आईएफटीएम विश्वविद्यालय, मुरादाबाद, उत्तर प्रदेश

IFTM University, Moradabad, Uttar Pradesh

NAAC ACCREDITED

E-Content

IFTM University, Moradabad

FUNDAMENTAL OF E-COMMERCE

Unit-1

E-Commerce

E-commerce is also known as electronic commerce or internet commerce. E-commerce is the **buying** and **selling** of goods, products and services over the internet. Transaction of money, funds, and data are also considered as E-commerce.

‘E-commerce’ and ‘online shopping’ are often used interchangeably but at its core e-commerce is much broader than this – it **represents a concept for doing business online**, incorporating a multitude of different services e.g. **making online payments, booking flights etc.**

E-commerce has helped businesses establish a wider market presence by providing cheaper and more efficient distribution channels for their products or services.

These business transactions can be done in four ways: **Business to Business (B2B), Business to Customer (B2C), Customer to Customer (C2C), Customer to Business (C2B).**

Online stores like Amazon, Flipkart, Shopify, Myntra, Ebay, Quikr, Olx are examples of E-commerce websites.

History Of Ecommerce

The history of ecommerce started 40 years ago and, to this day, continues to grow with new technologies, innovations, and thousands of businesses entering the online market each year. Electronic Data Interchanges (EDI) and teleshopping in the 1970s paved the way for the modern-day ecommerce store. The history of ecommerce is closely intertwined with the history of the internet. Online shopping only became possible when the internet was opened to the public in 1991. Amazon.com was one of the first ecommerce sites in the US to start selling products online and thousands of businesses have followed since.

Online shopping was invented and pioneered in 1979 by Michael Aldrich in the United Kingdom. He connected a modified domestic television via a telephone line to a real-time multi-user transaction processing computer.

E-Commerce Process

The convenience of shopping online from home or work has changed the way today’s consumers purchase goods and services. E-Commerce process is a 6-steps process.

Below are 6 steps of E-Commerce process:

1) **Sourcing-** sourcing is the process of selecting suppliers to provide the goods and services you need to run your business.
2) **Cataloging-** Simply this means **quality photographs and good descriptions** A product catalog is a type of marketing collateral that lists essential product details that help buyers make a purchase decision. These details include product features, photos, descriptions, dimensions, price, weight, availability, color, customer reviews, and more.
3) **Listing-** in simple terms, is adding the products that you want to sell on the website. Ecommerce product listing service includes the placing of product in the list at Amazon, eBay, Magento, etc. website according to the specifications of products like colour, shape, size, price, etc. to make it more convenient for the customers while shopping at these websites.
4) **Marketing**- Ecommerce marketing is the act of driving awareness and action toward a business that sells its product or service electronically. Ecommerce marketers can use social media, digital content, search engines, and email campaigns to attract visitors and facilitate purchases online.
5) **Packaging-** Packaging is the process of creating a cover for the product which identifies the brand and also ensures its safety for storage and transport.
6) **Shipping-** Shipping is **the physical moving of good from one point to another**, such as the moving of merchandise from the warehouse to the customer.

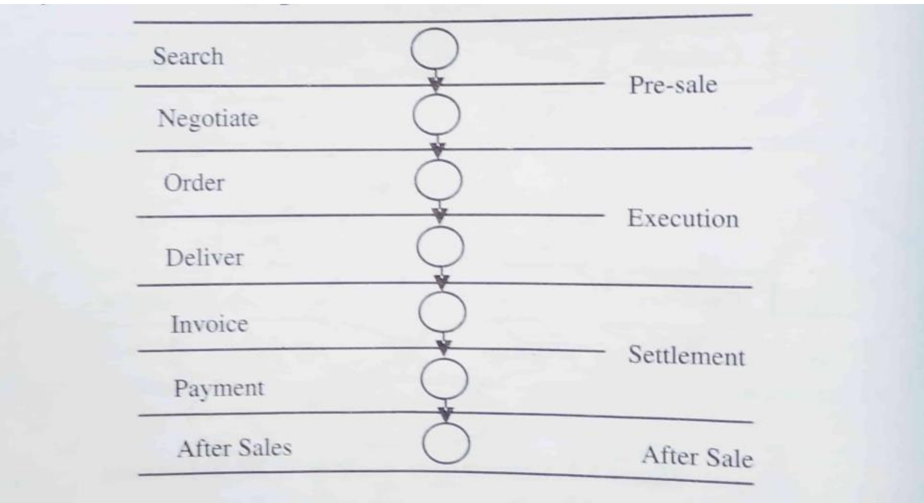
Trade Cycle

A trade cycle is the series of exchanges, between a customer and supplier, that take place when a commercial exchange is executed. A general trade cycle consists of:

- **Pre-Sales:** Finding a supplier and agreeing the terms.
- **Execution:** Selecting goods and taking delivery.
- **Settlement:** Invoice (if any) and payment.
- **After-Sales:** Following up complaints or providing maintenance.

The trade cycle has to support:

1. Finding goods or services appropriate to the requirement and agreeing the terms of trade (referred to as search and negotiation).
2. Placing the order, taking delivery and making payment (execution and settlement).
3. After-sales activities such as warrantee, service, etc.



Features of a Trade Cycle:

1. A business cycle is synchronic. When cyclical fluctuations start in one sector it spreads to other sectors.

2. In a trade cycle, a period of prosperity is followed by a period of depression. Hence trade cycle is a wave like movement.

3. Business cycle is recurrent and rhythmic; prosperity is followed by depression and vice versa.

4. A trade cycle is cumulative and self-reinforcing. Each phase feeds on itself and creates further movement in the same direction.

5. A trade cycle is asymmetrical. The prosperity phase is slow and gradual and the phase of depression is rapid.

6. The business cycle is not periodical. Some trade cycles last for three or four years, while others last for six or eight or even more years.

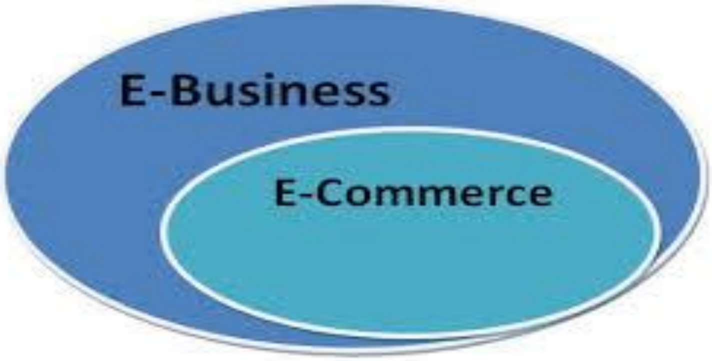
7. The impact of a trade cycle is differential. It affects different industries in different ways.

8. A trade cycle is international in character. Through international trade, booms and depressions in one country are passed to other countries.

E-commerce Vs E-Business

Some people use the terms "e-business" and "e-commerce" interchangeably, but they aren't synonymous. E-commerce can be viewed as a subset of e-business.

E- commerce (EC) describes the process of buying, selling, transferring, or exchanging products, services, and/or information via computer networks, including the Internet. E-business refers to a broader definition of EC, not just the buying and selling of goods and services, but also servicing customers, collaborating with business partners, conducting e-learning, and conducting electronic transactions within an organization.



Key Differences Between e-commerce and e-business

- **Definition**: Buying and selling of goods and services through the internet is known as e-commerce. Unlike e-business, which is an electronic presence of business, by which all the business activities are conducted through the internet.
- **Scope:** E-commerce is a major component of e-business. In other words, we can say, scope of E-commerce is narrow while E-Business's is wide.
- **Money:** E-commerce includes transactions which are related to money, but e-business includes monetary as well as allied activities.
- **Approach**: E-commerce has an extroverted approach that covers customers, suppliers. On the other hand, e-business has an ambient approach that covers internal as well as external processes.
- **Requirement:** E-commerce requires a website that can represent the business. Conversely, e-business requires a website, Customer Relationship Management and Enterprise Resource Planning for running the business over the internet.
- **Network:** E-commerce uses the internet to connect with the rest of the world. In contrast to e-business, the internet, intranet and extranet are used for connecting with the parties.

Traditional Comm Vs E-Comm.

Gone are the days when the commercial activities like the exchange of goods and services for money, between parties, takes place only in the traditional mode, i.e. the customer has to go to the market, look at the variety of products, choose the required stuff and the purchasing them by paying the specified amount. But with the advent of e-Commerce, people can buy goods, pay bills, or transfer money in just one click.

BASIS FOR COMPARISON	TRADITIONAL COMMERCE	E-COMMERCE
Meaning	Traditional commerce is a branch of business which focuses on the exchange of products and services, and includes all those activities which encourages exchange, in some way or the other.	e-Commerce means carryng out commercial transactions or exchange of information, electronically on the internet.
Processing of Transactions	Manual	Automatic
Accessibility	Limited Time	24×7×365
Physical inspection	Goods can be inspected physically before purchase.	Goods cannot be inspected physically before purchase.
Customer interaction	Face-to-face	Screen-to-face
Scope of business	Limited to particular area.	Worldwide reach
Information exchange	No uniform platform for exchange of information.	Provides a uniform platform for information exchange.
Resource focus	Supply side	Demand side
Business Relationship	Linear	End-to-end
Marketing	One way marketing	One-to-one marketing
Payment	Cash, cheque, credit card, etc.	Credit card, fund transfer etc.
Delivery of goods	Instantly	Takes time

Features

E-Commerce provides the following features −

- **Non-Cash Payment** − E-Commerce enables the use of credit cards, debit cards, smart cards, electronic fund transfer via bank's website, and other modes of electronics payment.
- **24x7 Service availability** − E-commerce automates the business of enterprises and the way they provide services to their customers. It is available anytime, anywhere.
- **Advertising / Marketing** − E-commerce increases the reach of advertising of products and services of businesses. It helps in better marketing management of products/services.
- **Improved Sales** − Using e-commerce, orders for the products can be generated anytime, anywhere without any human intervention. It gives a big boost to existing sales volumes.
- **Support** − E-commerce provides various ways to provide pre-sales and post-sales assistance to provide better services to customers.
- **Inventory Management** − E-commerce automates inventory management. Reports get generated instantly when required. Product inventory management becomes very efficient and easy to maintain.
- **Communication improvement** − E-commerce provides ways for faster, efficient, reliable communication with customers and partners

Advantages and Disadvantages of EComm.

Advantages

1. A Larger Market

eCommerce allows you to reach customers all over the country and around the world. Your customers can make a purchase anywhere and anytime, especially more people are getting used to shopping on their mobile devices.

2. Lower Cost

With the advance in eCommerce platform technologies, it has become very easy and affordable to set up and maintain an eCommerce store with a low overhead. Merchants no longer have to spend a large budget on TV ads or billboard, nor worry about the expense for personnel and real estate.

3. More Opportunities To "Sell"

Merchants can only provide a limited amount of information on a product in a physical store. On the other hand, eCommerce websites allow the space to include more information such as demo videos, reviews, and customer testimonials to help increase conversion.

4. Time Saving

It literally speeds up the buying process because when someone thinks of buying one specific product from the physical store which is very far and not easily available. Here how the eCommerce helps the customer to avail the specific product easily and speedily.

Easily retarget your customers.

There are many ways to retarget the customer and sell the product nicely. Below are some of the techniques which you can use to retarget customers:-

5. Easier to encourage an impulse buy

Impulse buying is one of the techniques where it works as a common behavior of customer’s perception towards a particular product. It is related to the control of human psychological behavior which is like some people possess personality traits that can be said as impulse buying tendencies.

6. Reviews Available

It has so many positive recommendations which can give more values to your **eCommerce website** and help customers to build more trust over a particular product. It can help you to be clear and more visible about the product that helps you with more product selection too. All of the reviews are valuable to customers, which can really help a lot to built trust over the products and services.

7. Provide flexibility to the customer to buy product 24/7.

It has more flexibility over the regular store because the services are available 24/7 and though helps to serve you the services at any time and anyplace.

8.No Geographical limitation

tap the global market form the day one.It is like the customer will have access to the online store from anywhere in the world, which can globally be accessed. This is what every customer is looking forward to having as their service because sometimes customers are not able to find a particular product which not available at the store location but though online store works like a magic to provide them with multiple options. So, that they can avail the services easily.

Disadvantages

1. Lack of personal touch

It is kind of consumer feeling that consumer can’t feel and touch the product. Sometimes no matter how good a product is explained and expressed you will not be able to sense the touch, smell, taste, and sound, through the dimensionality of a screen.

2. Unsure about the quality

One of the biggest problems with buying things online is that you will have no guarantee of a products’ quality. Reviews are not always helpful and though all the researches will never assure you about the quality of a product.

3. Late Delivery

When someone plans to order a product online, they are never assured to get delivered as per time and there are plenty of issues which make such situation very delicate for customers.

It is like you are waiting for an entire day leaving your work to just receive your new phone for example and though you are not getting delivered on that day itself.

4.Security issues

E-commerce sites record all the important details about the customers which are to be kept secured because it includes details like name, phone no, address, and bank details. If in these case sites don’t implement rigorous cybersecurity quantity.

Every online store has an issue with security whether they are small, medium or enterprise businesses. In short, you can say that online store has security issues which can never be predicted in this world of eCommerce.

5. Difficult to try before buying.

You can say that **online shoppers** will not have much ability to inspect physically, even sometimes they lose the power to negotiate the price and payment terms might exist different as compared to local stores.

6. Internet bandwidth

E-commerce is the store which totally runs on the internet and though it needs a good connection to run the business online. If you are not the good bandwidth connection than you might face issue with placing the orders, loading pages, and check out issues too.

7. Site Crash issues

The worst of the ecommerce disadvantages is when no one can buy from your store if your site crashes. That’s why it’s important to ensure your website is hosted on the right platform.

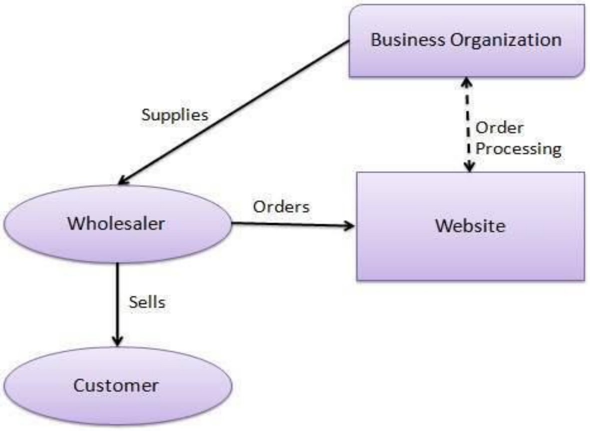
Types of e-commerce

Generally speaking, when most people think of e-commerce, they think of the purchase of goods or services by use of the internet. However, there is a more specific way to refer to the type of online transaction by the means of mentioning which e-commerce category the transfer falls under. There are six basic types of e-commerce

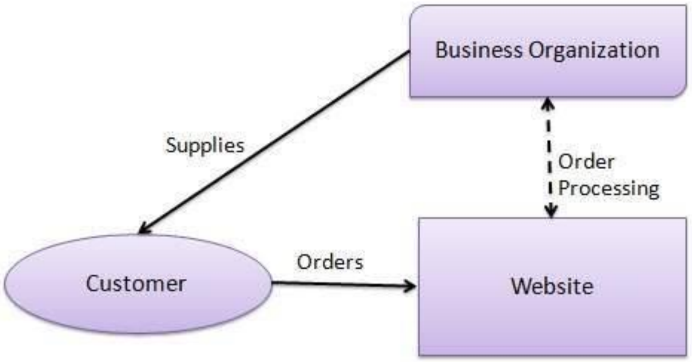
- Business-to-Business (B2B),
- Business-to-Consumer (B2C),
- Consumer-to-Consumer (C2C),
- Consumer-to-Business (C2B),
- Business-to-Administration (B2A) and
- Consumer-to-Administration (C2A) — and all of them represent a different purchasing dynamic.

Types of
E-commerc
B2B
C2C
B2C
C2B
C2A
B2A

Business-to-business (B2B) e-commerce refers to the electronic exchange of products, services or information between businesses rather than between businesses and consumers. (e.g. A business sells software-as-a-service for other businesses to use). **Example** : Intel selles micro-processors to Dell.



Business-to-consumer (B2C) is the retail part of e-commerce on the internet. It is when businesses sell products, services or information directly to consumers. (e.g. You buy a pair of shoes from an online retailer). **Example**: Amazon, Flipkart etc.



Today, there are innumerable virtual stores and malls on the internet selling all types of consumer goods. The most recognized example of these sites is Amazon, which dominates the B2C market.

Consumer-to-consumer (C2C) is a type of e-commerce in which consumers trade products, services and information with each other online. These transactions are generally conducted through a third party that provides an online platform on which the transactions are carried out.(e.g. You sell your old furniture on eBay to another consumer). **Example**: OLX, Quickr, Ebay etc.

Consumer-to-business (C2B) is a type of e-commerce in which consumers make their products and services available online for companies to bid on and purchase. (e.g. An influencer offers exposure to their online audience in exchange for a fee, or a photographer licenses their photo for a business to use).

Business-to-administration (B2A) refers to transactions conducted online between companies and public administration or government bodies. Many branches of government are dependent on e-services or products, especially when it comes to legal documents, registers, social security, fiscals and employment. Businesses can supply these electronically.

Consumer-to-administration (C2A) refers to transactions conducted online between individual consumers and public administration or government bodies. The government rarely buys products or services from citizens, but individuals frequently use electronic means in the following areas:

Education: disseminating information, distance learning/online lectures, etc.

Social security: distributing information, making payments, etc.

Taxes: filing tax returns, making payments, etc.

Health: making appointments, providing information about illnesses, making health services payments, etc.

FUNCTIONS OF AN E-COMMERCE

The following are five functions we should be doing daily in our e-commerce business. These simple steps can really improve conversion rates and, again, need to be done on a daily basis for any successful online business.

1) Search Engine Optimization (SEO)

- Generate unique relevant content. Google loves unique content that is related to what your site is all about.
    - Ensure you are using good keywords that you want to focus on.
- Ensure H1 tag is added around the focus of the page. For example, product name, category name, or static content title should be wrapped inside the H1 tag.
- Leverage H2 tags as well for other important page sections.
    - Keywords in optimized page titles.
- Internal linking. Link keywords in your unique content to pages related to that keyword.
- Friendly URLs with related phrases. E.g. When talking about Zobrist’s Mobiecom, the URL looks like this: “https://www.zobristinc.com/products/mobiecom/”

- Avoid any duplicate content appearing on multiple URLs by using the canonical tag. The canonical tag tells the search engine to group multiple URLs together since they share the same content.

2) <u>Selecting New Products</u>

- Sell what the customer wants to buy, not what you want to sell! This is a common mistake, especially when merchandisers are given a great price to sell a particular product. If nobody wants to buy that product, it doesn't matter what price you set it at.
- Find out what customers want. What is your value proposition on products you sell? Capitalize on your niche!

3) <u>Merchandising New Productions</u>

- Pictures, pictures, pictures! It is very important to have high-quality images of the products.
- Hero photos: if you have a big seller, feature it on a category page with a hero image of the product.
- Promote the latest releases in your newsletters and feature them in categories or on your homepage.
- Market to customers who have purchased related items in the past.

4) <u>Customer Service</u>

- Be proactive, and engage customers on the site constantly. If a customer stays on a page for some time, chances are they need help. Prompt the customers, and see if he/she would like to chat with one of the representatives. Business and technical teams should look into what the "friction" is, and address accordingly.
- Provide delivery estimation. If customers subscribe to the notification, ensure that you push any shipment updates information to customers via different channels (e.g., email / SMS / IoT devices — Amazon Alexa / Google Mini). Customers should not need to login and research the status of their orders.
- Deliver orders on time.
- Reship promptly if a package failed to be delivered to the customer, if it was damaged, or if it had missing parts. If an order was not delivered to customers within the estimated timeframe due to package loss, the system should determine if an order should be re-shipped. At the same time, a notification should be sent to customers and let them know of the delay or that the order has been re-shipped.

- In order to retain customers' loyalty, we need to make sure customers feel comfortable with the purchase experience. We must earn their trust. With trust, customers will come back again.

5) <u>Monitoring your KPIs (Key Performance Indicator) / Analytics</u>

- Monitor your analytics reports. View what items are selling and bubble them to the top of product listings so customers can find them more easily. A great tool for this, if you are on HCL Commerce (formerly IBM WebSphere Commerce), is our Smart Merchandiser product. With it, you can see analytic overlays on each product, in each category, to help you make smart merchandising decisions. Tackle cart abandonment. Remarket those products to the customers if you have their email addresses. Incentivize them to complete their checkout within X days.
- From the report, you should also check for possible "friction" on the site. A good indicator would be where the number of sessions dropped. For example, customers have added items to their carts, but not many of them have placed orders. In this scenario, there might be "friction" in the checkout flow where the customer has no choice but abandon the cart.

<u>Applications of E-Comm</u>

The most common E-commerce applications are as follows:

- **<u>Online marketing and purchasing</u>** Data collection about customer behavior, preferences, needs and buying patterns is possible through Web and E-commerce. This helps marketing activities such as price fixation, negotiation, product feature enhancement and relationship with the customer.

- **<u>Retail and wholesale</u>** E-commerce has a number of applications in retail and wholesale. E-retailing or on-line retailing is the selling of goods from Business-to-Consumer through electronic stores that are designed using the electronic catalog and shopping cart model. Cybermall is a single website that offers different products and services at one Internet location. It attracts the customer and the seller into one virtual space through a Web browser.

- **Finance** Financial companies are using E-commerce to a large extent. Customers can check the balances of their savings and loan accounts, transfer money to their other account and pay their bill through on-line banking or E-banking.

- **Manufacturing** E-commerce is also used in the supply chain operations of a company. Some companies form an electronic exchange by providing together buy and sell goods, trade market information and run back-office information such as inventory control. These speeds up the flow of raw material and finished goods among the members of the business community.

- **Online Auction Customer**-to-Customer E-commerce is direct selling of goods and services among customers. It also includes electronic auctions that involve bidding. Bidding is a special type of auction that allows prospective buyers to bid for an item. For example, airline companies give the customer an opportunity to quote the price for a seat on a specific route on the specified date and time.

- **E-Banking** Online banking or E- banking is an electronic payment system that enables customers of a financial institution to conduct financial transactions on a website operated by the institution, Online banking is also referred as internet banking, e-banking, virtual banking and by other terms.

- **Online publishing** Electronic publishing (also referred to as e-publishing or digital publishing) includes the digital publication of e-books, digital magazines, and the development of digital libraries and catalogs.

- **Online booking (ticket, seat.etc)** An **Internet booking engine** (IBE) is an application which helps the travel and tourism industry support reservation through the Internet. It helps consumers to book flights, hotels, holiday packages, insurance and other services online.

Tools & Technologies for E-commerce

TOOLS

Website tools – Website tools are used to set up our store and help us to manage it.

Ex- SaaS (Software as a service)- Shopify, HubSpot, BoostMySales, BuildaBazaar, BigCommerce, X-Cart, WooCommerce etc.

Research tools –Research tools helps us to find **winning products**, **estimate sales**, **research keywords**, and **spy on competitors** all from one easy-to-use dashboard. Basically, it instantly shows us what products will be the most profitable and easiest to grow your business with. Such types of tools are also used for improving online visibility and discovering marketing insights.

EX-JungleScout, SEMRush.

Business tools – Business tools are used to manage the day-to-day operations, logistics and finances of our ecommerce store. Once we have a store, we've got to fill it with inventory, keep track of our employees or outsource workers, track our budget, and tackle the day-to-day financials.

EX-Monday, Sourcify, Inventory Source

Marketing tools – Marketing tools are essential because they are used by businesses as a means of communication to inform the public of its products and services. These tools create market awareness which in the long run can make a business profitable. These tools are used to let the world know you exist, drive traffic, convert leads into customers, and build your brand. Your ecommerce store won't make sales if you don't market it. There are hundreds of marketing apps, addressing everything from social media automation to affiliate and relationship marketing and loyalty management.

EX-MailChimp, Campaign Monitor, Bulk.Ly, ReferralCandy

Analytics tools – Data can help businesses better understand their customers, improve their advertising campaigns, personalize their content and improve their bottom lines. The advantages of data are many, but you can't access these benefits without the proper data analytics tools and processes.

So such types of tools are used to tell you how well everything we're doing is working and spot any leaks in your sales funnels. Analytics tools use data science to help you understand what your customers want, why they came to your store in the first place, and how you can attract more of them.

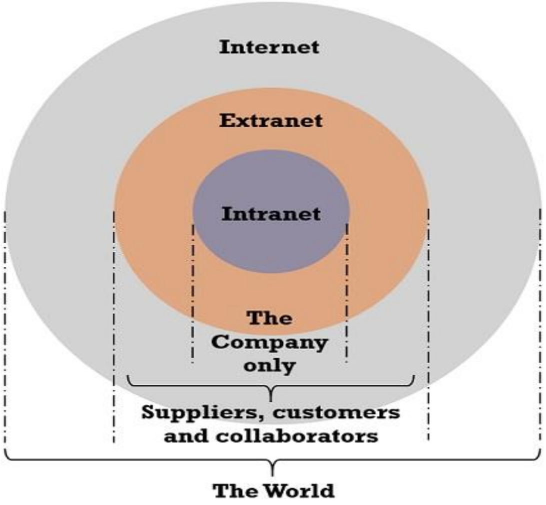
EX-VWO: Visual Website Optimizer, Google Analytics.

Technologies

- Internet, Intranet, Extranet
- Networking Devices (Hub, Switch, Router)
- Protocols
- Electronic Data Interchange (EDI)
- Electronic Fund Transfer (EFT)
  - ➢ SSL Certificates
  - ➢ Payment Gateways
  - ➢ Trust Marks

Internet, Intranet, Extranet

An intranet is a private network, operated by a large company or other organization, which uses internet technologies, but is insulated from the global internet. An extranet is an intranet that is accessible to some people from outside the company, or possibly shared by more than one organization.



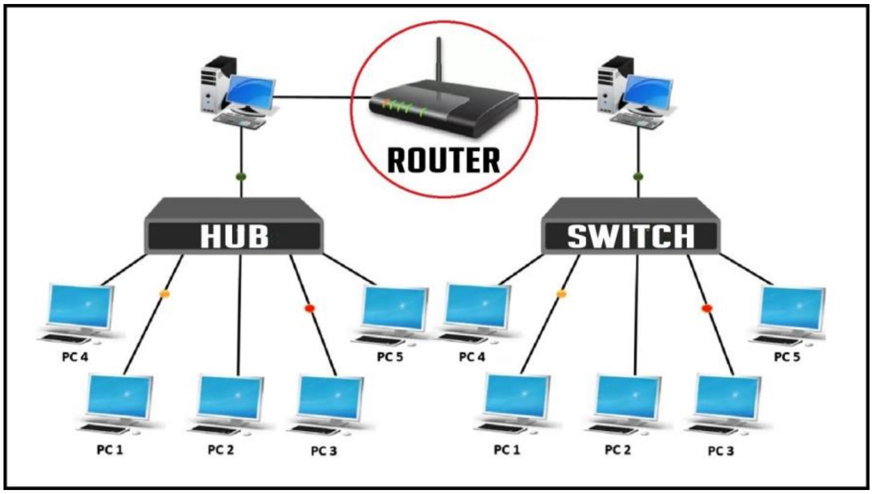
BASIS FOR COMPARISON	**INTERNET**	**INTRANET**
Meaning	Connects different network of computers together	It is a part of Internet which is privately owned by a particular firm
Accessibility	Anyone can access the Internet	Accessible only by the organization members, having

		login details.
Safety	Is not as safe as compared to Intranet	Safe
No of Users	Unlimited	Limited
Visitors Traffic	More	Less
Network Type	Public	Private
Information Provided	Unlimited, and can be viewed by everyone	Limited, and circulates among the members of an organization

Networking Devices (Hub, Switch, Router etc.)

- **Hub**- Hub is a networking device operates at the physical layer of **OSI model.** It refers to a hardware device that enables multiple devices or connections to be connected to a computer. An **example** is a USB **hub**, which allows multiple USB devices to be connected to one computer, even though that computer may only have a few USB connections.

- **Switch**- A switch is a networking device works under Data Link Layer of OSI Model. A switch is used to network multiple computers together. Switches made for the consumer market are typically small, flat boxes. These ports can connect to computers, cable or DSL modems, and other switches. Switches are more advanced than hubs and less capable than routers.



- **Router**- The router is a inter-networking device works under the networking layer of the **OSI model**. A router is a networking device that forwards data packets between computer networks. It that allows communication between your local home network — like your personal computers and other connected devices — and the internet.

Protocols

- **TCP/IP (Transmission Control Protocol/Internet Protocol)** specifies how data is exchanged over the internet by providing end-to-end communications that identify how it should be broken into packets, addressed, transmitted, routed and received at the destination. TCP/IP requires little central management, and it is designed to make networks reliable, with the ability to recover automatically from the failure of any device on the network. The two main protocols in the internet protocol suite serves specific functions. **TCP** defines how applications can create channels of communication across a network. It also manages how a message is assembled into smaller packets before they are then transmitted over the internet and reassembled in the right order at the destination address. **IP** defines how to address and route each packet to make sure it reaches the right destination. Each gateway computer on the network checks this IP address to determine where to forward the message.

- **HTTP (Hypertext Transfer Protocol)** is the set of rules for transferring files, such as text, graphic images, sound, video, and other multimedia files, on the World Wide Web. As soon as a Web user opens their Web browser, the user is indirectly making use of HTTP. It is the communications protocol used to connect to Web servers on **the** Internet or on a local network (intranet). **Its** primary **function** is to establish a connection with **the** server and send HTML pages back to **the** user's browser.

  TCP/IP made the internet, and **HTTP** made the web.

  There would be no web without HTTP and no internet without TCP and IP.

- **File Transfer Protocol (FTP)** is a standard Internet protocol for transmitting files between computers on the Internet over TCP/IP connections. FTP is a client-server protocol where a client will ask for a file, and a local or remote server will provide it.

- **SMTP (Simple Mail Transfer Protocol)** is a TCP/IP protocol used in sending and receiving e-mail. However, since it is limited in its ability to queue messages at the receiving end, it is usually used with one of two other protocols, POP3 (Post Office Protocol) or IMAP (Internet Message Access Protocol), that let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving e-mail.

SMTP works as a three-step process, using a client/server model. First, an e-mail server uses SMTP to send a message from an e-mail client, such as Outlook or Gmail, to an e-mail server. Second, the e-mail server uses SMTP as a relay service to send the e-mail to the receiving e-mail server. Third, the receiving server uses an e-mail client to download incoming mail via IMAP and place it in the inbox of the recipient.

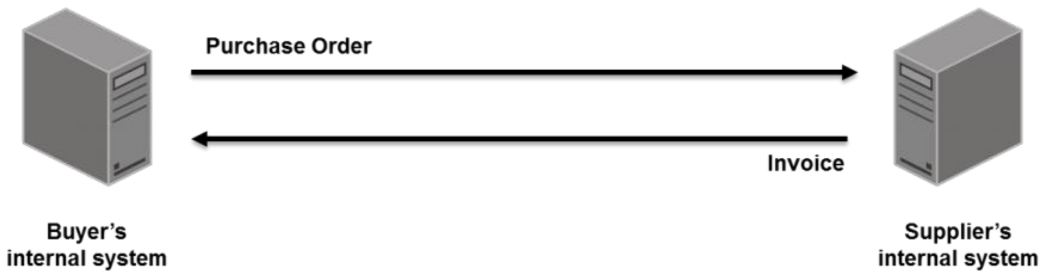
Difference-

- POP3 will download all the emails to our system for us to view, and by doing so, all emails are removed from the mail server
- IMAP will send a copy of the emails to our system, but leaving the originals on our mail server.

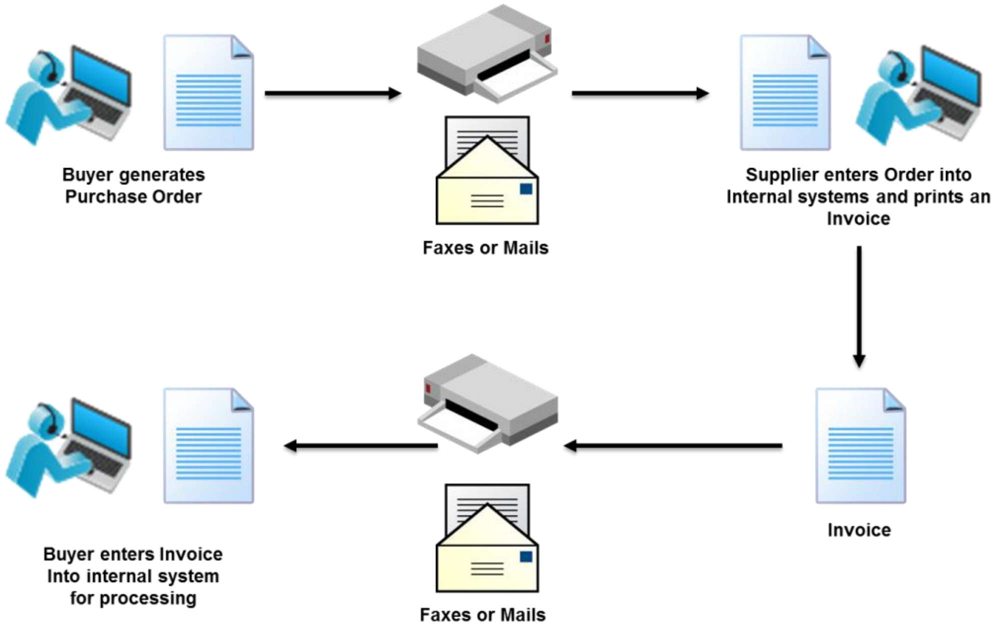
Electronic Data Interchange (EDI) - a process which allows one company to send information/data to another company electronically rather than with paper.

Electronic Data Interchange (EDI) is the automated, **computer-to-computer** exchange of standard electronic **business documents** between **business partners** over a secure, standardized connection.

The EDI process looks like this — no paper, no people involved:



A typical manual process looks like this, with lots of paper and people involvement:



Each term in the definition is significant:

- **Computer-to-computer**– EDI replaces postal mail, fax and email. While email is also an electronic approach, the documents exchanged via email must still be handled by people rather than computers.

  Having people involved slows down the processing of the documents and also introduces errors. Instead, EDI documents can flow straight through to the appropriate application on the receiver's computer (e.g., the Order Management System) and processing can begin immediately.
- **Business documents** – These are any of the documents that are typically exchanged between businesses. The most common documents exchanged via EDI are purchase orders, invoices and advance ship notices. But there are many, many others such as bill of lading, customs documents, inventory documents, shipping status documents and payment documents.
- **Standard format**– Because EDI documents must be processed by computers rather than humans, a standard format must be used so that the computer will be able to read and understand the documents. A standard format describes what each piece of information is and in what format (e.g., integer, decimal, mmddyy). Without a standard format, each company would send documents using its company-specific format and, much as an English-speaking person probably doesn't understand Japanese, the receiver's computer system doesn't understand the company-specific format of the sender's format.

  Standard EDI Format

  - EDI documents are processed by computers and use standard, computer-friendly formats.
  - Standards describe each piece of data and its format (e.g., type of document, parties involved, actions to take, mmddyy).
  - Standards eliminate company-to-company variations, allowing each business partner's computer system to speak a common language.
  - There are a variety of EDI standards for various industries, regions and use cases - each with different versions, so EDI partners must use the same standard and version
  - Popular standards include: ANSI X12 in the U.S., UN/EDIFACT globally and industry-specific standards, such as HIPAA
- **Business partners** – The exchange of EDI documents is typically between two different companies, referred to as business partners or trading partners. For example, Company A may buy goods from Company B. Company A sends orders to Company B. Company A and Company B are business partners.

Electronic Fund Transfer

An electronic funds transfer is a widely used method for moving funds from one account to another using a computer network. Electronic funds transfers replace paper-based transfers and human mediators.

One of the most widely-used EFT programs is direct deposit, through which payroll is deposited straight into an employee's bank account. However, EFT refers to any transfer of funds initiated through an electronic terminal, including credit card, ATM, Fedwire and point-of-sale (POS) transactions. It is used for both credit transfers, such as payroll payments, and for debit transfers, such as mortgage payments.

Every time a banking customer uses her credit or debit card, whether at a physical point-of-sale or online, she’s engaging in an electronic funds transfer. Any preauthorized charges, such as direct deposits or utility bills, also utilize an EFT.

Types of EFTs

The most common types of EFTs include:

- **Direct deposit**: Enables businesses to pay employees. During the employee onboarding process, new employees typically specify the financial institution to receive the direct deposit payments.
- **Wire transfers**: Used for non-regular payments, such as the down payment on a house.

- **Automated Teller Machines (ATMs)**: Allows cash withdrawals and deposits, fund transfers and checking of account balances at multiple locations, such as branch locations, retail stores, shopping malls and airports.
- **Debit cards:** Allows users to pay for transactions and have those funds deducted from the account linked to the card.
- **Pay-by-phone systems**: Allows users to pay bills or transfer money over the phone.
- **Online banking**: Available via personal computer, tablet or smartphone. Using online banking, users can access accounts to make payments, transfer funds and check balances.

An eCommerce website is very different from the static website. Customers make an online payment, enters credit card info on the website, and many more. A Study of more than 350 active internet users showed that 90% of the people are worried about their credit card information and identities that can be stolen online. Hence an eCommerce website needs stronger security to protect from any attacks. **SSL Certificate, Payment Gateways, Trust Marks** are important from them.

- **SSL Certificate**

An **SSL certificate** is a bit of code on your web server that provides security for online communications. When a web browser contacts your secured website, the **SSL certificate** enables an encrypted connection. It's kind of like sealing a letter in an envelope before sending it through the mail.

ecommerce websites ask customers to provide credit/debit card passwords during the checkout process. In these scenarios, it is the responsibility of the eCommerce website owner to make the online transaction error free & secure. An SSL encryption ensures a secure transaction between the webserver & web page. The keys required to decrypt the information is known only to the webserver & web page and hence makes it impossible for any third person to hack the information.

- **Payment Gateways**

A payment gateway is a technology used by merchants to accept debit or credit card purchases from customers. Payment gateway allows the merchants to process credit, debit and other alternative online payments. Payment gateway acts as the go-between to make sure that customer data is encrypted and secure. Using payment gateway can help to lessen frequency and severity of credit card fraud within e-commerce business.

- **Trust Marks**

An e-commerce Trustmark is a badge, image or logo found on an electronic commerce website that indicates the site is a member of a professional organization or has passed security tests. it can give customers confidence and can encourage them to do business with you. These trust marks show our audience that our website is totally reliable and that their personal information is 100% secure.

While you may not be familiar with the term, you’ve definitely seen these symbols on your favorite company websites:

Customers recognized several of the logos, but the most well-known are:

- McAfee (79%)
- Verisign (76%)
- Paypal (72%)
- BBB (37%)
- TRUSTe (28%)

Issues & Challenges in E-commerce

E-commerce has grown at an incredible rate since its birth, and so has the competition to make the best use of it. There are challenges standing in the way of companies, big and small alike. Developing an e-commerce business is hard. You have to take great care over everything, from website maintenance through to customer service.

1. Online Identity Verification

When a visitor registers on an eCommerce website, the information they enter may not be genuine – therefore you cannot know if they are genuinely interested in purchasing. For instance, cash-on-delivery purchases made with a fake phone number and address can make massive losses in revenue.

2. Cybersecurity Issues

Cyberattacks can compromise the security of your eCommerce website by infecting it with viruses and, what's even worse, they may compromise the security of your registered customers' data. Hackers can potentially gain access to this confidential data, including your users' credit card details. This scenario is one of the greatest challenges to overcome in eCommerce business – and is certainly one of the biggest nightmares of every eCommerce owner.

3. Product Returns and Refunds

Returns and refunds are a very big deal in the minds of customers. Over 60% of online shoppers look at the shop's return policy before making a purchase.

48% of customers would shop more if stores offered less complicated returns and inconvenient returns policy deters 80% customers. Furthermore, 89% of online shoppers have made a return at one point during their shopping experience.

4. Competition

Manufacturers and retailers that online stores buy products from in bulk eventually begin selling their goods directly to customers. This way, the company that used to be your partner becomes your competitor which only gets worse if they create their own network of distributors.

5. Choosing the right technology & partners

Some online retailers may face growth challenges because their technology is limiting them or they've hired the wrong partners/agencies to help them manage their projects.

6. Finding the right products to sell

Anyone can launch an online store within days and start selling all sorts of products.

Amazon is taking over the eCommerce world with their massive online product catalog. Their marketplace and fulfillment services have enabled sellers from all over the world to easily reach paying customers.

7) Maintaining customer loyalty

Even with the best-designed website out there, without customer trust and loyalty, the business is bound to struggle.

Creating new customers and then maintaining them requires a massive effort. One of the reasons e-commerce companies in particular face a challenge in building customer trust and loyalty is the seller and buyer don't know each other. Nor can they see each other.

M-commerce

M-commerce (mobile commerce) is the buying and selling of goods and services through wireless handheld devices such as smart phones and tablets. As a form of e-commerce, m-commerce enables users to access online shopping platforms without needing to use a desktop computer. Examples of m-commerce include in-app purchasing, mobile banking, virtual marketplace apps like the Amazon mobile app or a digital wallet such as Apple Pay, Android Pay and Samsung Pay.

Over time, content delivery over wireless devices has become faster, more secure and scalable. As of 2017 the use of m-commerce accounted for 34.5% of e-commerce sales. The industries affected most by m-commerce include:

- Financial services, which includes mobile banking (when customers use their handheld devices to access their accounts and pay their bills) as well as brokerage services, in which stock quotes can be displayed and trading conducted from the same handheld device.
- Telecommunications, in which service changes, bill payment and account reviews can all be performed from the same handheld device.
- Service and retail, as consumers are given the ability to place and pay for orders on-the-fly.
- Information services, which include the delivery of financial news, sports figures and traffic updates to a single mobile device.

Types of m-commerce

M-commerce can be categorized by function as mobile shopping, mobile banking or mobile payments. Mobile shopping allows for a customer to purchase a product from a mobile device, using an application such as Amazon, or over a web app. A subcategory of mobile shopping is app commerce, which is a transaction that takes place over a native app. Mobile banking includes any handheld technology that enables customers to conduct fanatical transactions. This is typically done through a secure, dedicated app provided by the banking institution. Mobile payments enable users to buy products in-person using a mobile device. Digital wallets, such as Apple Pay, allow a customer to buy a product without needing to swipe a card or pay with physical cash.

Advantages of M-Commerce

1. Through M-commerce, the companies can be in regular touch with the users through the **Push Notifications**. Any discount, scheme, pay back benefits can be communicated to the customers through a message to their mobile phones. **E.g.** ShoppersStop always sends a message to its members about the Season Sale.
2. M-Commerce enables local business to grow by tracking the **location** of the potential customer and sharing the information on their mobile phones. **E.g**. The educational institutes track down the local students and give information about the courses offered by them.
3. With the help of M-commerce, the users can **pay** their mobile bills, electricity bills, without standing in the long queues.

   E.g. Mobile applications such as Paytm, Freerecharge are the online payment platforms.
4. M-commerce enables the customers to **book** movie tickets, railway tickets, air tickets, event tickets thereby saving a lot of time.

   E.g. Book My Show, IRCTC mobile applications offers the online reservation services.
5. Through M-Commerce, customers can **easily access** the complete information about the product or service provider before availing its services.

   E.g. Any new restaurant is opened in the city; one can access about it in detail through mobile.
6. M-Commerce helps the marketer to have a **wider reach** of potential customers than he can have by visiting all personally.

   E.g. Text can be sent to the mobile phones of many potential customers residing in different parts of the country Make My trip is the best example.

Disadvantages of M-Commerce

1. The **Screen** of mobile phones is generally **small** as compared to the computer screen and, therefore, the display of cellular gadgets may not influence the user to make the purchase. **E.g.** Through Flipkart Mobile Application a customer can see several products, but the user may not decide on the purchase because of the smaller image of the product and rather rely on E-commerce i.e. computers for the better view to make a purchase decision.
2. M-Commerce **software is costly** as compared to the E-commerce, many retailers may not go for it, and hence the mobile users may have fewer options.

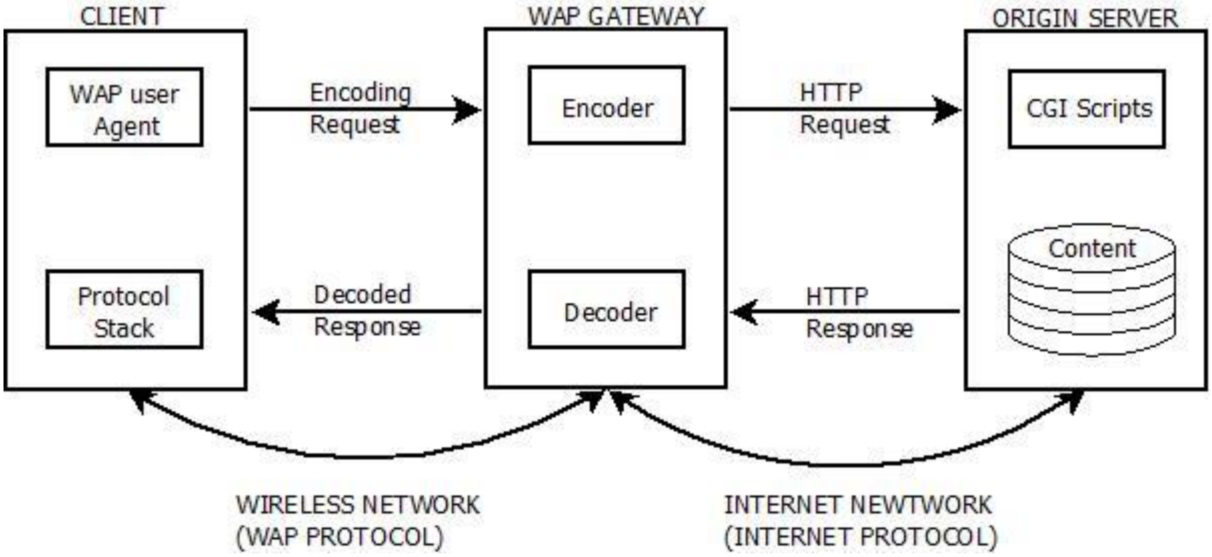
3. **Poor connectivity** also hampers the M-commerce to flourish. Sometimes the data is too slow to access the websites through mobile applications.
4. M-commerce, being the latest technology is struggling with its **applications in terms of its graphics and the content** that result in more reliance on the E-commerce applications.
5. Information shared through the wireless medium have higher chances of getting **hacked**. Therefore, people use more of E-commerce applications to perform the money transactions.

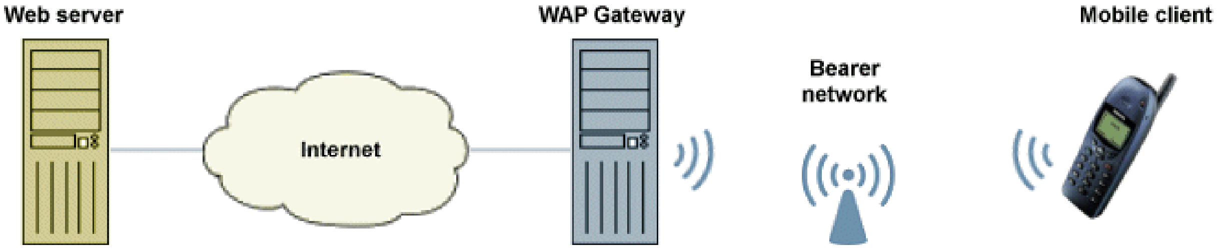
WAP (Wireless Application Protocol)

On June 26, 1997, Ericsson, Motorola, Nokia, and Unwired Planet took the initiative to start a rapid creation of a standard for making advanced services within the wireless domain a reality. **W***ireless* **A***pplication* **P**rotocol is a secure specification that allows users to access information instantly via handheld wireless devices such as mobile phones, pagers, two-way radios, smart phones and communicators.

WAP stands for Wireless Application Protocol. The dictionary definition of these terms are as follows –

- **Wireless** − Lacking or not requiring a wire or wires pertaining to transmission.
- **Application** − A computer program or piece of computer software that is designed to do a specific task.
- **Protocol** − A set of technical rules about how information should be transmitted and received using computers.





- Wireless Session Protocol (WSP) - with WTP, a complete replacement for HTTP, allowing the efficient exchange of data between mobile web applications.
- Wireless Transaction Protocol (WTP) - provides transaction support (reliable request/response) to the datagram service provided by WDP.
- Wireless Transport Layer Security (WTLS) - an optional security layer based on the Secure Sockets Layer (SSL) protocol that provides a secure transport layer connection using encryption.
- Wireless Datagram Protocol (WDP) - a transport layer datagram service like UDP that sends and receives messages via any available bearer network, providing unreliable transport of data. The precise implementation of WDP is dependent on the network layer protocol used by the bearer network, although on IP-based networks it is effectively the same as UDP.

FUNDAMENTAL OF E-COMMERCE

UNIT-2

WEB BASED E-COMMERCE

Web based e-comm. generally means E-Commerce with **WWW/Internet**: Both the Web and the Internet have grown, but the Web has grown much faster as a whole.

Web-based E-commerce is one of the **fastest-growing** segments of the technology that defines the business strategy. Web-based E-commerce provides easy and better communication between geographically separated buyers and sellers.

E-commerce is a way of doing business by enabling better interaction among customers, business partners and business relationship managers using electronic tools. The Web provides a collection of electronics tools such as e-mail and Web pages for E-commerce and its related processes. Web-based E-commerce continues to improve convenience and versatility using increased processing power and expanded cellular capabilities and makes it more reachable to the customers.

NEED FOR WEB BASED BUSINESS

The new requirements of e-commerce gave rise to web-based business.

- **High performance**. A popular Web site will typically have tens of millions of "hits" per day, and users expect low latency from it. Customers will not tolerate the site simply refusing their requests.
- **High availability**. E-commerce sites are expected to be available "24/7." They never close, so must have minimal downtime-perhaps a few minutes per year.
- **Scalability**. As Web sites grow in popularity, their processing capacity must be able to similarly grow, to both expand the amount of data they can manage and maintain acceptable levels of customer service.
- **Security**. Users must be assured that any sensitive information they send across the Web is secure from snooping. Operators of Web sites must be assured that their system is secure from attack (stealing or modifying data, rendering data unusable by flooding it with requests, crashing it, etc.).
- **Modifiability**. E-commerce Web sites change frequently, in many cases daily, and so their content must be very simple to change.

TECHNOLOGIES OF WEB BASED BUSINESS

- **WEB BROWSERS** For Modifiability
- **HTTPS** For Security
- **PROXY SERVERS** For Performance
- **ROUTERS AND FIREWALLS** For Security
- **LOAD BALANCING** For Performance, Scalability, And Availability
- **WEB SERVERS** For Performance
- **APPLICATION SERVERS** For Modifiability, Performance, And Scalability
- **DATABASES** For Performance, Scalability, And Availability

Steps for setting up a web-based business.

- **Choosing the right format of website**
  - Characteristics of a good web-site
  - Horizontal portals
  - Vertical portals
- **Steps in setting up business on Internet**
  - Selection & registration of domain name
  - Website Development
    - Client & server-side tools,
    - Web authoring tools,
    - Website hosting,
    - Website Maintenance
- **Online Promotion tools & techniques**
  - Online promotion tools,
  - Offline promotion tools.
- **Web Traffic**
  - Various measures
  - Need of web traffic analysis
  - Web Log File
- **Search Engine optimization techniques**
- **Payment Gateways for online payment**
- **Security of transactions on Web**

Choosing the right format of website

We need to choose the right eCommerce template to ensure your online store is making a good first impression. And it's not only a color scheme that should be taken into account. A perfect universally **appealing website design** is about careful selection of fonts, an appropriate theme that fits the products you sell, page loading speed, retina-ready images, responsive easy-to-navigate layout and many other things combined in one place.

- Your template design should create an excellent experience for your customers, making them come back over and over again
- Intuitive interface on all pages, including checkout, homepage and product page, will improve your conversions
- Responsiveness is what makes your online store look good across all devices
- The ideal template works for SEO and lets your positions in search engines improve
- If your template is ready for marketing activities, then you are ready for sales
- Honed to perfection site search and autocomplete is a way to improving your UX
- The ability to customize your store to match your brand
- Good template evokes warm feelings inside your customers' hearts and souls

Characteristics of a good web-site

- Well Designed and Functional
- Easy to Use
- Optimized for Mobile
- Fresh, Quality Content
- Readily accessible contact and location
- Clear calls to action
- Optimized for Search and the Social Web

Web-Portal

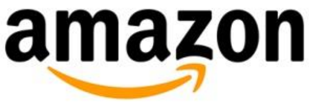
A portal is a web-based platform that collects information from different sources into a single user interface.

Websites are for driving traffic, whereas **web portals** are for limiting traffic to a specific group of users. Most web portals require a user to log in, which allows the site to deliver more specific content and services based on who that user is.

Horizontal Portal:

These are web portals which focus on a wide array of interests and topics. They focus on general audience and try to present something for everybody. It is not mainly focused on a specific category of items to sell but sells almost everything thus, reach a broader audience.

The most famous horizontal e-commerce business is Amazon.com It sells books, furniture, food, grocery, apparel, toys, software, music, gadgets, and a whole lot more.



An arrow pointed from **a to z** defines the concept of horizontal marketing i.e., it sells everything right from the product name starts with the very first alphabet **a** to the last alphabet **z**. And the arrow pointed in such a way that it forms a smile that shows customer satisfaction i.e., customers must be happy with the product they purchase from Amazon.com.

Vertical Portal:

These are web portals which focus only on one specific industry, domain or vertical. Vertical portals provide tools, information, articles, research and statistics on the specific industry or vertical. Unlike the horizontal marketplace model, vertical marketplaces aimed at a single market sector to serve some specific category of products to the targeted audience.

Example Bluestone.com, Netmed.com

Steps in setting up business on Internet

Selection of domain name:

A domain name is your **website name**. A domain name is the address where Internet users can **access your website**. A domain name is used for finding and identifying website on the Internet. Computers use **IP addresses**, which are a series of number. However, it is difficult for humans to remember strings of numbers. Because of this, domain names were developed and used to identify entities on the Internet rather than using IP addresses. The domain name must be registered before you can use it. Every domain name is unique. No two websites can have the same domain name.

A domain name takes the form of two main elements. For example, the domain name **Facebook.com** consists of the website's name (Facebook) and the domain name extension (.com).

POINT TO REMEMBER WHEN CHOOSING A DOMAIN NAME

1. Make it easy to type

Finding a domain name that's easy to type is critical to online success. If you use slang (u instead of you) or words with multiple spellings (express vs. xpress), it might be harder for customers to find your site.

2. Keep it short

If your domain name is long and complex, you risk customers mistyping or misspelling it. Short and simple is the way to go.

3. Use keywords

Try using keywords that describe your business and the services you offer. For example, if you're a Brass replacement business, you may want to register BrassRepair.com or BrassReplacement.com.

4. Target your geographic area

If your business is local, consider including your city or state in your domain name to make it easy for local customers to find and remember. Example: MoradabadBrass.com.

5. Avoid numbers and hyphens

Numbers and hyphens are often misunderstood — people who hear your website address don’t know if you’re using a numeral (5) or it’s spelled out (five) or they misplace or forget the dash. If you need these in your domain, register the different variations to be safe.

6. Be memorable

There are millions of registered domain names, so having a domain that’s catchy and memorable is essential. Once you’ve come up with a name, share it with close friends to make sure it sounds appealing and makes sense to others.

7. Research it

Make sure the name you’ve selected isn’t trademarked, copyrighted or being used by another company. It could result in a huge legal mess that could cost you a fortune, as well as your domain!

8. Use an appropriate domain name extension

Extensions are suffixes, such as .com or .net, at the end of web addresses. These can have specific uses, so make sure to choose one that works for your business. The .com domain extension is the most popular, but it can be tough to get a short and memorable .com domain name because.

A good option is .in, as it tells all who see it that your business located right here in India.

- .cricket : for youth leagues, pro teams and fans.
- .dev : for web developers, coders and other tech professionals.
- .green : for businesses involved in the global sustainability movement.

9. Protect and build your brand

To protect your brand, you should purchase various domain extensions, as well as misspelled versions of your domain name. This prevents competitors from registering other versions and ensures your customers are directed to your website, even if they mistype it.

10. Act fast

Domain names sell quickly. Thankfully, they’re also inexpensive, so register your favorite domain names as soon as possible. If you’re having trouble finding an available name, domain registrars like GoDaddy will suggest alternate names during your domain search to help you find the perfect domain name.

Registration of domain name

There isn't a business in existence these days that doesn't need a website and a registered domain name in order to survive. Once we've chosen the perfect (and available) domain name, the hard part is over. We just need to register the domain name. Getting a domain name involves registering the name we want with an organization called **ICANN** **(The Internet Corporation for Assigned Names and Numbers)** through a domain name registrar like **GoDaddy**, **Domain.com** (also known as Dotster), 123-reg, Namecheap etc.

For example, if we choose a name like "example.com", we will have to go to a registrar, pay a registration fee that costs around INR700 to INR2500 for that name. That will give us the right to the name for a year, and we have to renew it annually for (usually) the same amount per annum.

Website development

Web development is not a single activity—it's an umbrella term for several fields of website creation. The primary forms of web development are **client-side**, **server-side**, and **full-stack development**. Both client and server-side programs are necessary to make a website function.

Server-side is the systems that run on the server, and **client-side** is the software that runs on a user's web browser. Client-side web development involves interactivity and displaying data, server-side is about working behind the scenes to manage data. **Full-stack developers**, on the other hand, have the skills of both client-side and server-side web developers.

Client-Side Web Development: Client-side developers use their coding skills to create visually appealing, functional, and helpful web applications and dynamic websites. These programmers are responsible for every part of a website that users see or interact with. Homepages, shopping pages, slideshows—virtually any visible feature that shows up in a web browser or requires user input falls under this discipline. Client-side developers are also known as 'front end' programmers, as the 'front' of a web page is what receives user interaction. Common scripting languages used by front end developers to create client-side code include JavaScript, HTML, and CSS.

Server-Side Web Development

To understand what a server-side developer does, we must first go over how a website works and how it’s different from a picture or an interactive text document. These software developers **design**, **build**, and **maintain** the server-side code that makes this **exchange of data possible**. These programmers are also known as **backend developers**. They work behind-the-scenes, making sure everything runs as it should on the application servers.

Web authoring tools

A category of software that enables the user to **develop a web site** in a desktop publishing format. Web authoring tools are used to create **Web content**, and cover a wide range of software programs we can download to our computer or access online. The World Wide Web Consortium, or W3, issues guidelines for web authoring tools that create a basic industry standard for web accessibility. The guidelines encourage web-authoring tool manufacturers to include specific features in their products that will aid Internet users with disabilities. All of the major web-authoring tool manufacturers follow the W3 guidelines. Some web authoring tools are here as-

- **Word Processors**

  Word processors like **Microsoft Word**, **WordPerfect** or **OpenOffice Writer** are some of the most popular web authoring tools available. Users can create a Web page just as they would a printable document and then save it in HTML format, creating a quick and easy web page.

- **Desktop Publishing Programs**

  Desktop publishing programs, like **Adobe InDesign** and **Scribus** are designed for producing material like newspapers, magazines, books and Web pages.

- **Online Web Page Builders**

  Website hosting sites usually offer their customers many web-authoring tool options to create and maintain their web pages online. Tools can include Web page builders, shopping systems, audio/visual editors and domain options.

- **HTML Editors**

  HTML editing programs like **Adobe Dreamweaver** are some of the most powerful web authoring tools available. They are generally used by professional Web designers to create commercial websites.
- **Plain Text Editors**

  Basic text editors like **Notepad** are also a useful Web authoring tool for those familiar with the code. Unlike word processors or desktop publishing programs, plain text editors do not apply additional code to what appears in the document. Plain text editors are also useful for quickly making edits to completed pages that require updates.

Website Hosting

To make a website available online, its files need to be uploaded to a web server, which is typically purchased from a hosting provider. This service is known as **web hosting**.

In other words, we can say that a web hosting is a service that comprises a website (code, images, etc.) available for viewing online. Every website you've ever visited is hosted on a server. Choosing the right hosting plan will mean having access to the right allocation of resources to keep your website loading quickly and reliably for your visitors.

How does web hosting work?

Web hosting happens when the files that make up a website are uploaded from a local computer on to a web server. The server's resources, (RAM, hard drive space, and bandwidth) are allocated to the websites using it. The division of server resources varies depending on the type of hosting plan chosen. Choosing web hosting is similar to searching for office space. Once the website's files are uploaded to a hosting company's web server, the host is then responsible for delivering the files to users.

Types of web hosting

As technology has progressed, different types of web hosting have been introduced to meet the different needs of websites and customers best. These include:

- Dedicated Hosting
- VPS Hosting
- Shared Web Hosting
- Reseller
- Cloud

Dedicated Hosting

Dedicated hosting is an Internet hosting option in which a physical server (or servers) is dedicated to a single business customer. The customer has complete control over the machine, so they can optimize it for their unique requirements, including performance and security.

It is like when your website comes with its server. It offers reliable power and flexibility but at a higher cost. It provides entire servers to rent. It is only really used when a website has a lot of traffic. It can handle up to 30 times an increase in your daily traffic. It also comes with guaranteed security and faster page loading.

VPS (Virtual Private Server) Hosting

Virtual Private Server (VPS) is hosting that virtually mimics dedicated server environments within a shared server. VPS hosting has become a popular choice because it is generally lower in cost than dedicated hosting but provides better reliability, security, and performance than shared hosting.

It is when a virtual server appears to each client as a dedicated server even though it's actually serving multiple websites.

VPS is often used by smaller websites and organizations that want the flexibility of having a dedicated server, without the high costs implied.

Shared Web Hosting

A shared web hosting service is a web hosting service where many websites reside on one web server connected to the Internet. This is generally the most economical option for hosting, as the overall cost of server maintenance is spread over many customers.

The advantage of this setup is the shared cost. The biggest disadvantage of a shared hosting account is that we're at the mercy of the other sites on your server. A really popular site may adversely affect the performance of our own site. It is difficult to provide better performance in this type of web hosting.

Reseller Web Hosting

Reseller hosting packages are basically a shared hosting account with extra tools to help you resell hosting space. Reseller hosting is a form of web hosting wherein the account owner has the ability to use his or her allotted hard drive space and bandwidth to host websites on behalf of third parties.

Cloud Hosting

Cloud hosting makes applications and websites accessible using cloud resources. Unlike traditional hosting, solutions are not deployed on a single server. Instead, a network of connected virtual and physical cloud servers hosts the application or website, ensuring greater flexibility and scalability.

Cloud hosting is the latest hosting type to hit the market, and it's become extremely popular in recent years. This type of hosting combines several clustered servers to provide your site services based on individual needs. Cloud-based web hosting is easy to use and quite affordable. It allows you to create more servers when your site gets busy and reduce in case of a reduction in the traffic. Most of the Cloud-Based Web Hosting plans will have a simple form of the pay-for-what-you-use pricing structure. It will be very effective and the user can pay only for the resource they used.

Website Maintenance

Our website is the foundation of our business's online presence. People visit it to **learn about our company**, **find our contact information**, and **purchase our products**. If our website isn't working properly or is out of date, we may lose out on significant opportunities, such as **new customers and sales**. Regular website maintenance helps prevent these issues.

Website maintenance refers to the tasks required to keep our website functioning properly and up to date. It involves regularly **checking our website for issues**, **correcting any issues**, and **making updates**. Website maintenance is also required to **maintain the value of the website** over time.

A website maintenance plan is an ongoing premium service to keep the website up-to-date. This usually includes the website's WordPress core, plugins, and themes. Plans can also include other services. For example, the website will also need to be **tested and improved**. Many maintenance plans include **backups** and site **monitoring**.

Website maintenance costs may vary depending on the type of site. Here are a few examples of potential website maintenance costs for various types of websites:

- **Personal website** will have low maintenance costs, typically from INR300 to INR1800 per month
- **Small business** website maintenance may cost up to INR7000 per month
- A corporate website may have maintenance costs of INR14,000 to INR2.5Lack
- **Ecommerce website** maintenance costs may range from INR1Lack to INR2Lack

Website maintenance includes

- Testing your whole website annually
- Testing browser compatibility
- Testing your forms and checkout process quarterly
- Checking for software updates monthly
- Backing up your website
- Reviewing key metrics weekly

Importance of website maintenance

Here are some of the top reasons.

1. The majority of customers conduct online research

Before making a purchase online, most of people conduct online research. People that are considering buying a product from you will likely end up on your website.

If your website gives them a negative impression of your company, they'll likely continue their research on a competitor's site, and you could miss out on a sale.

2. Your website informs users' first impressions

If your website doesn't work properly or looks outdated, customers will often click away. It will set a negative first impression of your business. If your website looks unprofessional, customers may think that your business is too.

3. Your website helps grow your sales

Your website plays an essential role in guiding users toward making a purchase. In the case of ecommerce sites, your site facilitates purchases. If your site doesn't work properly, you'll miss out on potential sales.

4. Site visitors value user experience

Among consumers who have a poor user experience on a site, most of them consumers will shop with a competitor instead. Regular maintenance prevents these poor user experiences and encourages potential customers to stay on your site, increasing your chances of making a sale.

5. A website maintenance plan improves security

Regular maintenance helps protect your site from cyber threats by keeping your security systems up to date. When you maintain your security protections, customers will feel more comfortable making purchases on your site.

6. Website maintenance supports your SEO strategy

If users frequently leave your website shortly after arriving on it, Google may view this as a sign that your site isn't relevant. This increase in bounce rate can lead to lower rankings in search results, which means you'll drive less traffic to your site.

Persistent technical issues, security issues, and outdated website design, structure, or content all contribute to diminishing your search engine rankings.

Additional website maintenance costs

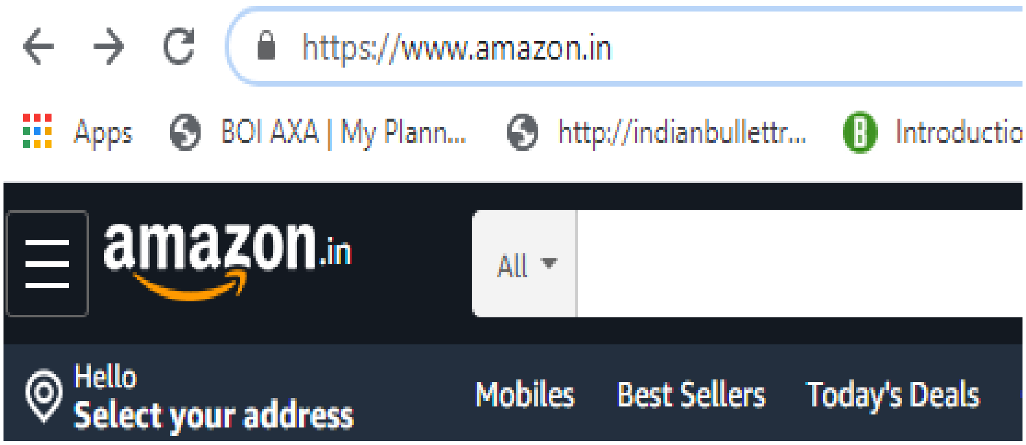
Some website maintenance costs to keep in mind include:

1. Domain name renewal

When you created your website, you purchased a domain name You might pay for your domain name on a monthly or yearly basis.

2. Secure Sockets Layer (SSL) certificate

You'll also want to ensure that your website has an SSL certificate, which helps keep your site secure. An SSL certificate enables your site to receive and transfer sensitive information securely.



Sites that have an active SSL certificate have HTTPS, instead of HTTP, in their URL. They also have a padlock image next to the URL in many browsers.

3. Website hosting

Website hosting is another website maintenance cost to consider.

- With a **shared host**, your website shares a server with several other websites. It's the least expensive option at **INR1,500 to INR8,000 per year**.
- If you choose a **virtual private server (VPS)**, you still share a server with other sites. However, the provider divides the server up into several VPSs, giving your site a dedicated amount of server space. VPSs cost **INR17,000 to INR40,000** per year.
- With a **dedicated server**, you get full access to your own server. This option costs between **INR90,000 to INR1.75Lack per year.**

Online Promotion tools & techniques

Creating your website is just the beginning. All the effort put into setting it up will go to waste if nobody sees it. So, we need to promote our website so that customers get to know about our business, products, and services.

Website promotion refers to marketing strategies that help increase the visibility of a site. It is a collection of online and offline marketing tactics and techniques that can be used to increase the visibility of a website so that people can find it. Such strategies are designed to bring targeted traffic (visitors who fit your target market) to your website, which is essential for a business.

Types of Website Promotion

Websites can be promoted both online and offline.

Online Website Promotion

Promotional techniques carried out over the internet include:

- **Search engine optimization**: SEO involves getting your website listed by search engines and ranked highly in search engine results. It includes designing a website with SEO friendly coding structure, making the website fast loading and secure, implementing the META tags on each page correctly, using well-optimized images with proper alt tags, making the design responsive, and adding an XML sitemap and so on.
- **Email marketing**: Email marketing requires getting permission from people interested in your business and sending them regular emails on timely topics (a product sale, for example), usually via an email list, to generate interest, customers, and sales.
- **Content marketing**: Content marketing involves creating blog posts on your blog or another firm's blog (known as "guest blogging"). The content can be the description of your product. The main purpose of a blog is to connect you to the relevant audience.
- **Social media marketing**: This involves creating profiles on major social media platforms and maintaining an active, useful presence by posting relevant, enticing text (a promotional contest conducted over Twitter, for example) or visual content (like Instagram photos and face book ad or YouTube videos).
- **Digital marketing**: Digital marketing typically refers to taking out paid or unpaid ads promoting your business website. Ads can take a number of forms, including ads on social media sites , banner ads for your website that appear at the top or sides of other websites, or paid search.
- **Podcasting**: Podcasts are audio files (mp3) available for streaming or downloads. You can host your own podcast or serve as a guest on another host's show and point listeners to your website.

Offline Web Promotion

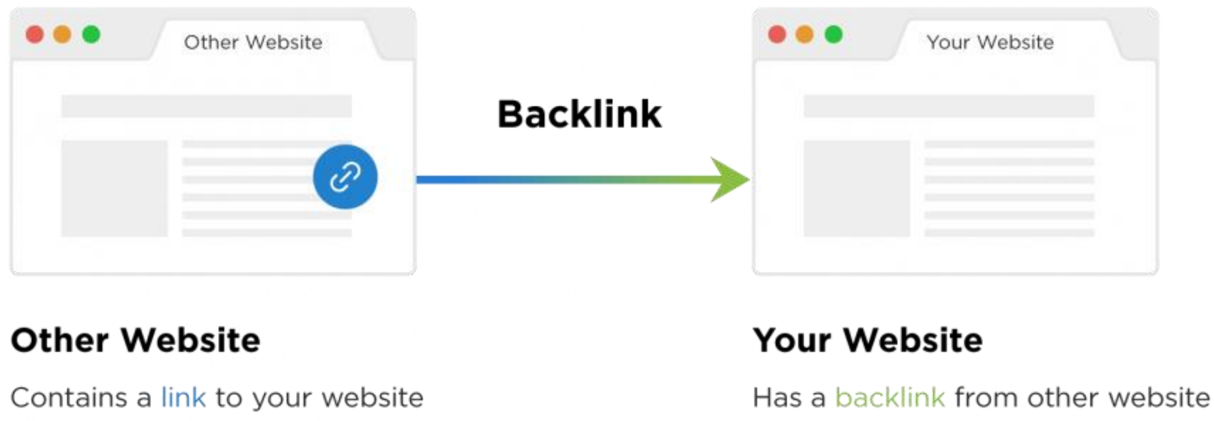
Promotional techniques that don't require the internet include:

- **Print advertising**: Run ads in newspapers or magazines. Ads in local newspapers are typically cheaper than those placed in national papers.

- **Television and radio advertising**: If you have the budget, pay to have an ad air on television or over the radio waves. Keep in mind that a television spot is generally more expensive than a radio spot and an ad on network television costs more than one on cable.
- **Press releases**: A press release is a document that highlights a business and its products and services. After you create one, submit it to newspapers or radio stations for publication. Ex-Sale announcement, coming soon announcement for new product etc.
- **Networking**: Share the URL of your business widely among your business and personal networks, either verbally or via a business card.
- **Article writing**: Write for magazines or other print publications, and you may be able to include a link to your website.
- **Trade shows**: These events are attended by industry professionals so present a great opportunity to talk about your business and distribute business cards containing your site URL.

Getting links to our site (Backlinking)

The web today is comprised of trillions of links. Who links to your site and how they link to it is the fundamental factor driving your search engine rank and your website traffic. Getting link to our side is known as backlinking. "Backlinks," meaning sites that link to your site.


Other Website
Backlink
Your Website
Other Website
Contains a link to your website
Your Website
Has a backlink from other website

Not all backlinks are created equal. In other words, if you want to rank higher in the SERPs, focus on **quality backlinks**. A single quality backlink can be more powerful than 1,000 low-quality backlinks.

1: They Come from Trusted, Authoritative Websites

The more authority a site has, the more authority it can pass on to your site (via a link).

2: They Include Your Target Keyword in the Link's Anchor Text

Anchor text is the visible text part of a link. In general, you want your links to have anchor text that includes your target keyword.

3: The Site (and Page) Linking to You Is Topically Related To Your Site

When a website links to another website, ensure that the two sites are related.

4: The Link Is a "Dofollow" Link

Google and other search engines ignore links with the "nofollow" tag attached to it. (In other words, nofollow links don't count search engine ranking algorithms).Fortunately, the vast majority of links on the web are "dofollow" links.

5: The Link Is From a Domain That Hasn't Linked to You Before

Links from the same website have diminishing returns. It's usually better to get 100 links from 100 different websites than 1,000 links from the same website.

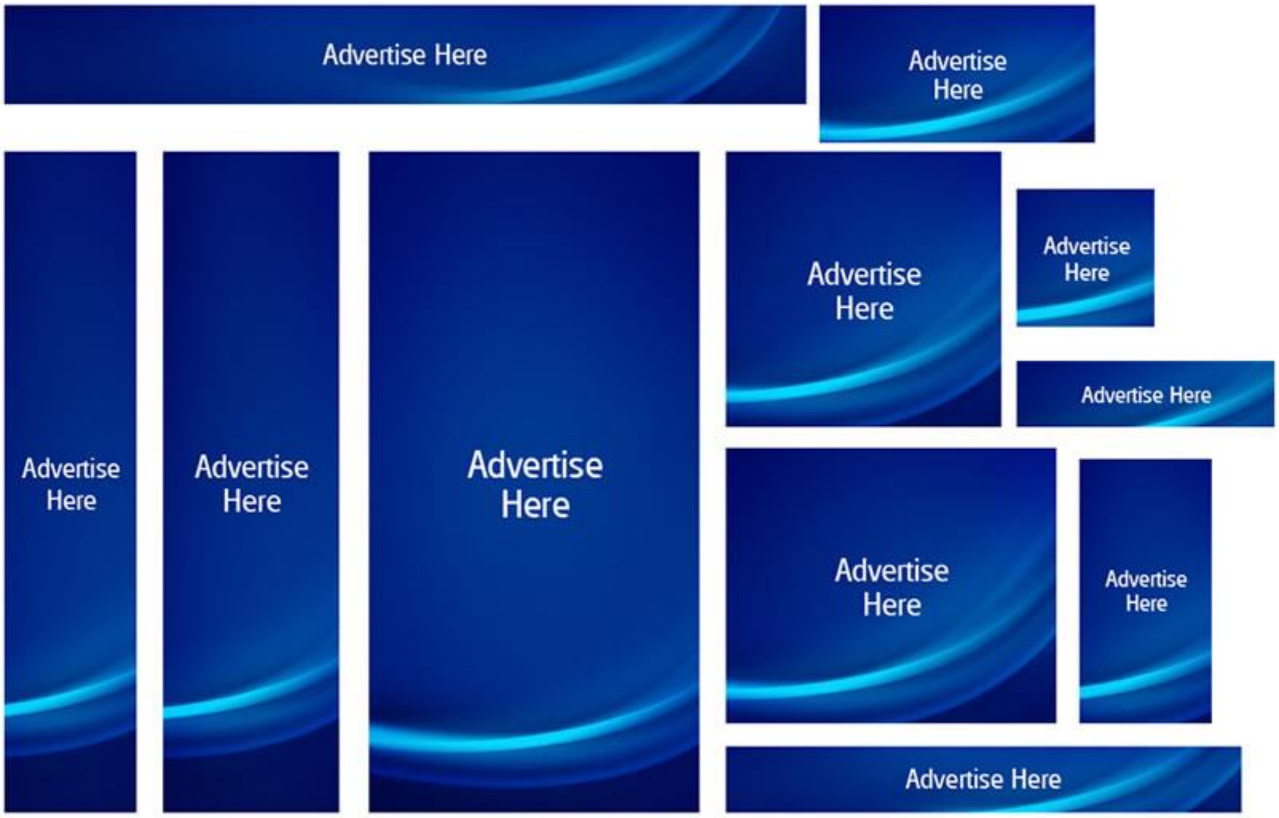
Banner Advertisement

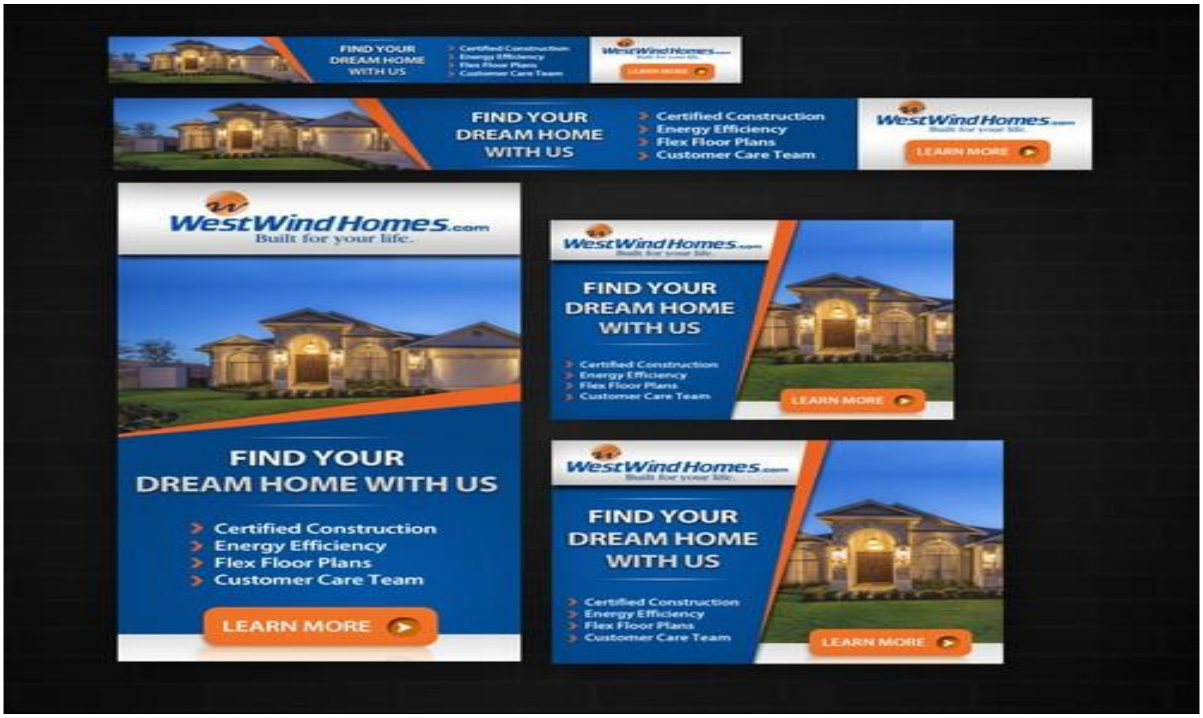
A banner ad, or a web banner, is **an advertisement displayed into a web page**. The first banner ad was launched in October 27 in 1994 on Wired Magazine.

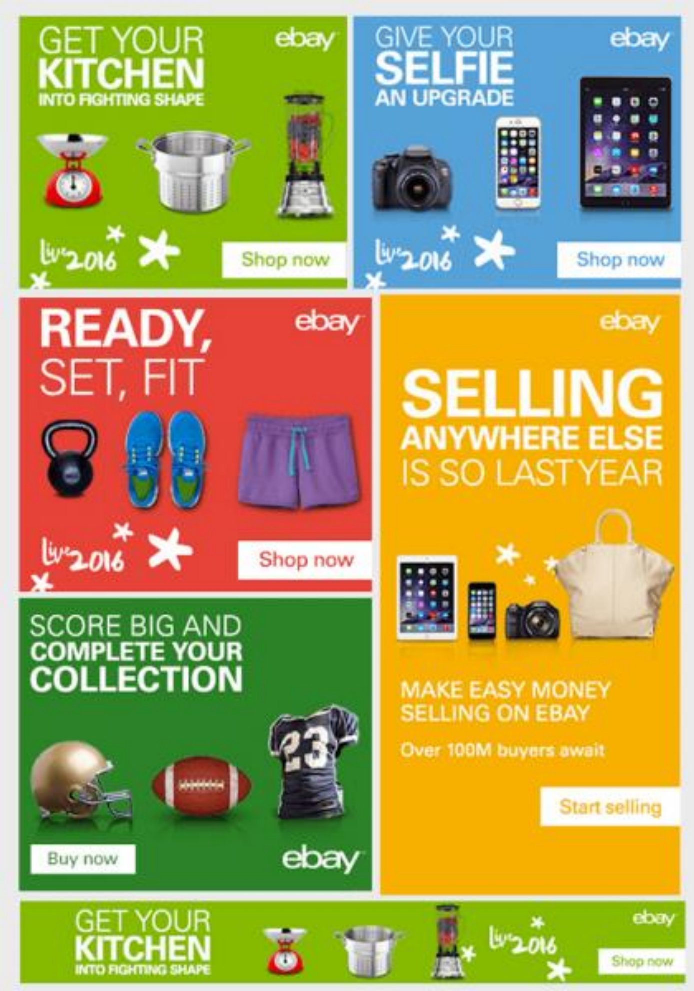
Banner ads are image-based rather than text-based and are a popular form of online advertising. The purpose of banner advertising is to promote a brand and/or to get visitors from the host website to go to the advertiser's website.

It is the use of a rectangular graphic display that stretches across the top, bottom, or sides of a website or online media property. The **horizontal type** of banner advertisement is called a leaderboard, while the **vertical banners** are called a skyscraper.

Standard Sizes Used for Banner Ads




FIND YOUR DREAM HOME WITH US
Certified Construction
Energy Efficiency
Flex Floor Plans
Customer Care Team
WestWindHomes.com
Built for your life.
LEARN MORE


GET YOUR KITCHEN INTO FIGHTING SHAPE
ebay
live 2016
Shop now
GIVE YOUR SELFIE AN UPGRADE
ebay
live 2016
Shop now
READY, SET, FIT
ebay
live 2016
Shop now
SELLING ANYWHERE ELSE IS SO LAST YEAR
ebay
MAKE EASY MONEY SELLING ON EBAY
Over 100M buyers await
Start selling
SCORE BIG AND COMPLETE YOUR COLLECTION
Buy now
ebay
GET YOUR KITCHEN INTO FIGHTING SHAPE
live 2016
ebay
Shop now

Advertisement Effectiveness:

1. Increasing customer traffic

The banner ad encourages the visitors to go on the advertiser’s website by clicking on it.

2. Sell a product

Banner ads encourage you to buy certain products.

3. Grab the customer’s attention

Capturing someone’s attention nowadays can be very challenging, especially in the digital environment. Banner ads are good option for this.

4. Announcing discounts and sales

Another way for businesses to generate and increase revenue is through sales and discounts.

Point To Remember When Creating Banner Advertisement

1. Who is your main target and what do you want from them.
2. Choose a Standard web banner ad size
3. Use readable fonts
4. Use high quality photos
5. Use your brand colors
6. Don’t overcrowd your banner ad
7. Don’t forget to use a branding element (logo, company name or website).

Web Traffic

Website traffic refers to web users who visit a website. Web traffic is measured in visits, sometimes called "sessions,”.

Just like traffic on a highway refers to the number of cars traveling down the road, web traffic is the number of web users who travel to any given website. Each person who logs on to a website is recorded as a **visit** or **session**, with a **starting** and **ending point**, thanks to behind-the-scenes communications between a user's device and the website itself.

Web traffic is specific to each page of your website as well, so whether you have a one-page site or a 50-page site, each of that page’s traffic is configured independently of all other pages.

Web traffic metrics can help us to develop a strategy to monitor our website traffic, and some of these metrics are:

- ***Total visits.*** Measuring the total number of visits to your website will give you with a bigger picture of how well your marketing campaign is driving traffic. You should expect the total number of visits to your site to increase progressively.
- ***New sessions.*** This metric is found within Google Analytics, and it tells you how many new visitors you have vs. the number of return visitors. This will tell you if your site is encouraging repeat customers.
- ***Bounce rate.*** This metric shows the amount of your visitors that leave your site before clicking onto any links or exploring it further.
- ***Total conversions.*** This is one of the most important measures to determine how profitability your marketing strategy is. You can measure conversions directly on your website or can use Google Analytics in order to track your progress. Low conversion numbers, poor offerings or a bad design could be the problems.

Need To Monitor Web Traffic

- We can monitor how effective our site is.
- We can figure out how long visitors are sticking around.
- We can see which pages are triggering visitors' interest.
- We can monitor the impact of our marketing efforts.
- We can determine where web traffic is coming from (such as social media sites).
- We can increase the efficiency of your site overall.

To measure the performance of a website, analysts look at website traffic: the total number of website visitors along with information on where they came from and how they got from there to the site.

These are the key terms in web traffic analytics:

- **Hits** — visitors' interactions on the website
- **Sessions** — collections of hits grouped by time and interaction logic
- **Users** — collections of sessions grouped on the basis of similarities in device, browser, system, and other parameters.

Web Log Files

Web log files are the text files which get generated whenever there is an **interaction** between **user** and the **web**. Each user interaction with web will be recorded as a single record in the web log file. Generally, web log file records contain fields such as IP address, URL accessed, time stamp, number of bytes, method used for making request and protocol details.

These web log files can be used to understand or study the web user behavior. The data which is stored in web log files will be consisting of huge amount.

A sample web log record is shown below,

123.46.7.79.8 - [18/Mar/2020:04:06:50 -0500] ―GET/HTTP/1.0‖ 200 3240

Where,

- 123.46.7.79.8- IP address
- "-"(hyphen) indicates Anonymous user id
- 18/Mar/2020:04:06:50- Web page access time
- -0500- The time zone
- GET/HTTP- HTTP request method
- 200- HTTP status code
- 3240- Number of bytes transmitted

Every single time that you visit a page on a website, a line with this information is output, recorded, and stored by the server.

Aspects of a log file analysis

A log file analysis can show the following data about the users of a website:

- IP Address and host name
- Country or region of origin
- Browser and operating system used
- Direct access by the user or reference from another website or advertising measure
- Type of search engine and search term entered
- Duration and number of pages visited by the user
- Page on which the user has left the website again

Importance of log files analysis

For Tracking Your Site's/Platform's Visitors

For Production Monitoring and Debugging

For Resource Usage

For HTTP Errors

For Slow Queries

For Security

Log analysis tools

1. Loggly Loggly is a cloud-based logging management and analytics service provider founded in 2009. Their main focus is that log management needs to be much simpler and that DevOps, SysOps, and Engineers should not have to worry about log management.

2. GoAccess

GoAccess is designed to be a fast, terminal-based log analyzer. Its core idea is to quickly analyze and view web server statistics in real time without needing to use your browser. It is open source, and because of that, it is **completely free** to use.

3. logz.io

logz.io offers you real-time, actionable insights into your log analytics data with hosted ELK as a service. ELK is a simple but robust log analysis platform that costs a fraction of the price.

4. Graylog

Graylog is an open-source log management platform which allows you to search, analyze, and alert you across all your log files.

5. Splunk

Splunk is a big name in the log and application management space. They have been around since 2003 are no newcomers when it comes to analyzing and monitoring data. Splunk has both **free and paid plans**. Their free plan, Spunk light, allows you up to log up to 500 MB data per day.

6. Logmatic.io

Logmatic.io is a log analysis tool designed specifically to help improve software and business performance. The founders have more than 10 years experience in real-time and big data software.

7. Logstash

Logstash is a free open-source tool for managing events and logs. You can use it to collect logs, parse them, and store them for later use.

8. Sumo Logic

Sumo Logic focuses on machine learning for unified logs and metrics to uncover real-time insights into application needs and new customer opportunities. Sumo Logic has both **free and paid plans.**

9. Papertrail

Papertrail is more of a log management service, but they also offer some great features which make analyzing your logs fast. Papertrail has both **free and paid plans** starting at INR500 per month.

SEO Techniques to increase web traffic

Search engine optimization (SEO) is the art and science of getting pages to rank higher in search engines such as Google, Yahoo, Bing. Because search is one of the main ways in which users discover content online, ranking higher in search engines can lead to an increase in traffic to a website.

It is the process of optimizing our website or webpage so that a search engine likes to show it as a top result for searches of a certain keyword.

In its **simplest** form, **search engine optimization** is anything done to improve the ranking of a website on search engine results pages. It is the process of improving the quality and quantity of website traffic to a website or a web page from search engines.

Following are some techniques that are used to achieve high rank in search engine ranking:-

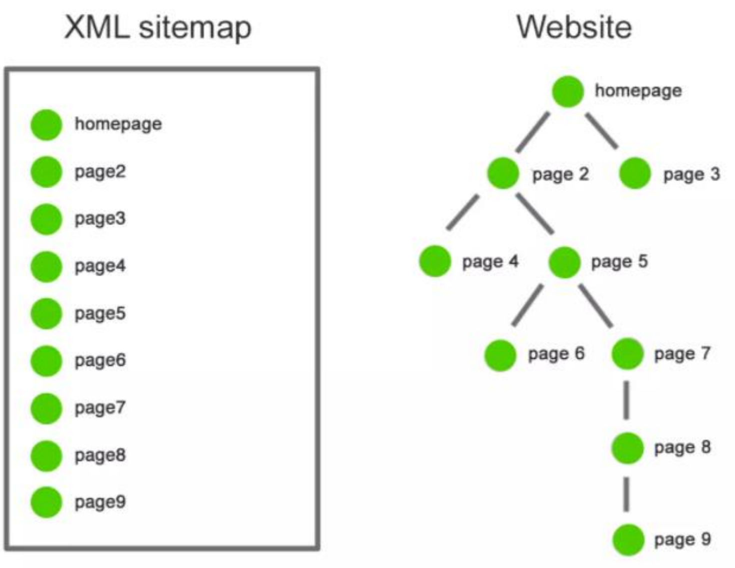
1. **Design a website with SEO friendly coding structure-** The better our site structure, the better our chance of ranking higher in the search engines. Every website has some “structure.” A good site structure means great user experience. Proper use of colors, fonts, kerning, graphics, images, and white space make good structure of website.
2. **Making the website fast loading and secure-** Having a fast-loading site is essential not just for ranking well, but also to keep our customers. If our site takes more than three seconds to load, we lose almost half of our visitors before they even arrive on our site. And if our site is not secure then we will lose our customer’s trust.
3. **Implement the META tags on each page correctly-** Meta tags are invisible tags that provide data about our page to search engines and website visitors. Meta tags

describe a page's content, meta tags don't appear on the page itself, but only in the page's source code.

4. **Use well-optimized images with proper alt tags-** Adding alt tags to photos is first and foremost a principle of web accessibility. While ALT tags need to be descriptive, they also need to be brief. They should not be full sentences or paragraphs.

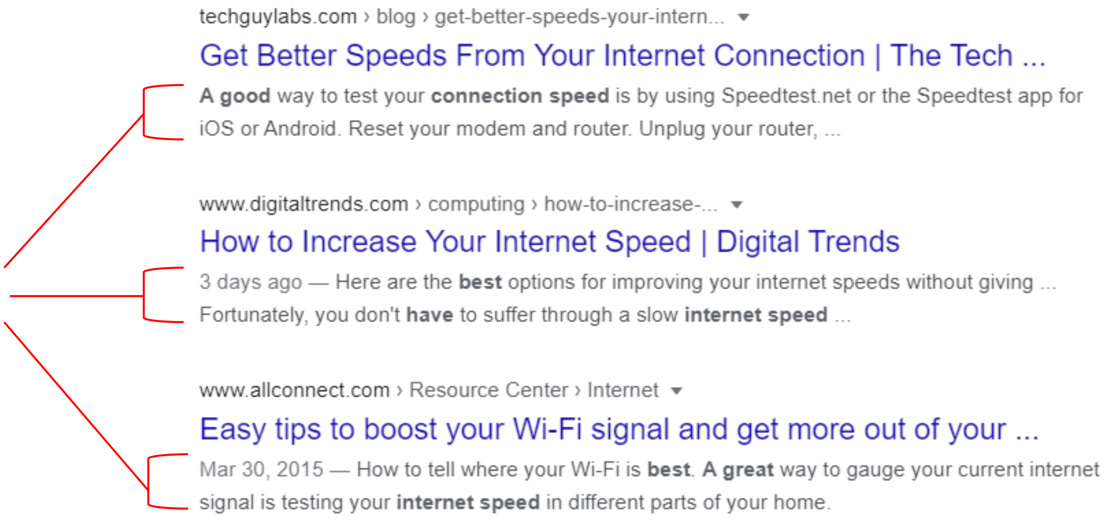
<img src="barbiedoll.png" alt="barbiedoll">

5. **Responsive web design –** Responsive web design (RWD) is a web development approach that creates **dynamic changes** to the appearance of a website, **depending on the screen size and orientation** of the device being used to view it. RWD is one approach to the problem of designing for the multitude of devices available to customers, ranging from tiny phones to huge desktop monitors.
6. **Add an XML sitemap-** In simple terms, an XML sitemap is a list of your website's URLs. It acts as a roadmap to tell search engines what content is available and how to reach it. An XML sitemap lists all important pages of a website.



7. **Keyword research**- Keyword research in SEO is as important as oxygen in human living. Keyword research means to research & choose words / terms that users will search in search engines for finding their queries. Research your more than 100 keywords, group them and plan content.

8. **Write appealing catchy lines in description**- The description is the short paragraph of text placed in the HTML of a webpage that describes its content. The description will then appear under your page's URL in the search results.



techguylabs.com › blog › get-better-speeds-your-intern... ▾

Get Better Speeds From Your Internet Connection | The Tech ...

A good way to test your **connection speed** is by using Speedtest.net or the Speedtest app for iOS or Android. Reset your modem and router. Unplug your router, ...

www.digitaltrends.com › computing › how-to-increase-... ▾

How to Increase Your Internet Speed | Digital Trends

3 days ago — Here are the **best** options for improving your internet speeds without giving ... Fortunately, you don't **have** to suffer through a slow **internet speed** ...

www.allconnect.com › Resource Center › Internet ▾

Easy tips to boost your Wi-Fi signal and get more out of your ...

Mar 30, 2015 — How to tell where your Wi-Fi is **best**. **A great** way to gauge your current internet signal is testing your **internet speed** in different parts of your home.

9. **Headings and Subheading (H1, H2, H3…)**- Headings help users and search engines to read and understand text. Headings also define which parts of your content are important, and show how they're interconnected.

Except above technologies, we also should think about some other technologies to get high rank in search engine: -

- Create supporting visual content like videos, images.
- Website Architecture, internal links, content hubs
- Optimize for Voice Search
- Design for Mobile First
- Create a Diverse Backlink Portfolio
- Improve User Experience Across Your Entire Site
- Regularly update your old content

Online payment

Online payment refers to money that is exchanged electronically. An online payment system is an Internet-based method of processing monetary transactions. It allows a vendor to accept payments over the web or over other Internet connections. Online payment systems greatly expand the reach of a business and its ability to make sales.

Online payment systems typically are run by third-party corporations, such as PayPal, Stripe, PayU, PayTM, GooglePay or Click2Pay. These companies make a profit by taking a small percentage of every transaction, or by signing contracts with institutions that need to make a large number of transactions.

Payment Gateways for online payment

A payment gateway is the simplest way for a business to collect digital or online payments from their website or app. Paying online is a fundamental feature that every e-commerce platform in the world offers. And they can provide this facility by integrating with a payment gateway. Online payments are swift and convenient. They allow you to buy products and services from all over the world.

An online payment gateway (PG) is a tunnel that connects your bank account to the platform where you need to transfer your money. A PG is software that authorizes you to conduct an online transaction through different payment modes like net banking, credit card, debit card, UPI or the many online wallets that are available these days. It plays the role of a third party that securely transfers your money from the bank account to the merchant’s payment portal.

- A payment gateway focuses on securing the sensitive information given by the user throughout the process.
- It ensures security by encrypting data like card and bank details that have been provided by the user.

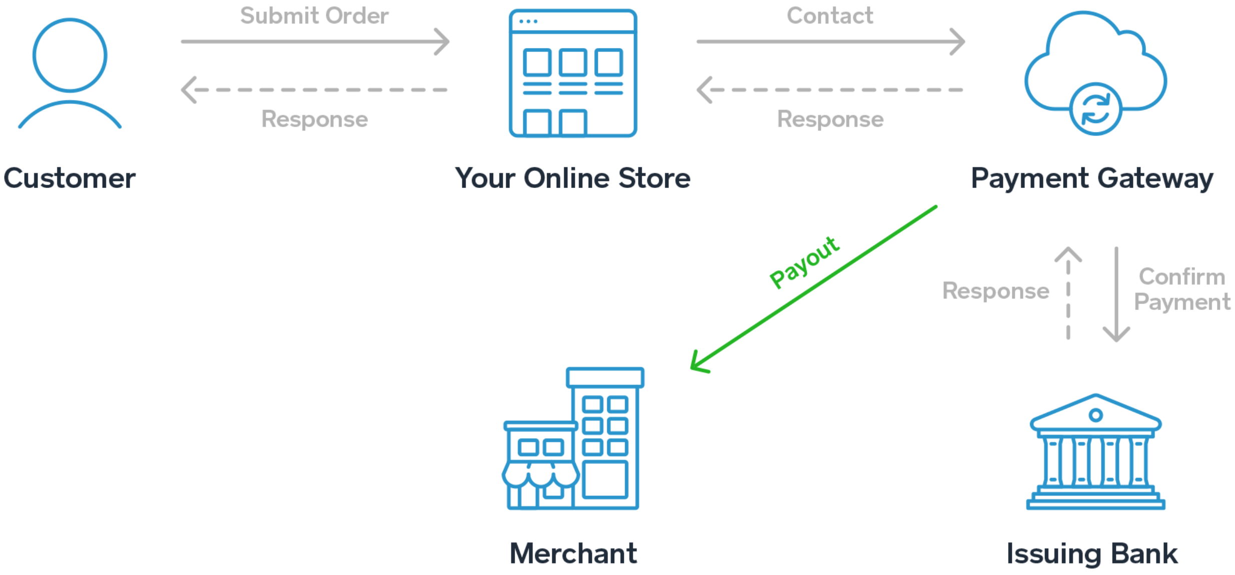
In simple steps, a payment gateway:

1. **Captures** the credit card transaction
2. **Encrypts** the transaction information
3. **Routes** it to the credit card processor and then
4. **Returns** either an approval or a decline notice.

The following are the basic steps showing how a typical payment gateway works.

Step 1: A customer places his or her order and then presses the Submit or Checkout button, or its equivalent button, on the website.

Step 2: Once this happens, the website or the e-commerce platform takes the customer to a payment gateway where he or she enters all the relevant information about the bank or the card they are using to pay. The PG then takes the user directly to the page of the issuing bank or a 3D secure page, asking for the transaction to be authorized.



Step 3: Once the payment gateway gets the approval for the transaction, the bank then checks whether the customer has sufficient balance in the account to make this transaction a success or not.

Step 4: The payment gateway sends a message to the merchant accordingly. If the reply from the bank is a “No’”, then the merchant subsequently sends an error message to the customer, telling them about the issue with the card or the bank account. If the response is a “Yes” from the bank portal, then the merchant seeks the transaction from the bank.

Step 5: The bank settles the money with the payment gateway, which in turn settles the money with the merchant.

Once this process is completed, the customer gets a confirmation message of the order being placed.

Security of Transactions on Web

Shopping and banking online occur constantly in the Internet marketplace. Unfortunately, online fraud and identify theft occurs just as frequently. Ecommerce security refers to the measures taken to protect your business and your customers against cyber threats.

Measures to ensure Security

Major security measures are following −

- **Encryption** − It is a very effective and practical way to safeguard the data being transmitted over the network. Sender of the information encrypts the data using a secret code and only the specified receiver can decrypt the data using the same or a different secret code.
- **Digital Signature** − Digital signature ensures the authenticity of the information. A digital signature is an e-signature authenticated through encryption and password.
- **Security Certificates** − Security certificate is a unique digital id used to verify the identity of an individual website or user.

Some terminologies for security on web are as follows:

1. TLS Encryption(Transport Layer Security) and SSL (Secure Sockets Layer)

Data security on e-commerce websites or an online payment system begins the moment a user lands on the site. The TLS Certificate tells users that the data transmitted between the web server and their browser is safe.

Without TLS Encryption in place, all data sent over the Internet is unencrypted and is visible to anyone with the means and intent to intercept it.

2. PCI-DSS Compliance (Payment Card Industry Data Security Standard)

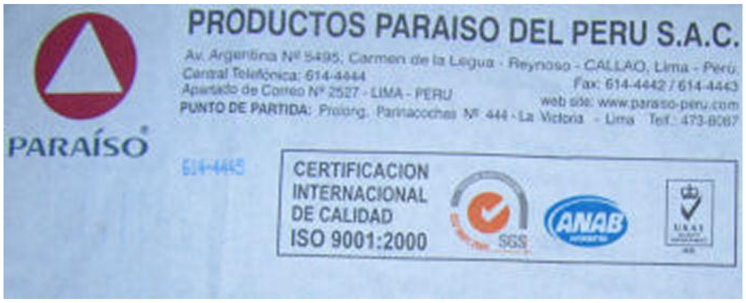
The PCI Security Standards Council is a global organization that maintains and promotes compliance rules for managing cardholder data for all e-commerce websites and online payment systems.

For an e-commerce website or an online payment system to be PCI-DSS compliant they have to follow certain directives:

- ***Maintain a secure network to process payments*** (This involves using robust firewalls which can protect against malicious security threats.)
- ***Ensure all data is encrypted during transmission*** (When cardholder data is transmitted online, it is imperative that it be encrypted. Almost all payment gateways encrypts all information you share using checkout via TLS (Transport Layer Security))
- ***Keep infrastructure secure*** (This directive involves keeping abreast of new PCI-DSS mandates and using updated software and spyware to protection)
- ***Restrict information access*** (An important part of securing online payments on e-commerce websites is restricting access to confidential information so that only authorized personnel will have access to cardholder data. Cardholder data must be protected at all times – both electronically and physically.)

3. International Organization for Standardization (ISO)

ISO certification certifies that a management system, manufacturing process, service, or documentation procedure has all the requirements for standardization and quality assurance. ISO is an independent, non-governmental, international organization that develops standards to


PARAÍSO®
SGS
ANAB
UKAS

PRODUCTOS PARAISO DEL PERU S.A.C.
Av. Argentina Nº 5495, Carmen de la Legua - Reynoso - CALLAO, Lima - Perú
Central Telefónica: 614-4444
Fax: 614-4442 / 614-4443
Apartado de Correo Nº 2527 - LIMA - PERU
web site: www.paraiso-peru.com
PUNTO DE PARTIDA: Prolong. Parinacochas Nº 444 - La Victoria - Lima Telf.: 473-8087

614-4445

CERTIFICACION
INTERNACIONAL
DE CALIDAD
ISO 9001:2000

ensure the quality, safety, and efficiency of products, services, and systems. Achieving this certification means a business has high quality management systems, data security, risk-aversion strategies, and standardized business practices.

4. Tokenization

Tokenization is a process by which a 16-digit card number gets replaced by a digital identifier known as a 'token'. This is done to ensure the safety of the original data while allowing payment gateways to securely access the cardholder data and initiate a secure payment.

5. Two-Factor Authentication

Two Factor Authentication, or 2FA, or two-step verification is an extra layer of security added by e-commerce websites to ensure a secure payment for a customer.

Many banks and other e-payment gateways also use the 2FA for their own payment modes. When you use Net Banking for a transaction, you are first asked to enter your username and password. As a final confirmation, the bank sends you an OTP on your registered mobile number. This process is divided into two levels of authentication:

- **What the user knows:** In this step, users fill in their card/Net Banking details such as username and password. This helps the payment gateway recognize which bank the card belongs to.
- **What the user (and only the user) has:** This step is known as '**Authorization**'and is done through the OTP/PIN/CVV. The bank (and the payment gateway) can then confirm that the request for payment is initiated by the rightful user.

6. Fraud Prevention

Apart from these mandatory protocols, most e-commerce websites and payment gateways have their own fraud and risk prevention systems.

7. Deal with reputed websites only

Do not directly pay to any website unless you know about it. The advanced security features used in payment processor such as PayTabs will prevent your financial information from getting into wrong hands.

8. <u>Do not use public computers</u>

In order to maintain security during online transactions, make sure that you’re using your own computer or mobile device. Do not use the computers installed at public libraries or internet cafes, as these computers can easily be manipulated by tweaking its hardware or software.

9. <u>Set a strong and complex password</u>

Don’t use common passwords or the password that can easily be guessed. Use a combination of alphanumeric and special characters and make sure the password length is more than 6 digits.

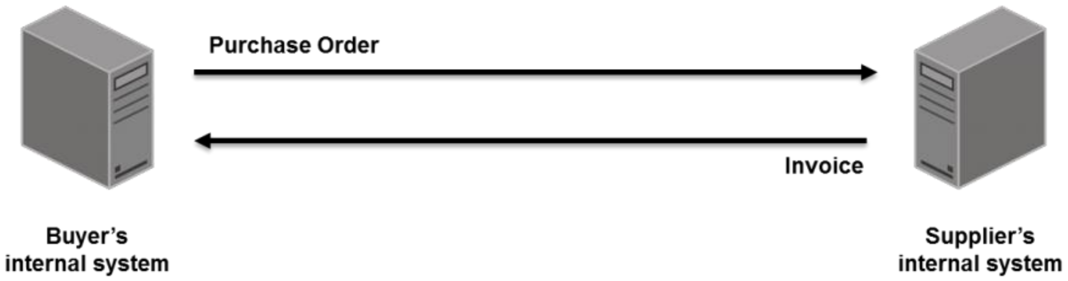
Fundamental of E-Commerce

Unit-3

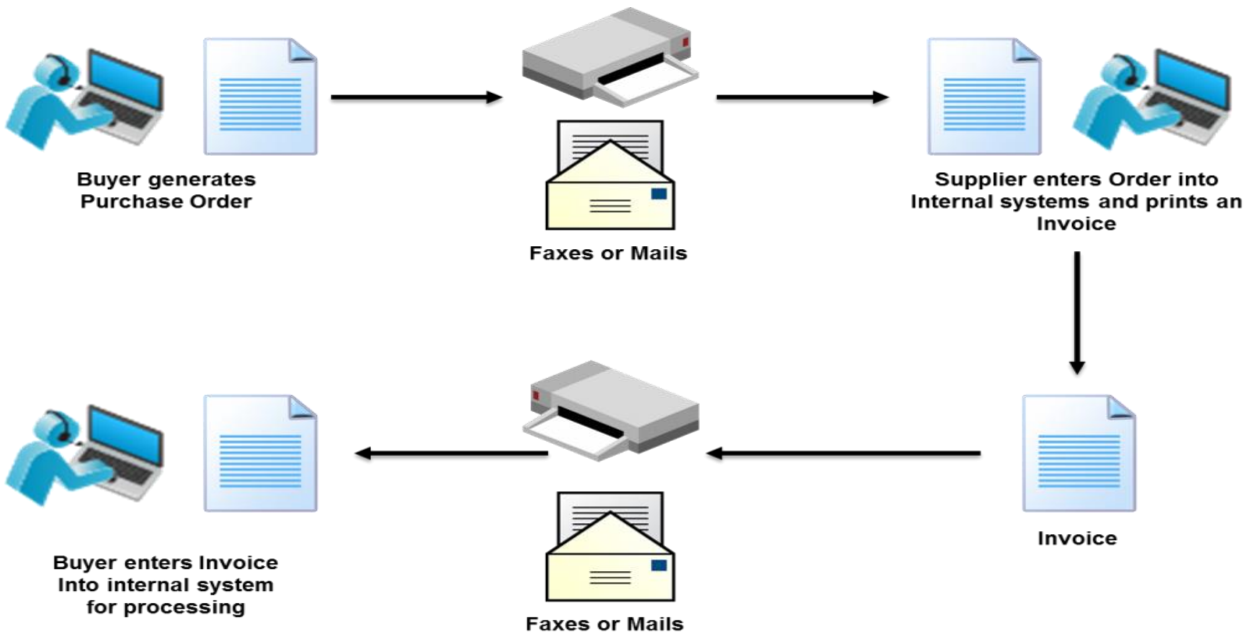
Electronic Data Interchange (EDI)

EDI stands for Electronic Data Interchange. EDI is an electronic way of transferring business documents in an organization internally, between its various departments or externally with suppliers, customers, or any subsidiaries. In EDI, paper documents are replaced with electronic documents such as word documents, spreadsheets, etc.

The EDI process looks like this — no paper, no people involved:



A typical manual process looks like this, with lots of paper and people involvement:


Buyer generates Purchase Order
Faxes or Mails
Supplier enters Order into Internal systems and prints an Invoice
Invoice
Faxes or Mails
Buyer enters Invoice Into internal system for processing

Electronic Data Interchange (EDI) is the automated, computer-to-computer exchange of standard electronic business documents between business partners over a secure, standardized connection. Each term in the definition is significant:

- **Computer-to-computer**– EDI replaces postal mail, fax and email. While email is also an electronic approach, the documents exchanged via email must still be handled by people rather than computers.

  Having people involved slows down the processing of the documents and also introduces errors. Instead, EDI documents can flow straight through to the appropriate application on the receiver’s computer (e.g., the Order Management System) and processing can begin immediately.
- **Business documents** – These are any of the documents that are typically exchanged between businesses. The most common documents exchanged via EDI are purchase orders, invoices and advance ship notices. But there are many, many others such as bill of lading, customs documents, inventory documents, shipping status documents and payment documents.
- **Standard format**– Because EDI documents must be processed by computers rather than humans, a standard format must be used so that the computer will be able to read and understand the documents. A standard format describes what each piece of information is and in what format (e.g., integer, decimal, mmddyy). Without a standard format, each company would send documents using its company-specific format and, much as an English-speaking person probably doesn’t understand Japanese, the receiver’s computer system doesn’t understand the company-specific format of the sender’s format.

  Standard EDI Format

  - EDI documents are processed by computers and use standard, computer-friendly formats.
  - Standards describe each piece of data and its format (e.g., type of document, parties involved, actions to take, mmddyy etc.).
  - Standards eliminate company-to-company variations, allowing each business partner's computer system to speak a common language.
  - There are a variety of EDI standards for various industries, regions and use cases - each with different versions, so EDI partners must use the same standard and version
  - Popular standards include: ANSI X12 in the U.S., UN/EDIFACT globally and industry-specific standards, such as HIPAA

- **Business partners** – The exchange of EDI documents is typically between two different companies, referred to as business partners or trading partners. For example, Company A may buy goods from Company B. Company A sends orders to Company B. Company A and Company B are business partners.

A Traditional Document Exchange of a Purchase Order	**An EDI Document Exchange of a Purchase Order**
This process normally takes between three and five days.	This process normally occurs overnight and can take less than an hour.
Buyer makes a buying decision, creates the purchase order and prints it. Buyer mails the purchase order to the supplier. Supplier receives the purchase order and enters it into the order entry system. Buyer calls supplier to determine if purchase order has been received, or supplier mails buyer an acknowledgment of the order.	Buyer makes a buying decision, creates the purchase order but does not print it. EDI software creates an electronic version of the purchase order and transmits it automatically to the supplier. Supplier's order entry system receives the purchase order and updates the system immediately on receipt. Supplier's order entry system creates an acknowledgment and transmits it back to confirm receipt.

EDI Documents

Following are the few important documents used in EDI −

- Invoices
- Purchase orders
- Shipping Requests
- Acknowledgement
- Business Correspondence letters
- Financial information letters

Steps in an EDI System

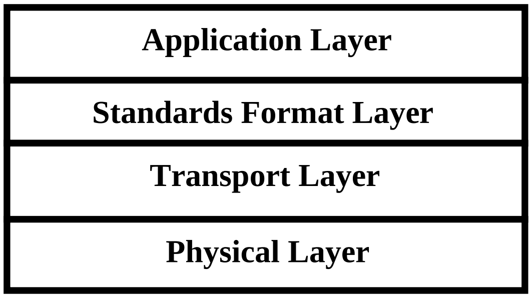
Following are the steps in an EDI System.

- A program generates a file that contains the processed document.
- The document is converted into an agreed standard format.
- The file containing the document is sent electronically on the network.
- The trading partner receives the file.
- An acknowledgement document is generated and sent to the originating organization.

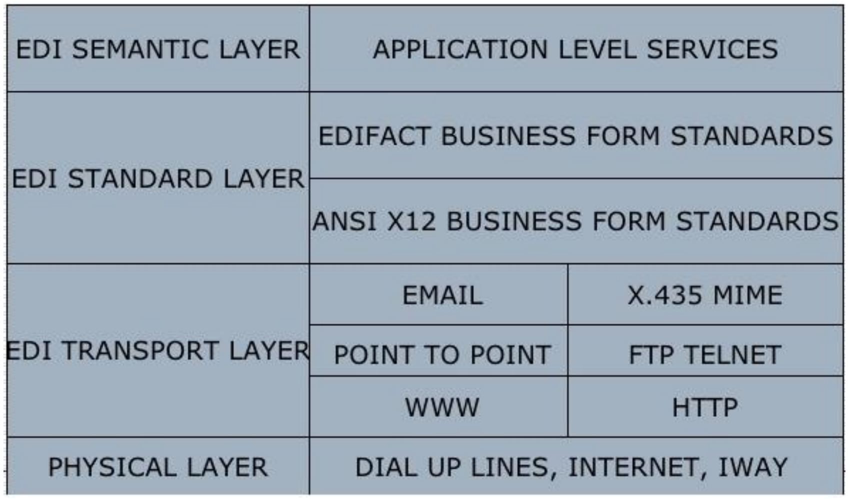
EDI layered Architecture

The architecture of EDI is divided into four layers-

1. EDI Semantic (Application) Layer
2. EDI Standards Format Layer
3. EDI Transport Layer
4. EDI Physical Network Infrastructure Layer



EDI layered Architecture



EDI SEMANTIC LAYER	APPLICATION LEVEL SERVICES	
EDI STANDARD LAYER	EDIFACT BUSINESS FORM STANDARDS	
	ANSI X12 BUSINESS FORM STANDARDS	
EDI TRANSPORT LAYER	EMAIL	X.435 MIME
	POINT TO POINT	FTP TELNET
	WWW	HTTP
PHYSICAL LAYER	DIAL UP LINES, INTERNET, IWAY	

1. **Application Layer-** The first layer of EDI defines the business applications that are used by EDI. This layer of EDI translates business application into request for quotes, purchase orders, acknowledgement and invoices. For every company this layer is specific and also for the software that company uses i.e. the user interface and content visible on the screen. The application layer also called the semantic layer.

By the semantic layer of the EDI the companies form are change into more specific format and then it may be send to various partners of the company have a several software applications to handle all forms aspects. To achieve all above activities the company must follow the EDI standard as X12, ANSI, EDIFACT etc. If the sender and receivers of company want to exchange some files then requires a compatible standards of Electronic Data Interchange. The Sender who want to send a data use a software application with EDI and exchange data in EDI format so that at the receivers end the receiver can read it. The EDI standards are very important in exchange of data because at sending end a sender manipulate data by EDI as in receiving end data is manipulated by EDI.

2. **Standard Layer-** This layer of EDI architecture defines the structures of the business form and some content which are related with the application layer. This layer of EDI has no mean without application layer so we can say that EDI applications and standard layer are interlinked. Over a period of time, two major EDI standards have evolved. The first, commonly known as X12, was developed by Accredited Standards X12 committee of American National Standards Institute (ANSI) and The second, the International Standard was developed by United Nations EDI for Administration, Commerce and Trade (EDIFACT) standard.
3. **Transport Layer-** EDI transport layer is a non electronic way of sending the business form from one company to another company. This non electronic way may be registered mail, postal services or private career, telecommunications, fax etc. Now-a-days the transportation method is more complex with compare to e-mail.
4. **Physical Layer-** The physical layer of EDI also called the infrastructure layer. It refers to the network infrastructure that is used for the exchange of information between trading partners. In the simplest and most basic form it may consist of dial-up lines, where trading partners dial-up through modem to each other and connect to exchange the messages.

Benefits of EDI

Following are the advantages of having an EDI system.

Minimal paper usage

EDI reduces associated expenses of storage, printing, postage, mailing and recycling

Enhanced quality of data

EDI minimizes data entry errors, improves accounts payable/receivable times as processes become streamlined and can be used for forecasting

Improved turnaround times

Your business cycle is improved and stock levels are kept constantly up to date and visible

Improved timelines

EDI transfer ensures real-time processing and eliminates times associated with manually sending, receiving and entering orders

Costs saving in operational efficiency

EDI reduces the time it takes your staff to manually create invoices and process purchase orders

Reduction in data entry errors − Chances of errors are much less while using a computer for data entry.

Electronic form of data − It is quite easy to transfer or share the data, as it is present in electronic format.

Standard Means of communication − EDI enforces standards on the content of data and its format which leads to clearer communication.

Helps create a greener world

EDI eliminates paper trails and ensures paper usage is kept to a minimum

E-payment system

An e-payment system is a way of making transactions or paying for goods and services through an electronic medium, without the use of checks or cash. It’s also called an electronic payment system or online payment system.

The electronic payment system has grown increasingly over the last decades due to the growing spread of internet-based banking and shopping. As the world advances more with technology development, we can see the rise of electronic payment systems and payment processing devices. With the rapid development of the computer, mobile, and network technology, e-commerce has become a routine part of human life. In e-commerce, the customer can order products at home and save time for doing other things. There is no need of visiting a store or a shop. The customer can select different stores on the Internet in a very short time and compare the products with different characteristics such as price, color, and quality.

The electronic payment systems have a very important role in e-commerce. E-commerce organizations use electronic payment systems that refer to paperless monetary transactions. It revolutionized the business processing by reducing paperwork, transaction costs, and labor cost. E-commerce processing is user-friendly and less time consuming than manual processing. Electronic commerce helps a business organization expand its market reach expansion.

Electronic Payment Methods

E-Commerce sites use electronic payment where electronic payment refers to paperless monetary transactions. Electronic payment has revolutionized the business processing by reducing paper work, transaction costs, labour cost. Being user friendly and less time consuming than manual processing, it helps business organization to expand its market reach / expansion. Some of the modes of electronic payments are following.

1. Credit Card
2. Debit Card
3. Smart Card
4. E-Money
5. Electronic Fund Transfer (EFT)

1. Credit Card:

Payment using credit card is one of most common mode of electronic payment. Credit card is small plastic card with a unique number attached with an account. It has also a magnetic strip embedded in it which is used to read credit card via card readers. When a customer purchases a product via credit card, credit card issuer bank pays on behalf of the customer and customer has a certain time period after which he/she can pay the credit card bill. It is usually credit card monthly payment cycle. Following are the actors in the credit card system.

The card holder - Customer

The merchant - seller of products who accepts credit card payments.

The card issuer bank - card holder's bank

The acquirer bank - the merchant's bank

The card brand - for example, visa or mastercard.

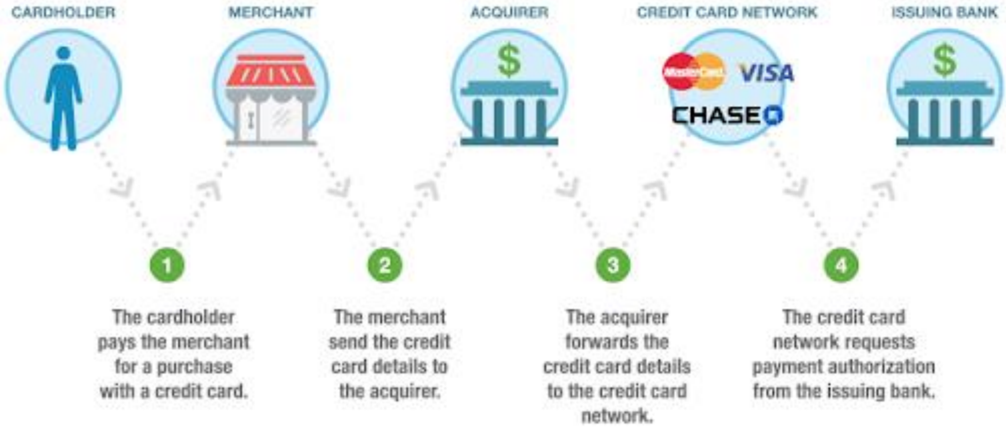

CARDHOLDER
MERCHANT
ACQUIRER
CREDIT CARD NETWORK
ISSUING BANK
MasterCard
VISA
CHASE
1
The cardholder pays the merchant for a purchase with a credit card.
2
The merchant send the credit card details to the acquirer.
3
The acquirer forwards the credit card details to the credit card network.
4
The credit card network requests payment authorization from the issuing bank.

Fig- Credit card payment process

Credit card payment process

Step Description

Step 1 Bank issues and activates a credit card to customer on his/her request.

Step 2 Customer presents credit card information to merchant site or to merchant from whom he/she want to purchase a product/service.

Step 3 Merchant validates customer's identity by asking for approval from card brand company.

Step 4 Card brand company authenticates the credit card and paid the transaction by credit. Merchant keeps the sales slip.

Step 5 Merchant submits the sales slip to acquirer banks and gets the service chargers paid to him/her.

Step 6 Acquirer bank requests the card brand company to clear the credit amount and gets the payment.

Step 7 Now card brand company asks to clear amount from the issuer bank and amount gets transferred to card brand company.

2. Debit Card:

Debit card, like credit card is a small plastic card with a unique number mapped with the bank account number. It is required to have a bank account before getting a debit card from the bank. The major difference between debit card and credit card is that in case of payment through debit card, amount gets deducted from card's bank account immediately and there should be sufficient balance in bank account for the transaction to get completed. Where as in case of credit card there is no such compulsion.

Debit cards free customer to carry cash, cheques and even merchants accepts debit card more readily. Having restriction on amount being in bank account also helps customer to keep a check on his/her spending.

3. Smart Card:

Smart card is again similar to credit card and debit card in appearance but it has a small microprocessor chip embedded in it. It has the capacity to store customer work related/personal information. Smart card is also used to store money which is reduced as per usage.

Smart card can be accessed only using a PIN of customer. Smart cards are secure as they stores information in encrypted format and are less expensive/provide faster processing. Mondex and Visa Cash cards are examples of smart cards.

4. E-Money:

E-Money transactions refer to situation where payment is done over the network and amount gets transferred from one financial body to another financial body without any involvement of a middleman. E-money transactions are faster, convenient and save a lot of time.

Online payments done via credit card, debit card or smart card are examples of e-money transactions. Another popular example is e-cash. In case of e-cash, both customer and merchant both have to sign up with the bank or company issuing e-cash.

E-cash

E-cash is a paperless cash system which facilitates the transfer of funds anonymously. E-cash is free to the user while the sellers have paid a fee for this. The e-cash fund can be either stored on a card itself or in an account which is associated with the card. The most common examples of e-cash system are transit card, PayPal, GooglePay, Paytm, etc.

E-cash has four major components-

- Issuers - They can be banks or a non-bank institution.
- Customers - They are the users who spend the e-cash.
- Merchants or Traders - They are the vendors who receive e-cash.
- Regulators - They are related to authorities or state tax agencies.

5. Electronic Fund Transfer:

It is a very popular electronic payment method to transfer money from one bank account to another bank account. Accounts can be in same bank or different bank. Fund transfer can be done using ATM (Automated Teller Machine) or using computer.

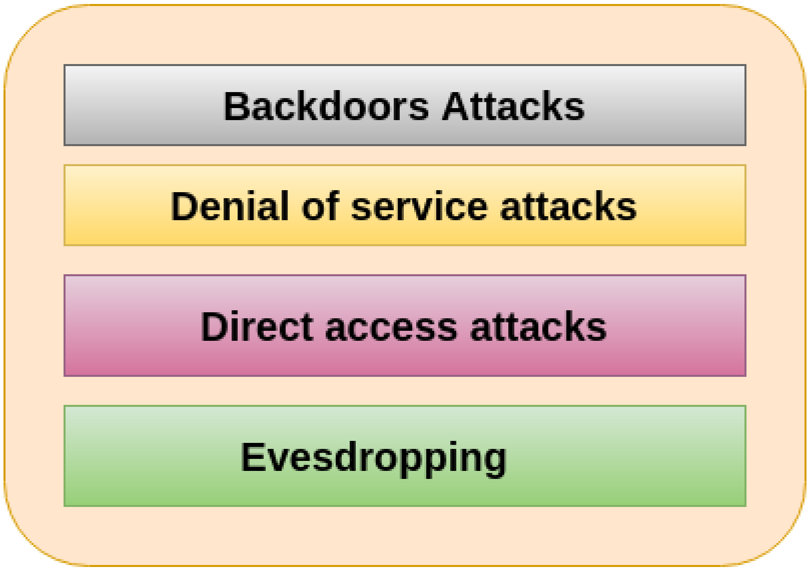
Now a day, internet based EFT is getting popularity. In this case, customer uses website provided by the bank. Customer logins to the bank's website and registers another bank account. He/she then places a request to transfer certain amount to that account. Customer's bank transfers amount to other account if it is in same bank otherwise transfer request is forwarded to ACH (Automated Clearing House) to transfer amount to other account and amount is deducted from customer's account. Once amount is transferred to other account, customer is notified of the fund transfer by the bank.

Difference between Credit card and Debit Card

Parameters	Debit Card	Credit Card
Definition	Deducts money directly from your saving's bank account or your current account.	Allows you to borrow funds to pay for goods and services.
Source of funds	Your savings bank account or current account.	Credit extended to you by your card issuer. It gives you access to money you otherwise do not have (like a very short-term loan).
Spending advantage	You can only spend how much you have.	Can spend more than what you have.
Who pays for the purchase	You pay for your purchase.	The credit card company pays the vendor for your purchase. You pay the credit card company.
Bill	There is no bill or statement	You get a bill or statement each month with details of the transactions you have made.
Payment	There is no payment that needs to be made since you are using your own money.	A bill needs to be paid each month since it is being borrowed.
Fees and charges	Annual fees and PIN regeneration fees are applicable.	Credit cards have multiple fees applicable. These include joining fees, annual fees, late payment fees, and bounced cheque fees among others.
Interest	There is no interest that is charged.	Interest is charged on the outstanding amount if it hasn't been paid by the due date.
Limit to funds that can be accessed	You can access any amount up to what is currently available in your savings bank or current account.	You can use the card only up to the pre-set credit limit on your card.
Rewards	Typically, the rewards you get are minimal	Get to enjoy cashback, air miles, and reward points which can be redeemed.
Privileges	Doesn't come with many privileges.	Come with numerous dining, retail, entertainment, and travel privileges (depending on the type of card you have).
Lost card liability	Protection from theft or loss of the card is minimal.	Most cards offer 100% lost liability protection. So, you are not liable for any unauthorized transactions made.

E-Cash Threats

In e-cash, we stored financial information on the computer, electronic device or on the internet which is vulnerable to the hackers. Some of the major threats related to e-cash system are-



E-cash Threats

Backdoors Attacks

A backdoor is a type of program that opens our system or site up to access to other people over the Internet. So a backdoor attack is a type of malware that is used to get unauthorized access to a system by the cybercriminals. The cybercriminals spread the malware in the system through unsecured points of entry, such as outdated plug-ins or input fields. The malware is entered in the system through the backdoor and it makes it ways to the system’s sensitive data including customer personally identifiable information. It works in the background and hides itself from the user that makes it difficult to detect and remove.

A well-known backdoor example is called FinSpy. When installed on a system, it enables the attacker to download and execute files remotely on the system the moment it connects to the internet, irrespective of the system's physical location. It compromises overall system security.

It’s difficult to identify and protect yourself against built-in backdoors. More often than not, the manufacturers don't even know the backdoor is there. The good news is that there are things you can do to protect yourself from the other kinds of backdoors.

- Change your default passwords.
- Monitor network activity.
- Use firewalls
- Choose applications and plugins carefully.
- Use a good cybersecurity solution.
- Use Antiviruses

Denial of service attacks

A denial-of-service attack (DoS attack) is a security attack in which the attacker takes action that prevents the legitimate (correct) users from accessing the electronic devices. It is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. It makes a network resource unavailable to its intended users by temporarily disrupting services of a host connected to the Internet.

Direct Access Attacks

Direct-access attack is an attack where a hacker is able to gain access to a computer and be able to directly download data from it. In such type of attack a hacker gains physical access to the computer to perform an unauthorized activity and installing various types of software to compromise security. These types of software loaded with worms and download a huge amount of sensitive data from the target victims.

There are simple, economical steps we can take to reduce our risk of falling victim to a costly attack:

1. Install, use and regularly update antivirus and antispyware software on every computer used in our business.
2. Never leave your system unlocked.
3. Use a firewall for our Internet connection.

4. Download and install software updates for our operating systems and applications as they become available.
5. Make backup copies of important business data and information.
6. Control physical access to our computers and network components.
7. Secure your Wi-Fi networks. If we have a Wi-Fi network for our workplace make sure it is secure and hidden.
8. Require individual user accounts for each employee.
9. Limit employee access to data and information and limit authority to install software.
10. Regularly change passwords.

Eavesdropping Attack

An eavesdropping attack, also known as a sniffing or snooping attack, is a theft of information as it is transmitted over a network by a computer, smartphone, or another connected device.

The attack takes advantage of unsecured network communications to access data as it is being sent or received by its user. This is an unauthorized way of listening to private communication over the network. It does not interfere with the normal operations of the targeting system so that the sender and the recipient of the messages are not aware that their conversation is tracking.

Following are some tactic through which such type of attacks can be prevented:

- Encryption
- Network Segmentation
- Security technologies-Firewalls, VPNs
- Avoid public Wi-Fi networks.
- Keep your antivirus software updated.
- Use strong passwords.
- Strong passwords that should changed frequently

Benefits of online payments

1) Instant Payment:

Online payments facilitate instant payments for an organization. It breaks the geographical restrictions and let customers purchase even without physical presence. One can easily make a payment sitting comfortably at home or office. The gateway to accept payment online provides the instant notification of the transaction that makes the customer remain assured of the purchased items.

2) Anytime, Anywhere:

E-money can be used anytime and anywhere. It is probably the best form of money to use for international transactions, as there are no hassles of currency exchange. It is reliable, faster than paper checks and drafts, and has low costs of transaction. Today, with e-money becoming more popular, banks are competing to reduce transfer costs and provide accountholders with good deals. If we send someone a check, it will take a few days to clear. But with an online money transaction, the money reaches the other person's account almost instantly. These transactions can be made after the bank has closed, and even on holidays.

3) ***Quick & Easy Setup to Facilitate More Sales:***

Setting up an option to receive online payment is easy and quick to start selling minutes after implementing it. Moreover, there are many service providers available today that offers affordable plans with zero setup fee and very low transaction rates.

4) Reliable Mode of Payments for Global Merchants:

An online invoice software with features to receive online payment is more secure and credible for merchants than receiving payments through cheques. A merchant instantly receives the money with no risk of bounced cheques and the fees associated with it.

5) Induces More Trust in Customers:

Customers today often consider those merchants more reliable that accept payment online through their site. It encourages them to do business with the merchant. At the same time, online invoice payment offers the consumer with the fraud protection that secures their money if they don't receive the product purchased online through a website.

6) Adds Convenience to Recurring Payments:

If we are offering some subscription-based services where our users/customers need to make payments after a certain period of time, the option to receive online payment could be more suitable for you. Instead of sending them reminders every time and requesting to send cheques for the payment, we can automatically collect payments after the end of the subscription term.

7) Credit Cards to Facilitate Low Balance Purchases:

Customers can use their credit cards to make payments, even though they don’t have money in their bank account. More importantly, we can break down the payment into several installments, if we are selling expensive items. And one can use credit cards to pay for the purchases in installments.

8) Boost Referral Marketing with Online Payment Vouchers:

If we have an online invoice payment system in place, we can create an affiliate program where our affiliates can earn referral commissions by sending buyers to you. This will boost our sales and can find an affiliate network, working to increase our revenue.

9) Getting a competitive edge:

For a merchant, an option to receive online payment can improve reputation, allowing it to gain the trust of the customers. Moreover, when others have online payment systems, we cannot afford to ask for payments via cheques as our strategies will significantly sound outdated.

10) Influences impulse buyers:

An online invoice payment method may influence customers to purchase items listed on the website. Since the transaction is quick and easy, and one can pay via credit cards, buyers are more likely to grab the deal, if there is an online payment system in place.

11) More Sales with Last-minute deals:

Many times, merchants throw cost-saving deals to lure customers. If we can receive online payment on our site, a customer can grab a deal even at the last minute. This will increase sales.

12) Record of Transactions:

Each and every transaction made with electronic money is recorded in the bank’s and the user’s online records. These records have all the essential information about the transaction: the name of the payer, the name of the receiver, the date, place and time it took place. This makes it more dependable, and users can access their record of transactions at any time of the day.

Disadvantages of online payments

1) Password Threats:

In case of e-banking or online financial transactions, we need to be a registered user with the respective website. Though most transactions involve the use of one-time passwords thus ensuring safety to a considerable extent, some parts of a transaction, or our personal details and bank account information is accessible through our credentials for the online portal. This gives rise to the need of password protection when handling financial accounts online. Also, if we are transacting with multiple financial institutions or have accounts with multiple banks, the risk of privacy breach is multiplied. For some, maintaining multiple accounts online feels tiresome.

2) Limitations on Amount and Time:

For withdrawal or fund transfer, certain banks may impose limits on the amount or the number of daily transactions, whereby an amount exceeding a certain figure cannot be withdrawn at once, or only a certain number of transactions are allowed per day. While this is taken as a safety measure, some may find it inconvenient.

3) Risk of Being Hacked:

When transacting online, our personal/account information and credit card number is exposed over the Internet. This leads to the risk of our account being hacked. Hackers may use our identity for fraudulent activities or make huge fund transfers from our account, which could mean financial losses for us.

4) False Identity:

There are no means to verify if the person entering information online is the same person he claims to be. This is because unlike physical transactions, the individual is not present in person, and one’s identity is not verified using a photograph or a physical signature. Mostly, electronic cash transactions are based on cryptographic systems. Information being transferred is encoded by means of numeric keys when the transaction details travel across the web. Though electronic payments carry less risk of forgery, the keys are vulnerable to attack.

5) Additional Cost and Effort:

Some electronic transaction services may require you to pay processing fees and the like, thus leading to increased costs. Some systems require setup fees, while some others enforce a certain number of transactions every month. Electronic payment systems need Internet access, which may invite additional costs. Setting up the account, accessing the Internet, familiarizing oneself with the interface and operating it efficiently, involves additional effort, and may be cumbersome for some.

6) Loss of Smart Cards:

Electronic payments involve the use of smart cards (credit and debit cards, ATM cards, identity cards, etc.) And this involves the risk of their theft or loss. In case a lost smart card falls in the wrong hands or if it is stolen, our identity is at the risk of theft and the money in the account that the card is linked to, may be spent by fraudulent users. There are measures to inform the bank about the loss of our card and get it blocked. But the time between losing the card and blocking it, is critical. Unauthorized users may carry out transactions in our name during that period.

7) Higher Interest Rates:

Credit card companies indeed have a higher interest rate than most offline banking systems. This is very panic for credit card users.

8) Transaction charges:

Another drawback of e-payments systems for merchants is that although they are generally free for the consumer to use, however, the merchant pays a charge to the payment provider to finance the system. This may eat into profit margins, especially on smaller transactions.

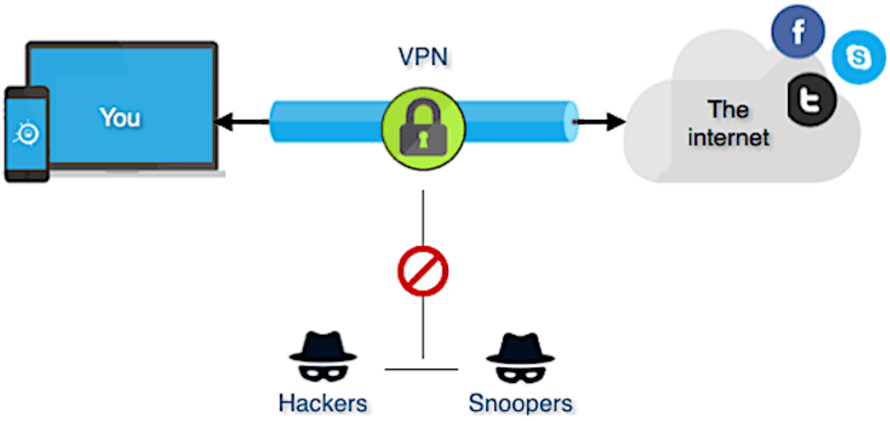
9) Dependency on technology:

As with any system that relies heavily on technology, e-payments put businesses at the mercy of the technology. Internet connection failure can leave companies unable to make or accept payments. Payment gateways may suffer technical issues or cyberattacks that leave them unable to approve transactions. For the consumer, these issues are frustrating; for businesses, they can mean a significant loss in revenue.

Virtual Private Network (VPN):

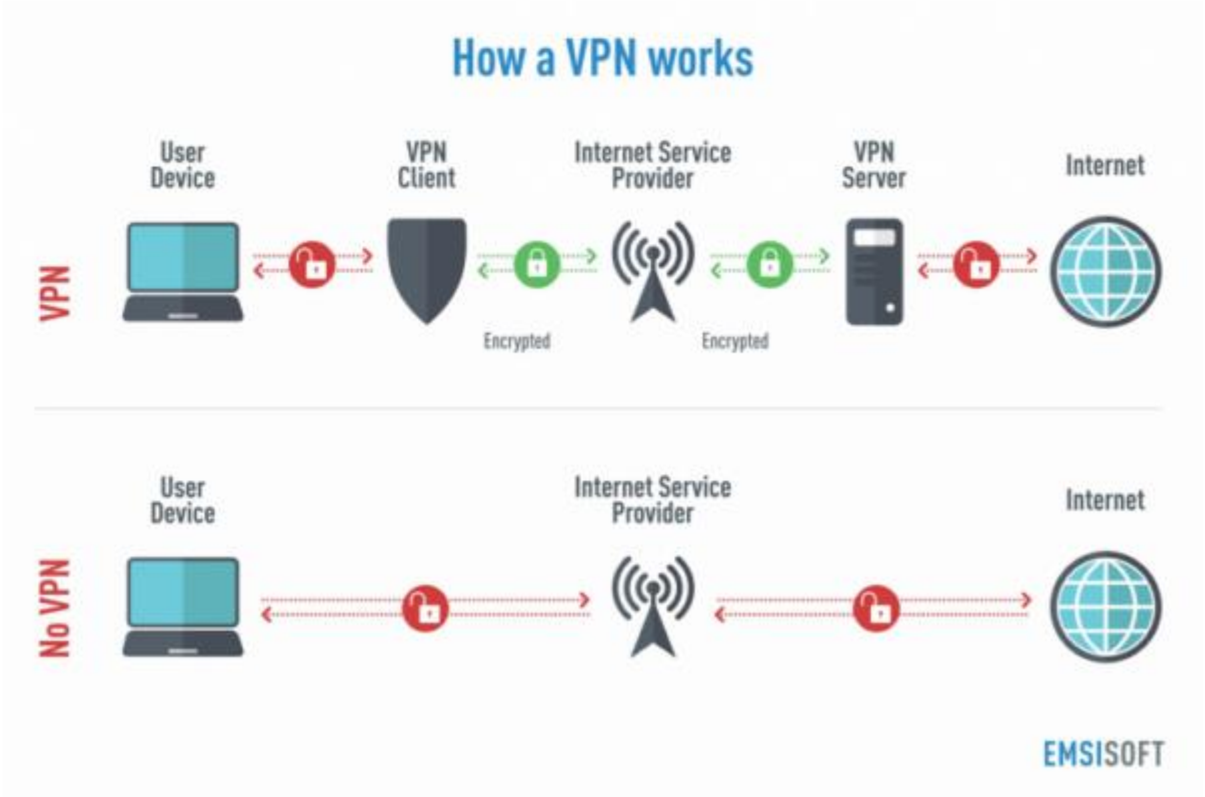
Virtual private networks (VPNs) can offer an additional layer of security and privacy. A virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely. VPN technology is widely used in e-commerce environments.

VPN is a way to extend a private network using a public network such as internet. The name only suggests that it is Virtual "private network" i.e. user can be the part of local network sitting at a remote location. It uses tunneling protocols to encrypt data at the sending end, and decrypt it at the receiving end. The originating and receiving network addresses are also encrypted to provide better security for online activities.



How a VPN works

A VPN works by routing our device's internet connection through our chosen VPN's private server rather than our internet service provider (ISP) so that when our data is transmitted to the internet, it comes from the VPN rather than our computer. The VPN acts as an intermediary of sorts as we connect to the internet, thereby hiding our IP address – the string of numbers our ISP assigns our device – and protecting our identity. Furthermore, if our data is somehow intercepted, it will be unreadable until it reaches its final destination. VPN creates a private "tunnel" from our device to the internet and hides our essential data through something that is known as encryption.



The Three Main Types of VPNs

VPNs can be divided into three main categories –

- **Remote access,**
- **Intranet-based site-to-site VPN, and**
- **Extranet-based site-to-site VPN**

Individual users are most likely to encounter remote access VPNs, whereas big businesses often implement site-to-site VPNs for corporate purposes.

1- Remote Access VPN

A remote access virtual private network (VPN) enables users who are working remotely to securely access and use applications and data that reside in the corporate data center and headquarters, encrypting all traffic the users send and receive.

Remote access VPN allows a user to connect to a private network and access its services and resources remotely. The connection between the user and the private network happens through the Internet and the connection is secure and private.

Remote Access VPN is useful for business users as well as home users.

A corporate employee, while traveling, uses a VPN to connect to his/her company's private network and remotely access files and resources on the private network.

Remote Access VPNs are the most popular type of VPN these days. Basically, these connect users to a remote server located in another country. Most commercial VPN services out there are built upon this foundation! They allow us to browse the internet using their own network, encrypting the data we send and receive in the process.

2. Intranet VPN

A company that has multiple remote locations can quickly and securely communicate with each other by creating an intranet VPN. This connects each local area network (LAN) to a single wide area network (WAN).

3. Extranet VPN

A company that has business ties with other companies can create an extranet VPN to connect each other's LANs. This enables all parties to work together in a shared network environment while restricting access to their respective intranets.

Remote Access VPN	**Site-to-Site VPN** **(Intranet VPN)** **(Extranet VPN)**
• Connects individual users to the open internet through a private network	• Connects entire networks consisting of multiple users to one another
• Users are typically required to have a VPN client installed	• Eliminates the need for each user to run VPN client software
• Suitable for personal use	• Suitable for corporate use
• Very cost-effective	• Costly to implement and maintain

VPN protocols

VPN protocols represent the processes and sets of instructions VPN providers rely on in order to ensure VPN users get to enjoy stable, secure VPN client-VPN server communications. At its core, a VPN protocol is basically a mix of transmission protocols and encryption standards.

VPN protocols ensure an appropriate level of security to connected systems, when the underlying network infrastructure alone cannot provide it. There are several different protocols used to secure and encrypt users and corporate data. They include:

1. Point-To-Point Tunneling Protocol (PPTP)
2. Layer 2 Tunneling Protocol (L2TP)
3. IP security (IPsec)
4. Open VPN
5. Secure Socket Tunneling Protocol (SSTP)

1. **Point–to–Point Tunneling Protocol (PPTP):**

PPTP stands for Point-to-Point Tunneling Protocol, and it's a VPN protocol that was developed by Microsoft back in the '90s. Nowadays, it's pretty popular for people who want to stream geo-restricted content because of its high speeds. Besides that, the VPN is also easy to configure and is already built into most platforms.

PPTP or Point-to-Point Tunneling Protocol generates a tunnel and confines the data packet. Point-to-Point Protocol (PPP) is used to encrypt the data between the connections. PPTP is one of the most widely used VPN protocol and has been in use since the early release of Windows. PPTP is also used on Mac and Linux apart from Windows.

PPTP protocol (set of communication rules) allows corporations to extend their own corporate network through private "tunnels" over the public Internet.

2. **Layer 2 Tunneling Protocol (L2TP): IPSec**

L2TP or Layer 2 Tunneling Protocol is a tunneling protocol that is often combined with another VPN security protocol like IPSec to establish a highly secure VPN connection.

L2TP generates a tunnel between two L2TP connection points and IPSec protocol encrypts the data and maintains secure communication between the tunnels.

Generally considered an improvement over PPTP, L2TP/IPSec is basically an extension of the PPTP protocol, with the main difference being that it uses double encapsulation:

- The first encapsulation sets up the PPP connection.
- The second encapsulation has the actual IPSec encryption.

While double encapsulation can make L2TP/IPSec more secure, it can also make it slower than PPTP since traffic needs to first be converted into L2TP form, and afterwards you also have an extra layer of encryption added on top.

3. **Internet Protocol Security (IPSec):**

   Internet Protocol Security, known as IPSec, is used to secure Internet communication across an IP network. IPSec secures Internet Protocol communication by verifying the session and encrypts each data packet during the connection.

   IPSec runs in 2 modes:

   (i) Transport mode

   (ii) Tunneling mode

   The work of transport mode is to encrypt the message in the data packet and the tunneling mode encrypts the whole data packet. IPSec can also be used with other security protocols to improve the security system. IPSec is pretty popular due to its high security and the fact that it can encrypt traffic without the end point application being aware of it.

4. **OpenVPN:**

   An open-source protocol, OpenVPN is one of the most popular VPN protocols among users. It’s very secure, configurable, and works on multiple platforms. Furthermore, OpenVPN is very difficult to block because OpenVPN traffic is extremely difficult to tell apart from HTTPS/SSL traffic.

   OpenVPN is an open source VPN that is commonly used for creating Point-to-Point and Site-to-Site connections. It uses a traditional security protocol based on SSL and TLS protocol.

5. **Secure Socket Tunneling Protocol (SSTP)**

   SSTP stands for Secure Socket Tunneling Protocol, and it was introduced by Microsoft with Windows Vista. Even though, it still works on other operating systems too (like Linux and Android). SSTP is significantly superior to PPTP when it comes to security since it can be configured with AES encryption. Online shopping websites commonly uses SSL and TLS protocol. It is easy to switch to SSL by web browsers and with almost no action required from the user as web browsers come integrated with SSL and TLS. SSL connections have “https” in the initial of the URL instead of “http”.

VPN Protocol Comparison

VPN Protocol	Connection Speed	Level of Encryption	Connection Stability	Media Streaming	Torrent Downloading	Compatible With
OpenVPN	Medium	Very Good	Stable	Medium	Good	Most OSs and devices
IPSec	Medium	Good	Stable	Good	Good	Most OSs and devices
SSTP	Fast	Good	Very Stable	Medium	Good	Windows, Ubuntu, Android, and routers
L2TP/IPSec	Medium	Medium	Stable	Good	Medium	Most OSs and devices
PPTP	Very Fast	Poor	Very Stable	Good	Poor	Most OSs and devices

VPN privacy and functionality

A VPN can hide a lot of information. Here are some of them.

1. ***Our browsing history:*** It's no secret where we go on the internet. Our internet service provider and our web browser can track just about everything we do on the internet. A lot of the websites we visit can also keep a history. Web browsers can track our search history and tie that information to our IP address. By VPN we can hide our browsing history.
2. ***Our IP address and location***: Anyone who captures our IP address can access what we've been searching on the internet and where we were located when we searched. Think of our IP address as the return address we'd put on a letter. It leads back to our device.

   Since a VPN uses an IP address that's not our own, it allows we to maintain our online privacy and search the web secretly. We're also protected against having our search history gathered, viewed, or sold.
3. ***Our location for streaming****:* We might pay for streaming services (Netflix, Amazon Prime Video, Disney Plus etc.) that enable us to watch things like professional sports. When we

travel outside the country, the streaming service may not be available. There are good reasons for this, including contractual terms and regulations in other countries. Even so, a VPN would allow us to select an IP address in our home country. That would likely give us access to any event shown on our streaming service. We may also be able to avoid data or speed throttling.

4. ***Our devices:*** A VPN can help protect our devices, including desktop computer, laptop, tablet, and smart phone from snooping eyes. Our devices can be prime targets for cybercriminals when we access the internet, especially if we're on a public Wi-Fi network. In short, a VPN helps protect the data you send and receive on our devices so hackers won't be able to watch our every move.
5. ***Our web activity — to maintain internet freedom:*** a VPN protects against our internet service provider seeing our browsing history. So we are protected if a government agency asks our internet service provider to supply records of our internet activity. Assuming our VPN provider doesn't log our browsing history (some VPN providers do), our VPN can help protect our internet freedom.
6. ***Encrypt data transfers:*** VPNs use encryption to scramble data when it's sent over a Wi-Fi network. Encryption makes the data unreadable. Data security is especially important when using a public Wi-Fi network, because it prevents anyone else on the network from eavesdropping on our internet activity.
7. ***Access blocked websites:*** Blocked content is a disappointment. Whether it's our school, work, the country we're traveling in, or something else preventing us from accessing a site, there are always ways to fight back. With the help of VPN we can access our favorite content.

Unit-4

FUNDAMENTAL OF E-COMMERCE (FEC)

E-Security concerns in E Commerce

eCommerce security is important for a number of reasons, specifically when it comes to protecting the privacy and sensitive data of customers on a website, safeguarding the finances of an online business, preventing fraud and financial scams and defending the reputation of an online store as a safe place to conduct transactions.

eCommerce security is the prevention that ensure safe transaction through the internet. It consists of protocols that safeguard people who engage in online selling and buying of goods and services. We need to gain our customers' trust by putting in place eCommerce security basics. Such basics include:

- Privacy
- Integrity
- Authentication
- Non-repudiation
- Confidentiality

1. Privacy

Privacy includes preventing any activity that will lead to the sharing of customers' data with unauthorized third parties. Apart from the online seller that a customer has chosen, no one else should access their personal information and account details.

A breach of confidentiality occurs when sellers let others have access to such information. An online business should put in place at least a necessary minimum of anti-virus, firewall, encryption, and other data protection. It will go a long way in protecting credit card and bank details of clients.

2. Integrity

Integrity is another crucial concept of eCommerce Security. It means ensuring that any information that customers have shared online remains unaltered. The principle states that the online business is utilizing the customers' information as given, without changing anything. Altering any part of the data causes the buyer to lose confidence in the security and integrity of the online enterprise.

3. Authentication

The principle of authentication in eCommerce security requires that both the seller and the buyer should be real. They should be who they say they are. The business should prove that it is real, deals with genuine items or services, and delivers what it promises. The clients should also give their proof of identity to make the seller feel secure about the online transactions. It is possible to ensure authentication and identification. If you are unable to do so, hiring an expert will help a lot. Among the standard solutions include client logins information and credit card PINs.

4. Non-repudiation

Repudiation means denial. Therefore, Non-repudiation is a legal principle that instructs players not to deny their actions in a transaction. The business and the buyer should follow through on the transaction part that they initiated. eCommerce can feel less safe since it occurs in cyberspace with no live video. Non-repudiation gives eCommerce security another layer. It confirms that the communication that occurred between the two players indeed reached the recipients. Therefore, a party in that particular transaction cannot deny a signature, email, or a purchase.

5. Confidentiality

Confidentiality refers to protecting information from being accessed by an unauthorized person on the internet. In other words, only the people who are authorized can gain access to view or modify or use the sensitive data of any customer or merchants.

Common Ecommerce Security Threats & Issues

Common examples of security threats include hacking, misuse of personal data, monetary theft, phishing attacks, unprotected provision of services, and credit card frauds.

1. *Financial Frauds*

There are various kinds of financial frauds widespread in the e-commerce industry, but we are going to discuss the two most common of them.

a. Credit Card Fraud

It happens when a cybercriminal uses stolen credit card data to buy products on our e-commerce store. Another form of credit card fraud is when the fraudster steals our personal details and identity to enable them to get a credit card.

b. Fake Return & Refund Fraud

The bad players perform unauthorized transactions and clear the trail, causing businesses great losses. Some hackers also engage in refund frauds, where they file fake requests for returns. Refund fraud is a common financial fraud where businesses refund illegally acquired products or damaged goods.

2. ***Phishing Attacks***

It is one of the common security threats of ecommerce where hackers masquerade as legitimate businesses and send emails to our clients to trick them into revealing their sensitive information by simply presenting them with a fake copy of our legitimate website or anything that allows the customer to believe the request is coming from the business.

Common phishing techniques include emailing our customers or our team with fake “you must take this action” messages. This technique only works our customers follow through with the action and provide them access to their login information or other personal data which the hacker can exploit as per his benefit.

3. ***Spamming***

Where emails are known as a strong medium for higher sales, it also remains one of the highly used mediums for spamming. Nonetheless, comments on our blog or contact forms are also an open invitation for online spammers where they leave infected links in order to harm us. They often send them via social media inbox and wait for us to click on such messages. Moreover, spamming not only affects our website’s security, but it also damages our website speed too.

4. ***DOS Attacks***

A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash.

5. ***Brute Force Attacks***

These attacks target our online store’s admin panel in an attempt to figure out our password by brute-force A brute force attack uses trial-and-error to guess login info, encryption keys, or find a hidden web page. Hackers work through all possible combinations hoping to guess correctly. We can protect our self against such attacks by using a strong, complex password. Do remember to change it regularly.

6. ***Malware***

A malware attack is a common cyberattack where malware (normally malicious software) executes unauthorized actions on the victim's system. Hackers may design a malicious software and install on our IT and computer systems without our knowledge. These malicious programs include spyware, viruses, Trojan horses, and ransomware.

The systems of our customers, admins, and other users might have Trojan Horses downloaded on them. These programs can easily swipe any sensitive data that might be present on the infected systems and may also infect our website.

7. e-Skimming

E-skimming involves infecting a website's checkout pages with malicious software. The intention is to steal the clients' personal and payment details. Skimming is an illegal practice used by identity thieves to capture credit card information from a cardholder surreptitiously. Fraudsters often use a device called a skimmer that can be installed at gas pumps or ATM machines to collect card data.

8. SQL Injections

SQL injections are cyber-attacks intended to access our database by targeting our query submission forms. Attacker can inject SQL of their choosing into the database and delete, copy, or modify the contents of the database. An attacker can also modify cookies to poison a web application's database query.

Ecommerce Security Solutions

1. HTTPS and SSL certificates

Using outdated HTTP protocols makes us exposed to attacks. It is strongly recommend that we switch to HTTPS that says "secured" next to the URL bar on our customer's computer. HTTPS protocols not only protect the sensitive information users submit, but their user data as well.

2. Secure Your Servers and Admin Panels

Most ecommerce platforms come with default passwords that are ridiculously easy to guess. And if we don't change them we are exposing our self to unnecessary hacks. Use complex password(s) and usernames and change them frequently.

We can go one step further and make the panel notify us every time an unknown IP attempts to log in. These simple steps can significantly improve your web store's security.

3. Securing Payment Gateway

Avoid storing the credit card information of our clients on our database. Instead, let a third party such as PayPal and Stripe handle the payment transactions away from our website. This ensures better safety for our customers' personal and financial data.

4. **Antivirus and Anti-Malware Software**

Always upkeep and update the network’s servers and equipment with antivirus and anti-malware software. Hackers can use stolen credit card information to place orders from anywhere in the world. An antivirus or an anti-fraud software can help us with this serious ecommerce issue.

5. **Use Firewalls**

Another effective ecommerce recommendation is to use firewall software that are pocket-friendly yet effective. They keep untrusted networks at bay and regulate traffic that enters and leaves our site.

6. **Backup Data**

Always back up data and do this regularly. A backup and restore plugin will help. If we have back up of our data so a business can recover quickly if an attack happens.

7. **Educating Staff and Clients**

Ensure our employees and customers get the latest knowledge concerning handling user data and how to engage with our website securely. Expunge former employees’ details and revoke all their access to our systems.

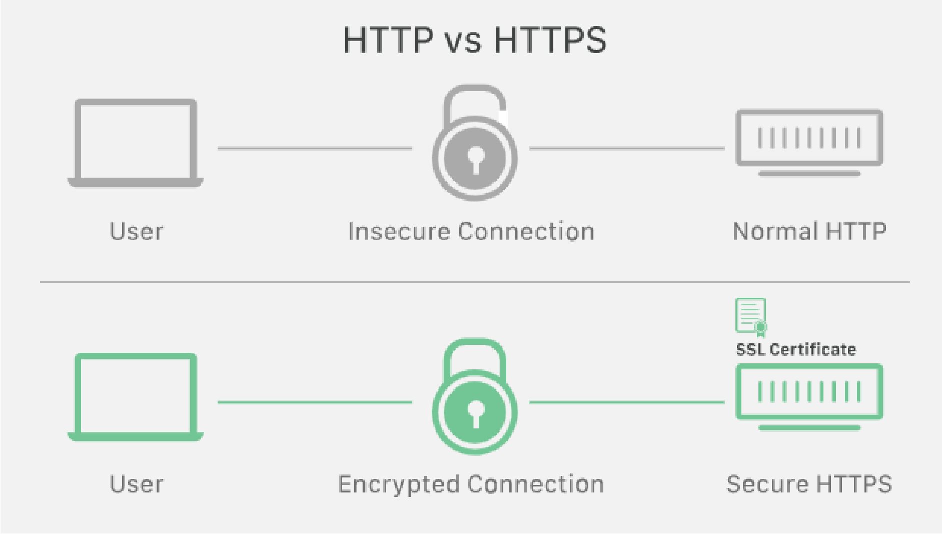
8. **Additional security implementations**

- Always scan your websites and other online resources for malware
- Employ Multi-Layer Security
- Ecommerce Security Plugins
- Update your systems frequently and employ effective e-commerce security plug-ins.
- Lastly, get a dedicated security platform that is secure from frequent cyber-attacks.

SSL (Secure Sockets Layer)

SSL, or Secure Sockets Layer, is an encryption-based Internet security protocol. It was first developed by Netscape in 1995 for the purpose of ensuring privacy, authentication, and data integrity in Internet communications. SSL is the predecessor to the modern TLS (Transport Layer Security) encryption used today.

A website that implements SSL/TLS has "HTTPS" in its URL instead of "HTTP."



SSL Certificates protect our sensitive information such as credit card information, usernames, passwords etc. They also:

- Keep data secure between servers
- Increase our Google Rankings
- Build/Enhance customer trust
- Improve conversion rates

What is an SSL certificate?

SSL can only be implemented by websites that have an SSL certificate (technically a "TLS certificate"). An SSL certificate is like an ID card or a badge that proves someone is who they say they are. SSL certificates are stored and displayed on the Web by a website's or application's server.

Where Do I Buy an SSL Certificate?

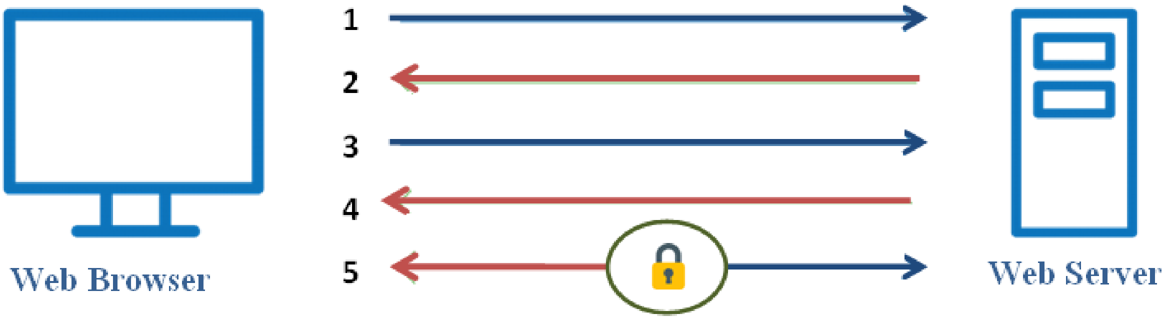
SSL Certificates need to be issued from a trusted Certificate Authority (CA). Browsers, operating systems, and mobile devices maintain lists of trusted CA root certificates.

The Root Certificate must be present on the end user's machine in order for the Certificate to be trusted. If it is not trusted the browser will present un-trusted error messages to the end user. In the case of e-commerce, such error messages result in immediate lack of confidence in the website and organizations risk losing confidence and business from consumers.

How Does the SSL Certificate Create a Secure Connection?

When a browser attempts to access a website that is secured by SSL, the browser and the web server establish an SSL connection using a process called an "SSL Handshake" (see diagram below). Note that the SSL Handshake is invisible to the user and happens instantaneously.

Essentially, three keys are used to set up the SSL connection: the public, private, and session keys. Anything encrypted with the public key can only be decrypted with the private key, and vice versa. Because encrypting and decrypting with private and public key takes a lot of processing power, they are only used during the SSL Handshake to create a symmetric session key. After the secure connection is made, the session key is used to encrypt all transmitted data.



1. **Browser** connects to a web server (website) secured with SSL (https). Browser requests that the server identify itself.
2. **Server** sends a copy of its SSL Certificate, including the server's public key.
3. **Browser** checks the certificate root against a list of trusted CAs and that the certificate is unexpired, unrevoked, and that its common name is valid for the website that it is connecting to. If the browser trusts the certificate, it creates, encrypts, and sends back a symmetric session key using the server's public key.
4. **Server** decrypts the symmetric session key using its private key and sends back an acknowledgement encrypted with the session key to start the encrypted session.
5. **Server** and **Browser** now encrypt all transmitted data with the session.

How does SSL/TLS work?

- In order to provide a high degree of privacy, SSL encrypts data that is transmitted across the web. This means that anyone who tries to intercept this data will only see a garbled mix of characters that is nearly impossible to decrypt.
- SSL initiates an authentication process called a handshake between two communicating devices to ensure that both devices are really who they claim to be.
- SSL also digitally signs data in order to provide data integrity, verifying that the data is not tampered with before reaching its intended recipient.

Why is SSL/TLS important?

Originally, data on the Web was transmitted in plaintext that anyone could read if they intercepted the message. For example, if a consumer visited a shopping website, placed an order, and entered their credit card number on the website, that credit card number would travel across the Internet unconcealed.

SSL was created to correct this problem and protect user privacy. By encrypting any data that goes between a user and a web server, SSL ensures that anyone who intercepts the data can only see a scrambled mess of characters. The consumer's credit card number is now safe, only visible to the shopping website where they entered it.

SSL also stops certain kinds of cyber attacks: It authenticates web servers, which is important because attackers will often try to set up fake websites to trick users and steal data. It also prevents attackers from tampering with data in transit.

Are SSL and TLS the same thing?

SSL is the direct predecessor of another protocol called TLS (Transport Layer Security). In 1999 the Internet Engineering Task Force (IETF) proposed an update to SSL. Since this update was being developed by the IETF and Netscape was no longer involved, the name was changed to TLS. The differences between the final version of SSL (3.0) and the first version of TLS are not drastic; the name change was applied to signify the change in ownership.

Since they are so closely related, the two terms are often used interchangeably and confused. Some people still use SSL to refer to TLS, others use the term "SSL/TLS encryption" because SSL still has so much name recognition.

What are the types of SSL certificates?

There are several different types of SSL certificates. One certificate can apply to a single website or several websites, depending on the type:

Single-domain SSL certificate: A single-domain SSL certificate applies to only one domain (a "domain" is the name of a website, like www.cloudflare.com).

Wildcard SSL certificate: Like a single-domain certificate, a wildcard SSL certificate applies to only one domain. However, it also includes that domain's subdomains. For example, a wildcard certificate could cover www.cloudflare.com, blog.cloudflare.com, and developers.cloudflare.com, while a single-domain certificate could only cover the first.

Multi-domain SSL certificate: As the name indicates, multi-domain SSL certificates can apply to multiple unrelated domains.

Digital Signatures

Digital Signature is a process that guarantees that the contents of a message have not been altered in transit. It is a technique that binds a person identity to the digital data. This binding can be independently verified by receiver. Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer.

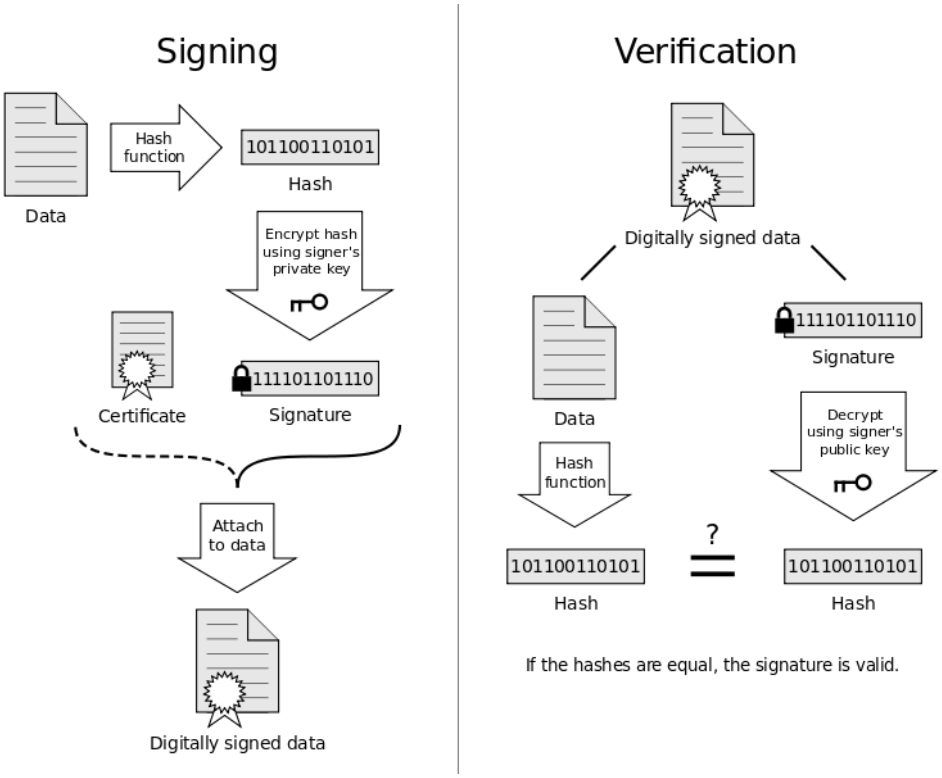
In real world, the receiver of message needs assurance that the message belongs to the sender and he should not be able to deny the origination of that message. This requirement is very important in business applications, since chances of a dispute over exchanged data are very high. To overcome this problem digital signature were introduced.

Digital Signature is a mathematical technique used to validate the authenticity and integrity of a digital document as well as to provide non-repudiation, meaning that the signer cannot claim they did not sign the document. As the digital equivalent of a handwritten signature or stamped seal, a digital signature offers far more inherent security, and it is intended to solve the problem of tampering and impersonation in digital communications.

Digital signatures are generated and verified through standardized frameworks such as the Digital Signature Algorithm (DSA).

There are typically three algorithms involved with the digital signature process:

- **Key generation algorithm** – This algorithm provides a private key along with its corresponding public key.
- **Signing algorithm** – This algorithm produces a signature upon receiving a private key and the message that is being signed.
- **Verification algorithm** – This algorithm checks for the authenticity of the message by verifying it along with the signature and public key.



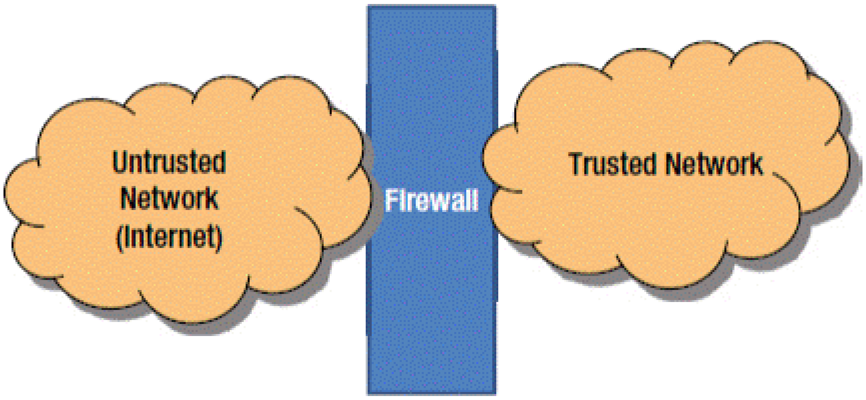
Importance of Digital Signature

Apart from ability to provide non-repudiation of message, the digital signature also provides message authentication and data integrity. Let us briefly see how this is achieved by the digital signature −

- **Message authentication** − When the verifier validates the digital signature using public key of a sender, he is assured that signature has been created only by sender who possess the corresponding secret private key and no one else.
- **Data Integrity** − In case an attacker has access to the data and modifies it, the digital signature verification at receiver end fails. The hash of modified data and the output provided by the verification algorithm will not match. Hence, receiver can safely deny the message assuming that data integrity has been breached.
- **Non-repudiation** − Since it is assumed that only the signer has the knowledge of the signature key, he can only create unique signature on a given data. Thus the receiver can present data and the digital signature to a third party as evidence if any dispute arises in the future.

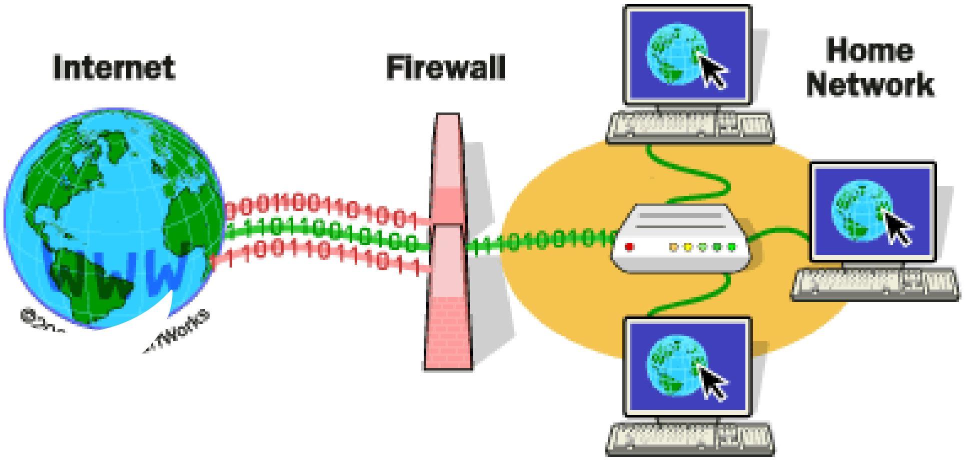
Firewalls

When it comes to prevent unauthorized access of third party in a private network, **firewalls** are used. A lfirewall is a type of security tool that is used to filter traffic on a network. It is a network security device that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules.



Firewalls have been a first line of defense in network security for over 25 years. They establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet.

A firewall can be hardware, software, or both.



Basic Functions of Firewall

A firewall in the networking world should examine the traffic that is entering into the network and pass the "Wall" based on some rules defined by the network and its resources. It acts as a security guard, who normally sits at the main gate, and checks your identity and access privileges and lets you in. Depending on the type of organization, the guards may screen people who are exiting the gate too.

Types of Firewalls

The three basic types of network firewalls are: **packet filtering (stateless), stateful**, and **application layer**.

Packet filtering, or stateless- Packet filtering is a firewall technique used to control network access by monitoring outgoing and incoming packets and allowing them to pass or halt based on the source and destination Internet Protocol (IP) addresses, protocols and ports.

Packet-filtering firewalls are very fast because there is not much logic going behind the decisions they make. They do not do any internal inspection of the traffic. They also do not store any state information. We have to manually open ports for all traffic that will flow through the firewall.

Packet-filtering firewalls are considered not to be very secure. This is because they will forward any traffic that is flowing on an approved port. So there could be malicious traffic being sent, but as long as it's on an acceptable port, it will not be blocked.

Stateful firewalls- Stateful firewalls are able to determine the connection state of packets, which makes them much more flexible than stateless firewalls. Stateful firewalls are capable of monitoring all aspects of network traffic, including their communication channels and characteristics. They are also referred to as dynamic pocket filters as they filter traffic packets based on the context and state.

- Context – it involves metadata of packets including ports and IP address belonging to the endpoint's and destination, packet length, layer 3 information related to reassembly and fragmentation, flags, and numbers for TCP sequence of layer 4, and more.
- State – firewalls apply their policy based on the state of the connection. To understand the state, let's take the example of TCP-based communication. In TCP, 4 bits control connection state – SYN, ACK, FIN, and RST.

When a connection initiates through a 3-way handshake, then the TCP indicates the SYN flag, which the firewall uses to indicate the arrival of a new connection. Next, the connection receives the flag SYN+ACK by the server. Until the client reverts with ACK, the connection does not establish.

Similarly, on seeing FIN+ACK or RST packet, the connection is marked for deletion right there along with for future packets.

Application firewalls- Application firewalls, or application layer firewalls, use a series of configured policies to determine whether to block or allow communications to or from an app. These are also known as proxy-based firewalls.

Traditional firewalls control data flow to and from the CPU, examining each packet as it passes through. An application firewall takes it further by controlling and checking data itself. This way, even if a hacker gains entry to a network or server, they can't execute malicious code.

Advantages of Firewall

1. **Monitor Traffic-**

   A major responsibility of a firewall is to monitor the traffic passing through it. Whatever the information traveling through a network is in the form of packets. Firewall inspects each of these packets for any hazardous threats. If any chance the firewall happens to find them it will immediately block them.

2. Protection against Malware

Malwares especially the type Trojans are dangerous to a user. A Trojan silently sits on your computer spying over all the works you do with it. Whatever the information they gather will be sent to a web server. Obviously you will not know their presence until the strange behaviours of your computer. A firewall in this instance will immediately block Trojans before they cause any damages to your system.

3. Prevent Hackers

Hackers on the internet constantly look for computers in order for carrying out their illegal activities. When the hackers happen to find such computers they will start to do even malicious activities such as spreading viruses. Apart from those hackers there can be unknown people such as the neighbours looking out for an open internet connection. Hence, to prevent such intrusions it is a good idea to be with a firewall security.

4. Access Control

Firewalls comes with an access policy that can be implemented for certain hosts and services. Some hosts can be exploited with the attackers. So the best in case is to block such hosts from accessing the system. If a user feels that they need protection from these types of unwanted access, this access policy can be enforced.

5. Better Privacy

Privacy is one of the major concerns of a user. Hackers constantly look out for privacy information for getting clues about the user. But by using a firewall many of the services offered by a site such as the domain name service and the finger can be blocked. Hence, the hackers are with no chance of getting privacy details. Additionally firewalls can block the DNS information of the site system. Due to this the names and the IP address will not be visible to the attackers.

E-Cash

eCash was created by Dr. David Chaum under his company, DigiCash, in 1990. E-cash is a paperless cash system which facilitates the transfer of funds anonymously. E-cash is free to the user while the sellers have paid a fee for this. The e-cash fund can be either stored on a card itself or in an account which is associated with the card. The most common examples of e-cash system are transit card, PayPal, GooglePay, Paytm, etc./ e-cash has no physical existence i.e they are intangible.

E-cash has four major components-

- **Issuers** - They can be banks or a non-bank institution.
- **Customers** - They are the users who spend the e-cash.
- **Merchants or Traders** - They are the vendors who receive e-cash.
- **Regulators** - They are related to authorities or state tax agencies.

Understanding eCash

Internet has connected people around the world and subsequently enables businesses to offer products and services around the globe without being physically present in front of the consumers or potential consumers. As time goes by, Internet has become a part of the daily life, which demands more and more applications being created and services being made available to make full use of the infrastructure. With the online business transaction, E-cash is one of the services that attract people attention for doing business transaction electronically. It is a replacement for traditional coins and paper notes, which is not viable for e-commerce.

Another alternative for online payment scheme is the credit cards, however notational schemes such as credit cards require recording of transactions to be made into some individual accounts. This method requires a trust from the merchant site, which usually facilitated by verification authority such as credit-card issuer or payment gateway. Because of the "trust" requirement, this method normally eliminates user-merchant transactional anonymity. On the other hand token-based payment schemes such as E-cash does not require transactions to be recorded since the token itself allows straightforward verification by the merchant.

E-cash can be implemented in two ways, on-line and off-line. On-line means E-cash is stored by the bank or issuer and consumer needs to request for it when a consumer makes payment. Off-line e-cash is kept by consumer in a devise such as smart card or other type of token.

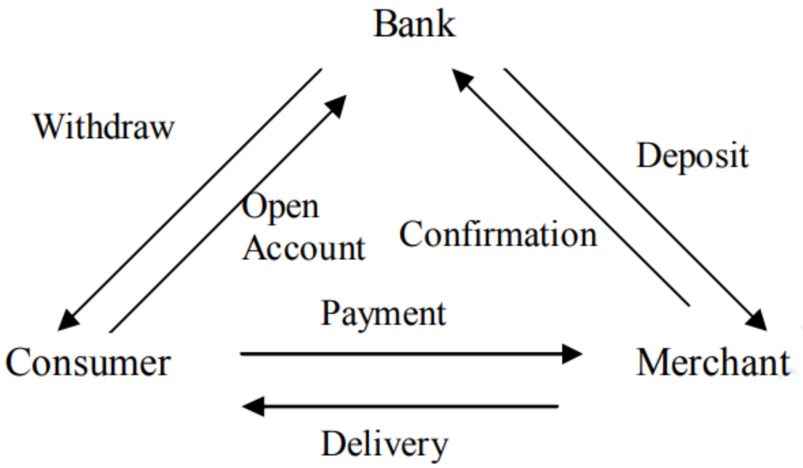
In 1990, Chaum created the company, DigiCash, to realize his idea for eCash. He was ahead of his time in thinking about privacy concerns in the age of the Internet. And not only he thought for privacy but he took it a few steps further in creating an anonymous based payment system. This was even before the Internet was available for public use.

The core concept behind eCash was blind signatures. A blind signature is a type of digital signature in which the message's content is invisible prior to signing. In this manner, no user is able to create a link between withdrawals and spend transactions.

General E-Cash Implementation

1. Consumer needs to open an account with a bank or issuer. Merchant who wants to participate in E-cash transaction need to have accounts with various banks in order to support consumer’s transaction who might use any bank account. The banks on the other hand will handle both consumers’ and merchants’ accounts.
2. When consumer decides to purchase, he or she will transfers the E-cash from his/her bank account to his/her electronic purse (on-line system) or E-cash token (off-line system). The E-cash can then be transferred to the merchant in exchange with the merchant’s products or services. The E-cash payment can be in term of softcopy (via software) or token based. Transactions via Internet are normally encrypted.
3. Upon receiving E-cash payment from consumer, merchant will get confirmation from the bank. The bank will then authenticate the E-cash transaction. At the same time the bank will debit consumer’s account based on the agreed amount. The merchant will then delivers the products or services and instructs the bank to deposit the agreed amount to the merchant’s bank account.

The diagram below represent E-cash processes in general:



Properties of E-Cash

To be able to replace coins and paper notes, E-cash should be as good as coins and paper notes in term of features.

1. **Security**

For any E-cash system to be accepted, security is one of the prime concerns that need to be considered. The originality of the message being transferred among consumers, merchants and banks need to be secured to avoid any unauthorized individual intercepting or changing the content of the messages. In order to protect E-cash from such illegal activity, E-cash system must possess quality such as integrity, non-repudiation and able to authenticate.

2. **Privacy**

Privacy in E-cash means the existence of anonymity for the consumers who made the payment. Similar to coins and paper notes there should not be any link or trace to individual who uses the E-cash for any transaction. This feature is needed in order to protect consumers’ privacy from being monitored for the purpose of financial surveillance.

3. **Portability**

E-cash should be portable, similar to the conventional money where it does not depends on physical location. E-cash should be transferable via network to portable storage devices.

4. Transferability

Transferability features allow consumers to transfer E-cash from one person to another without a need to refer to the bank. Similar to conventional cash where coins or paper notes can be transferred easily, E-cash should be able to do the same.

5. Divisibility

By divisible, it means E-cash should possess the ability to make change where E-cash can be divided into small denominations to allow small value transaction possible (this is known as micropayment). The challenge for divisible system is to be able to divide the E-cash value to small values where the total of the small E-cash value is equal to the original value.

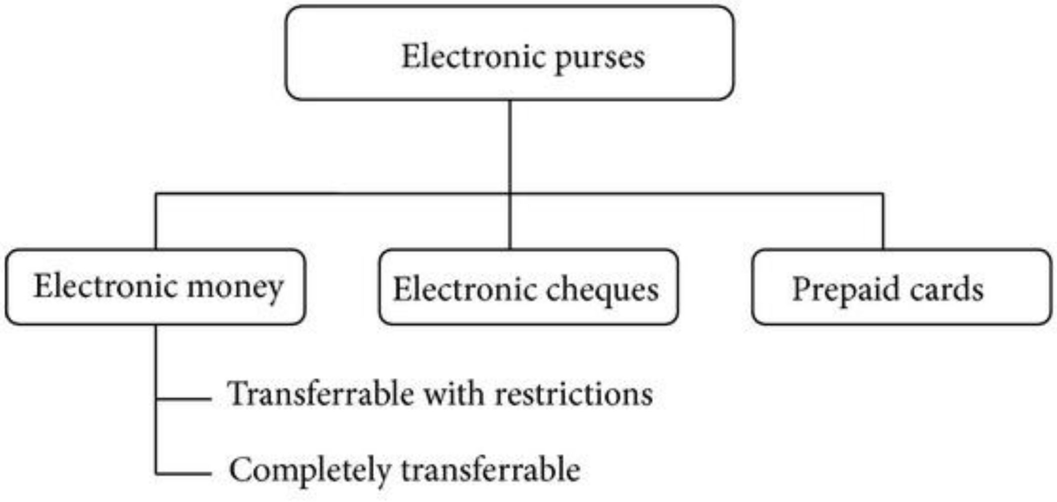
E-Purses

Definition: E- **Purses** is a type of electronic card which is used for transactions made online through a computer or a smartphone. Its utility is same as a credit or debit card. An E-wallet needs to be linked with the individual’s bank account to make payments.

Descriptions: E-wallet is a type of pre-paid account in which a user can store his/her money for any future online transaction. An E-wallet is protected with a password. With the help of an E-wallet, one can make payments for groceries, online purchases, and flight tickets, among others.

E-wallet has mainly two components, software and information. The software component stores personal information and provides security and encryption of the data. The information component is a database of details provided by the user which includes their name, shipping address, payment method, amount to be paid, credit or debit card details, etc.

For setting up an E-wallet account, the user needs to install the software on his/her device, and enter the relevant information required. After shopping online, the E-wallet automatically fills in the user’s information on the payment form. To activate the E-wallet, the user needs to enter his password. Once the online payment is made, the consumer is not required to fill the order form on any other website as the information gets stored in the database and is updated automatically.



e-cheque

An electronic version or representation of a paper cheque. The account holder writes an e-check (or e-cheque) using a computer or other type of electronic device and transmits the e-cheque to the payee electronically. Like paper cheques, e-checks are signed by the payer and endorsed by the payee. Rather than handwritten or machine-stamped signatures, however, e-checks are affixed with digital signatures, using a combination of smart cards and digital certificates. The payee deposits the e-check, receives credit, and the payee's bank clears the e-check to the paying bank. The paying bank validates the e-check and then charges the cheque writer's account for the cheque.

If you have linked your bank account but not a credit card, you can send money using your PayPal balance or an eCheque. If you have both a bank account and credit card linked to your account, your payments will be sent via Instant Bank Transfer.

To send an eCheque:

1. Go to Send and Request.
2. Select the type of payment.
3. Enter the required information.
4. Click Continue.
5. Click Change under “Payment Method”.
6. Select eCheque.
7. Click Continue.
8. Review the information and click Send Money to complete the transaction.

ATM (Automated Teller Machine)

An **automated teller machine (ATM)** or cash machine (British English) is an electronic telecommunications device that enables customers to perform financial transactions, such as cash withdrawals, deposits, funds transfers, or account information inquiries, at any time and without the need for direct interaction with bank staff.

How to Use an ATM

1. Safety First

The first thing to remember when using an ATM is to be safe. That machine has direct access to our bank account, and we might have a lot of cash on hand immediately before or after we use the ATM. For those reasons, thieves target ATMs and the people using them. Be aware of our surroundings, and don't use an ATM if anything looks suspicious.

2. The Card Reader

Once we've determined that an ATM is safe to use, insert our card into the card reader. There should be an image of a card showing us exactly how the card needs to be inserted. Look for the black magnetic stripe for guidance, or possibly an image showing how your name and card number should be lined up.

In some cases, we'll insert the card completely into the ATM, and the machine will hold onto it until our transaction is complete. Other machines allow us to just "dip" our card quickly so that we can get it back in our wallet as soon as possible. If the machine holds onto our card, make sure to get the card back before leaving the machine.

3. Enter PIN

Next, we'll have to enter our personal identification number (PIN) to prove that we are an authorized card user. As we learn how to use an ATM, develop the habit of hiding the keypad as we type in our PIN (use our free hand to cover our typing). Somebody might be watching you, and some thieves even install hidden cameras on ATMs to capture PINs.

4. Choose a Transaction

We can use an ATM to do several different things, so we'll have to tell the machine what we want to do. Getting cash is easiest, but we can eventually learn how to use an ATM for other transactions.

Withdrawals are the most common way to use an ATM—we simply get cash out of our account. For a withdrawal, we'll just indicate how much we want to take out.

Deposits can also be made at most ATMs. We can deposit cash and checks if our bank has a partnership with the ATM we're using. However, there are some risks to ATM deposits, so we should strongly consider making deposits with our mobile device as an alternative.

Balance inquiries show us how much money us have. Selecting this option will display our current account balance. This might be helpful if you need to know how much you can spend with your debit card.

Transfers and payments might also be available, depending on our bank. This option allows us to use the money in one of our accounts (without physically withdrawing cash).

5. Fees

If we're using an ATM that is *not* affiliated with our bank, we may have to pay a fee. ATMs display this fees before the transaction is complete, allowing us to back out if we don't want to pay the fee. However, the ATM only shows the fee that it charges. Our bank might also charge additional fees.

To avoid fees, it's always best to use an ATM that is owned by or affiliated with our bank.

6. Receipt?

If we want a written record of our transaction. In most cases, receipts are unnecessary, and they pose a potential security risk. If we throw the receipt away in a public space, somebody else could see our account information such as the amount we withdrew, or how much cash we have in your account.

There are times when we should take our receipt. For instance, if we deposit a check at an ATM, keeping our receipt is a good idea until the funds land in our account.

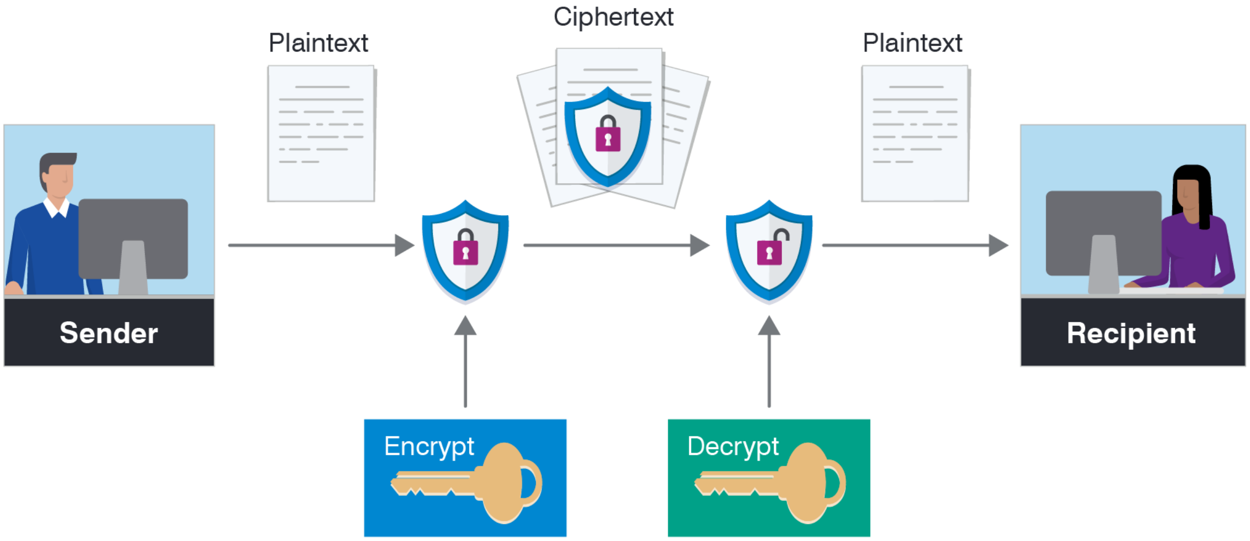
7. Finish Up

Once we've done what we need to do, close out our session with the ATM. Make sure that the machine is not waiting for us to perform another transaction. If we walk away before our session is closed, somebody could theoretically walk up behind us and withdraw cash from our account.

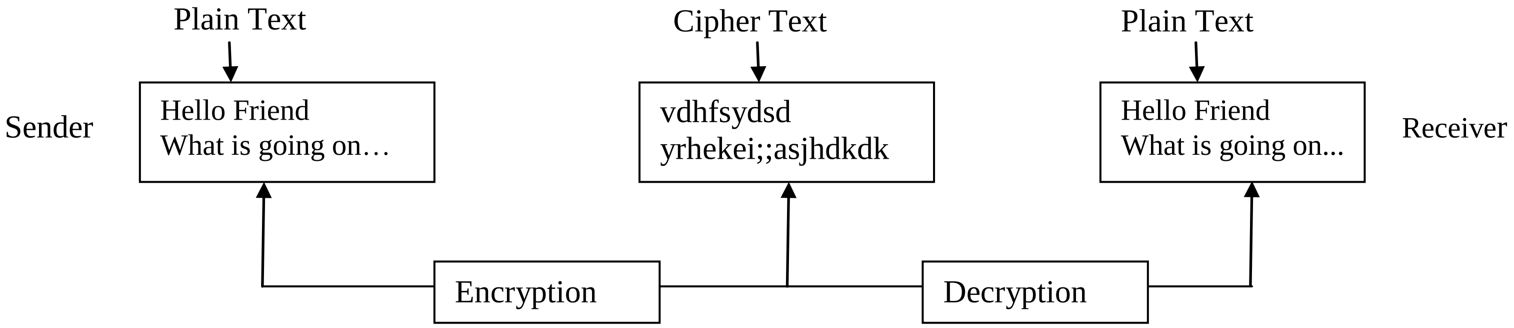
Encryption mechanism

Encryption is the method by which information is converted into secret code that hides the information's true meaning. This method of encrypting and decrypting information is called *cryptography*.

Unencrypted data is also known as plaintext, and encrypted data is called *ciphertext*. The formulas used to encode and decode messages are called *encryption algorithms*, or ciphers.



Encryption



Encryption has been a longstanding way for sensitive information to be protected. Historically, it was used by militaries and governments. In modern times, encryption is used to protect data stored on computers and storage devices, as well as data in transit over networks.

Importance of encryption

Encryption plays an important role in securing many different types of information technology (IT) assets. It provides the following:

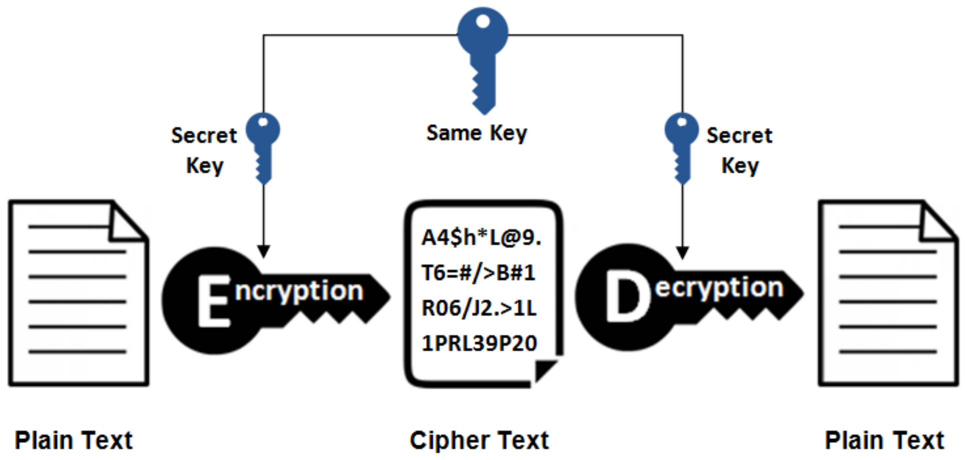
- **Confidentiality** encodes the message's content.
- **Authentication** verifies the origin of a message.
- **Integrity** proves the contents of a message have not been changed since it was sent.
- **Non-repudiation** prevents senders from denying they sent the encrypted message.

Encryption Methods

At the beginning of the encryption process, the sender must decide what cipher will best disguise the meaning of the message and what variable to use as a key to make the encoded message unique. The most widely used types of ciphers fall into two categories: **symmetric** and **asymmetric**.

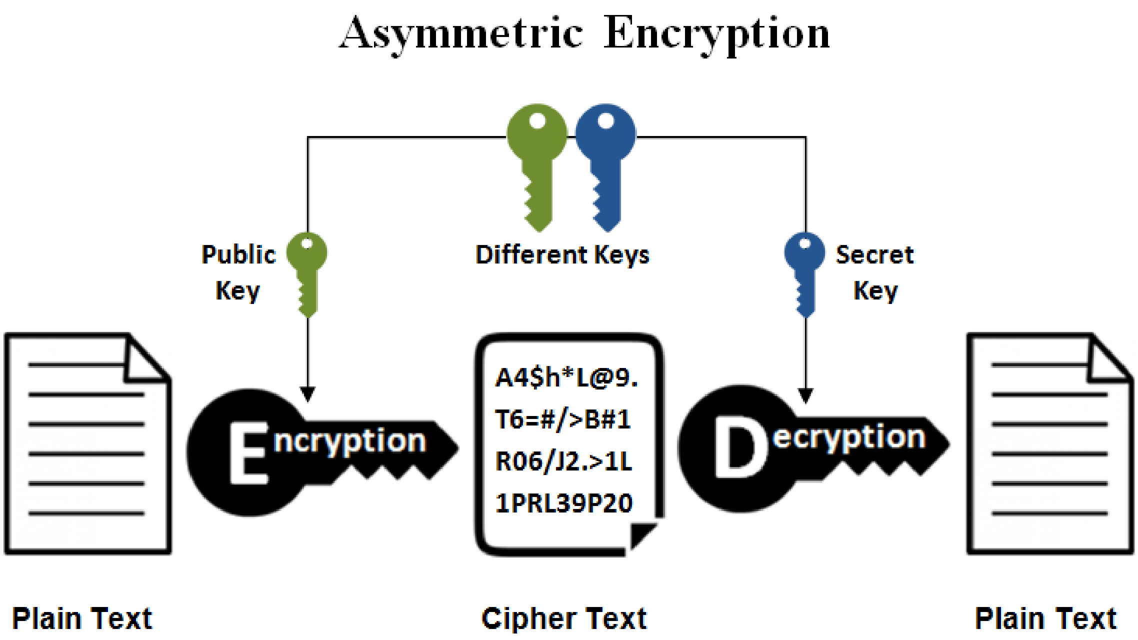
Symmetric Encryption- also referred to as ***secret key encryption.*** It is a type of encryption where only one key (a secret key) is used to both encrypt and decrypt electronic information. The entities communicating via symmetric encryption must exchange the key so that it can be used in the decryption process. This encryption method differs from asymmetric encryption where a pair of keys, one public and one private, is used to encrypt and decrypt messages.

Symmetric Encryption



By using symmetric encryption algorithms, data is converted to a form that cannot be understood by anyone who does not possess the secret key to decrypt it. Once the intended recipient who possesses the key has the message, the algorithm reverses its action so that the message is returned to its original and understandable form. The secret key that the sender and recipient both use could be a specific password/code and it can be random string of letters or numbers that have been generated by a secure random number generator (RNG).

Asymmetric Encryption- also known as ***public key encryption***. Asymmetric encryption makes use of a key-pair which constitutes of a **private key** a mathematically associated **public key.** Asymmetric cryptography offers better security because it uses two different keys .One key i.e. public key encrypts data, and then the other key i.e private can decrypt that data. This type of cryptography often uses prime numbers to create keys since it is computationally difficult to factor large prime numbers and reverse-engineer the encryption.


Asymmetric Encryption
Different Keys
Public Key
Secret Key
Encryption
A4$h*L@9.
T6=#/>B#1
R06/J2.>1L
1PRL39P20
Decryption
Plain Text
Cipher Text
Plain Text