam
- Phishing

Network Security

Network Security refers to the measures taken by any enterprise or organisation to secure its computer network and data using both hardware and software systems. This aims at securing

the confidentiality and accessibility of the data and network. Every company or organisation that handles large amount of data, has a degree of solutions against many cyber threats.

The most basic example of Network Security is password protection where the user of the network oneself chooses. In the recent times, Network Security has become the central topic of cyber security with many organisations inviting applications of people who have skills in this area. The network security solutions protect various vulnerabilities of the computer systems such as:

1**. Users**

2. Locations

3. Data

4. Devices

5. Applications

Types of Network Security:

- **Access Control:**

  Not every person should have complete allowance to the accessibility to the network or its data. The one way to examine this is by going through each personnel's details. This is done through Network Access Control which ensures that only a handful of authorized personnel must be able to work with allowed amount of resources.

- **Antivirus and Anti-malware Software:**

  This type of network security ensures that any malicious software does not enter the network and jeopardize the security of the data. The malicious software like Viruses, Trojans, Worms are handled by the same. This ensure that not only the entry of the malware is protected but also that the system is well equipped to fight once it has entered.

- **Cloud Security:**

  Now a day, a lot many organisations are joining hands with the cloud technology where a large amount of important data is stored over the internet. This type of security ensures in creating gaps in visibility of the data.

Cryptography

Cryptography is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it.

Thus preventing unauthorized access to information. The prefix “crypt” means “hidden” and suffix graphy means “writing”.

In Cryptography the techniques which are use to protect information are obtained from mathematical concepts and a set of rule based calculations known as algorithms to convert messages in ways that make it hard to decode it. These algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on internet and to protect confidential transactions such as credit card and debit card transactions.

Techniques used for Cryptography:

In today’s age of computers cryptography is often associated with the process where an ordinary plain text is converted to cipher text which is the text made such that intended receiver of the text can only decode it and hence this process is known as **encryption**. The process of conversion of cipher text to plain text this is known as **decryption.**

Features of Cryptography:

1. **Confidentiality:**
   Information can only be accessed by the person for whom it is intended and no other person except him can access it.

2. **Integrity:**
   Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.

3. **Non-repudiation:**
   The creator/sender of information cannot deny his or her intention to send information at later stage.

4. **Authentication:**
   The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.

Types of Cryptography:

There are three types Of cryptography:

1. **Symmetric Key Cryptography:**
   It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange key in a secure manner. The most popular symmetric key cryptography system is Data Encryption System(DES).

2. **Hash Functions:**
   There is no usage of any key in this algorithm. A hash value with fixed length is

calculated as per the plain text which makes it impossible for contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords.

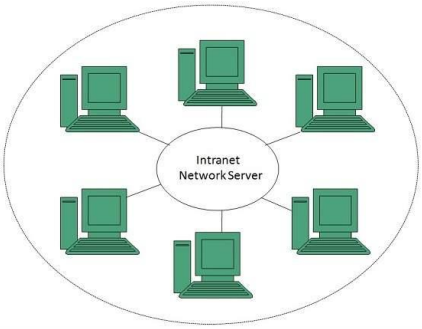
3. **Asymmetric Key Cryptography:**
   Under this system a pair of keys is used to encrypt and decrypt information. A public key is used for encryption and a private key is used for decryption. Public key and Private Key are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone knows the private key.

Intranet and Extranet

Intranet:

Intranet is defined as private network of computers within an organization with its own server and firewall. Moreover we can define Intranet as:

- Intranet is system in which multiple PCs are networked to be connected to each other. PCs in intranet are not available to the world outside of the intranet.
- Usually each company or organization has their own Intranet network and members/employees of that company can access the computers in their intranet.
- Every computer in internet is identified by a unique IP address.
- Each computer in Intranet is also identified by a IP Address, which is unique among the computers in that Intranet.



Benefits of Intranet:

- **Communication**
  Intranet offers easy and cheap communication within an organization. Employees can communicate using chat, e-mail or blogs.
- **Time Saving**
  Information on Intranet is shared in real time.
- **Collaboration**
  Information is distributed among the employees as according to requirement and it can be accessed by the authorized users, resulting in enhanced teamwork.
- **Platform Independency**
  Intranet can connect computers and other devices with different architecture.
- **Cost Effective**
  Employees can see the data and other documents using browser rather than printing them and distributing duplicate copies among the employees, which certainly decreases the cost.

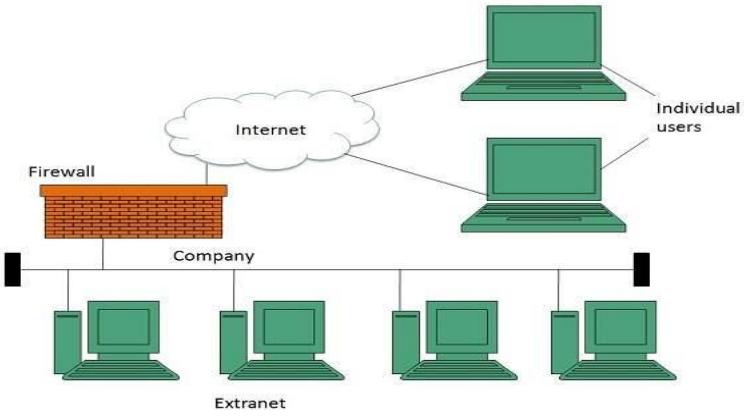
- **Workforce Productivity**
  Data is available at every time and can be accessed using company workstation. This helps the employees work faster.
- **Business Management**
  It is also possible to deploy applications that support business operations.
- **Security**
  Since information shared on intranet can only be accessed within an organization, therefore there is almost no chance of being theft.
- **Specific Users**
  Intranet targets only specific users within an organization therefore, once can exactly know whom he is interacting.
- **Immediate Updates**
  Any changes made to information are reflected immediately to all the users.

Difference between Internet and Intranet

S.No.	INTERNET	INTRANET
1.	Internet is used to connect different network of computers simultaneously.	Intranet is owned by private firms.
2.	In internet, there are multiple users.	In intranet, there are limited users.
3.	Internet is unsafe.	Intranet is safe.
4.	In internet, There are more number of visitors.	In intranet, There are less number of visitors.
5.	Internet is a public network.	Intranet is a private network.
6.	Anyone can access Internet.	In this, anyone can't access the Intranet.
7.	Internet provides unlimited information.	Intranet provides limited information.

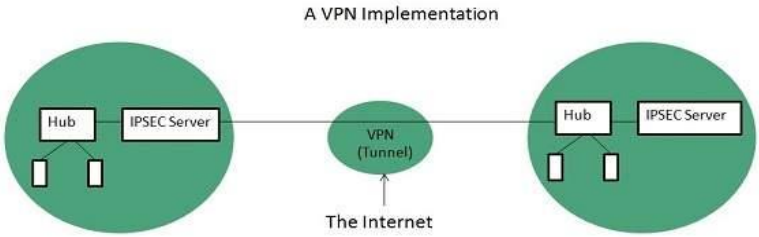
Extranet:

Extranet refers to network within an organization, using internet to connect to the outsiders in controlled manner. It helps to connect businesses with their customers and suppliers and therefore allows working in a collaborative manner.



Implementation

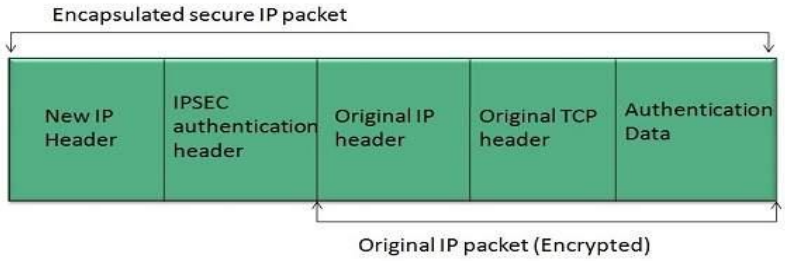
Extranet is implemented as a Virtual Private Networks (VPN) because it uses internet to connect to corporate organization and there is always a threat to information security. VPN offers a secure network in public infrastructure (Internet).



Key Points

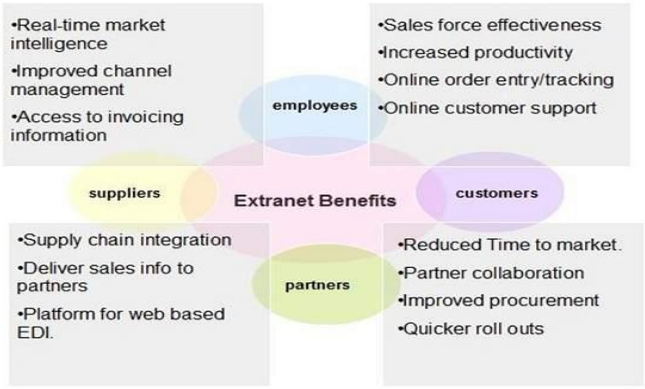
- The packet is encapsulated at boundary of networks in IPSEC complaint routers.
- It uses an encryption key to encapsulate packets and IP addresses as well.
- The packet is decoded only by the IPSEC complaint routers or servers.
- The message is sent over VPN via VPN Tunnel and this process is known as tunneling.

VPN uses **Internet Protocol Security Architecture (IPSEC)** Protocol to provide secure transactions by adding an additional security layer to TCP/IP protocol. This layer is created by encapsulating the IP packet to a new IP packet as shown in the following diagram:



Benefits of Extranet:

Extranet proves to be a successful model for all kind of businesses whether small or big. Here are some of the advantages of extranet for employees, suppliers, business partners, and customers:



Issues of Extranet:

Apart for advantages there are also some issues associated with extranet. These issues are discussed below:

- **Hosting**
  Where the extranet pages will be held i.e. who will host the extranet pages. In this context there are two choices:
  - Host it on your own server.
  - Host it with an Internet Service Provider (ISP) in the same way as web pages.

  But hosting extranet pages on your own server requires high bandwidth internet connection which is very costly.
- **Security**
  Additional firewall security is required if you host extranet pages on your own server which result in a complex security mechanism and increase work load.
- **Accessing Issues**
  Information can not be accessed without internet connection. However, information can be accessed in Intranet without internet connection.
- **Decreased Interaction**
  It decreases the face to face interaction in the business which results in lack of communication among customers, business partners and suppliers.

Difference between Intranet and Extranet

S.NO	INTRANET	EXTRANET
1.	Intranet is a tool for sharing information throughout the organization.	Whereas Extranet is a tool for sharing information between the internal members and external members.
2.	Intranet is owned by a single organization.	While Extranet is owned by either a single or a many organization.

3.	In intranet, security is implemented through a firewall.	Whereas in this, security is implemented through a firewall in order to separate the extranet and the internet.
4.	Intranet is managed by an organization.	Whereas Extranet is managed by many organizations.
5.	Intranet has a limited number of connected devices.	Whereas in the extranet, connected devices are comparable with the intranet.
6.	Intranet is a private network type for an organization.	While it is also a private network in which public network is used in order to share the information to the suppliers and customers.
7.	Intranet is used in order to get employee information, telephone directory etc.	While It is used to check status, access data, send mail, place order etc.

Difference between Internet and Extranet

S.NO	INTERNET	EXTRANET
1.	It is used as public network.	Whereas it is used as private network.
2.	An internet is less secure because it has zero security level in the firewall.	While the extranet is more secure than the Internet.
3.	In the case of the Internet, anyone can access it without a valid username and password.	Whereas in the case of extranet, no one can access it without a valid username and password.
4.	A large number of users can access the Internet.	Whereas here, a limited number of users can access the extranet.
5.	An internet acts as a tool for sharing information all over the world.	Whereas it acts as a medium to share the information between the internal and external members.
6.	An internet is not owned by anyone.	Whereas extranet is owned by a single or multiple organization.
7.	An Internet is not managed by either authority.	Unlike the internet, it is managed by numerous organizations.
8.	An internet is the largest network in the case of number of connected devices.	Whereas in the case of extranet, it is small in terms of connected devices as compared to the internet.

Unit-5
E-Banking or Internet banking

Online banking also known as internet banking, e-banking, or virtual banking, is an electronic payment system that enables customers of a bank or other financial institution to conduct a range of financial transactions through the financial institution's website.
Internet banking is a term used to describe the process whereby a client executes banking transactions via electronic means. This type of banking uses the internet as the chief medium of delivery by which banking activities are executed. The activities clients are able to carry out are can be classified to as transactional and non transactional.

Advantages of E-banking or Internet banking:

1. Convenience: Banks that offer internet banking are open for business transactions anywhere a client might be as long as there is internet connection. Apart from periods of website maintenance, services are available 24 hours a day and 365 days round the year. In a scenario where internet connection is unavailable, customer services are provided round the clock via telephone.

2. Low cost banking service: E-banking helps in reducing the operational costs of banking services. Better quality services can be ensured at low cost.

3. Higher interest rate: Lower operating cost results in higher interest rates on savings and lower rates on mortgages and loans offers from the banks. Some banks offer high yield certificate of deposits and don't penalize withdrawals on certificate of deposits, opening of accounts without minimum deposits and no minimum balance.

4. Transfer services: Online banking allows automatic funding of accounts from long established bank accounts via electronic funds transfers.

5. Ease of monitoring: A client can monitor his/her spending via a virtual wallet through certain banks and applications and enable payments.

6. Ease of transaction: The speed of transaction is faster relative to use of ATM's or customary banking.

7. Discounts: The credit cards and debit cards enables the Customers to obtain discounts from retail outlets.

8. Quality service: E-Banking helps the bank to provide efficient, economic and quality service to the customers. It helps the bank to create new customer and retaining the old ones successfully.

9. Any time cash facility: The customer can obtain funds at any time from ATM machines.

Disadvantages of E-banking or Internet banking:

1. High start-up cost: E-banking requires high initial start up cost. It includes internet installation cost, cost of advanced hardware and software, modem, computers and cost of maintenance of all computers.

2. Security Concerns: One of the biggest disadvantages of doing e-banking is the question of security. People worry that their bank accounts can be hacked and accessed without their knowledge or that the funds they transfer may not reach the intended recipients.

3. Training and Maintenance: E-banking requires 24 hours supportive environment, support of qualified staff. Bank has to spend a lot on training to its employees. Shortage of trained and qualified staff is a major obstacle in e-banking activities.

4. Transaction problems: Face to face meeting is better in handling complex transactions and problems. Banks may call for meetings and seek expert advice to solve issues.

5. Lack of personal contact between customer and banker: Customary banking allows creation of a personal touch between a bank and its clients. A personal touch with a bank manager can enable the manager to change terms in our account since he/she has some discretion in case of any personal circumstantial change. It can include reversal of an undeserved service charge.

Electronic-Cash(E-Cash)

E-cash, also known as electronic cash, is a digital currency that can be used via various online platforms and apps. While originally used primarily for online transactions, well-known e-cash facilitators such as Apple Pay, Venmo and Google Wallet are taking the concept mainstream and allowing for a wide range of uses. In short, e-cash is stored online in a digital wallet and can be used to pay for goods and services and to instantaneously transfer funds between accounts and people through electronic means.

Four major elements in an electronic cash system:-

- **Issuers**
- **Merchants**
- **Regulators**
- **Customers**

For E-Cash dealing, we want to go through a minimum of three stages:-

- **Account setup**
- **Purchase**
- **Authentication**

We can classify E-Cash payment systems:-

- **Account -based systems**
- **Token- based systems**
- **Notational systems**
- **Smart card-based notational systems.**

Advantages of e-cash:

- We can transfer funds, purchase stocks, and offer a variety of other services without having to handle physical cash or checks as long as bank is providing such services online.
- Debit cards and online bill payments allow immediate transfer of funds from an individual's personal account to a business's account regardless the designated place.
- Consumers will have greater privacy when shopping on the Internet using electronic money instead of ordinary credit cards.

Disadvantages of e-cash:

- E-cash and E-Cash transaction security are the major concern.
- Frauds on E-Cash are on the catch recent years.
- Hackers with good skill able to hack into bank accounts and illegally retrieve of banking records has led to a widespread invasion of privacy and has promoted identity theft.
- There are many other tricks including through phishing website of certain banks and emails.
- With the continued growth of E-Cash, money flow in and out of countries at immediate speed without being traced will weaken the government's ability to monitor and income in tax.

Properties of Electronic Cash:

- Digital cash must have a monetary value; it must be backed by cash, bank-authorized credit, or a bank-certified cashier’s check.
- When digital cash created by one bank is accepted by others, reconciliation must occur without any problems.
- Digital cash must be interoperable or exchangeable as payment for other digital cash, paper cash, goods or services, lines of credit, deposits in banking accounts, bank notes or obligations, electronic benefits transfers, and the like.
- Digital cash must be storable and retrievable.
- Digital cash should not be easy to copy with while it is being exchanged.
- It should be possible to prevent or detect duplication and double-spending of digital cash.