SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE
www.sathyabama.ac.in

SCHOOL OF MANAGEMENT STUDIES

UNIT – I- MANAGING EBUSINESS – SBAA 7033

I INTRODUCTION

Ecommerce, also known as **electronic commerce** or internet **commerce**, refers to the buying and selling of goods or services using the internet, and the transfer of money and data to execute these transactions.

Ebusiness Defined

The United States Census Bureau defines ebusiness as "any process that a business organization conducts over a computer mediated network. Business organizations include any for profit, governmental, non-profit entity.

Their processes include production-, customer-, and internal or management-focused business processes." In a shorter broader sense, ebusiness is the process of conducting business electronically or over the internet.

Electronic mail is e-mail, electronic commerce is e-commerce, and following this formula, electronic business is e-business. Every time business is conducted over the internet, e business takes place, and as the internet grows, so grows ebusiness. Electronic business (e-business) can be defined as the use of the internet to network and empower business processes, electronic commerce, organizational communication and collaboration within a company and with its customers, suppliers, and other stakeholders.

E-businesses utilise the internet, intranets, extranets and other net- works to support their commercial processes. Electronic commerce (e-commerce) is the buying and selling, marketing and servicing of products and services via computer networks. Since e-business includes the process of transacting with suppliers and customers there is an overlap in activities with e-commerce.

Although the terms ‘e-business’ and ‘e-commerce’ are often used synonymously, the distinction between them lies in the broader range of processes in e-business that incorporates internal transactions within an organisation. These include transactions relating to procurement, logistics, supply chain management, payments, stock control and order tracking. As Chaffey (2004) notes, e-commerce can best be conceived as a subset of e-business. Where the two concepts overlap is in the buying and selling of products and services.

Where does ebusiness take place?

Ebusiness is offered to all users via the internet, to internal users via an intranet (similar to the internet, an intranet is a smaller network of computers usually within a single organization), and to specified users via an extranet (an intranet partially accessible to specified users from outside an organization via a valid username and password).

Three Main Types of E-business

1. **Business to Consumer (B2C)**

The most widely recognized form of ebusiness, B2C is the exchange of information, products, or services taking place between a business and a consumer over the internet. As the internet develops, B2C is continually changing the way consumers acquire information, the way products are compared against one another, and the way in which they are purchased.

An example of a B2C only site is Amazon.com. AE.com is an example of a B2C site with a physical location as well.

2. **Business to Business (B2B)**

The largest form of ebusiness in terms of money spent is B2B. Business-to-business allows trading to take place between businesses using a low-cost sales channel for the sale of goods and services, and is responsible for constantly changing corporate buying habits.

An example of a B2B site would be a car part company selling parts to a car dealership—another company—rather than directly to consumers.

3. **Business to Government (B2G)**

B2G is the online exchange of information and transactions between businesses and government agencies, also known as egovernment. B2G allows government agencies and businesses to use electronic means to conduct business and interact with each other over the internet.

An example of a B2G site would be one that offers electronic tax filing.

Ecommerce and its Relation to Ebusiness

The United States Census Bureau defines ecommerce as "any transaction completed over a computer-mediated network that involves the transfer of ownership or rights to use goods and services. Transactions occur within selected e-business processes (eg. selling process) and are 'completed' when agreement is reached between buyer and seller to transfer ownership or rights to use goods or services." So while ebusiness covers the entire range of online business dealings (from customer service to selling), ecommerce refers specifically to one entity paying for goods or services from another entity via the internet.

Network software encompasses a broad range of **software** used for design, implementation, and operation and monitoring of computer **networks**. ... With the advent of **Software** – Defined **Networking** (SDN), **software** is separated from the hardware thus making it more adaptable to the ever-changing nature of the computer **network.**

E-business varies in scope and type of activities undertaken. The entire supply chain of many industries has been radically transformed by the development of the internet and related technologies. Some organisations specialise in business-to-business (B2B) activities by providing e-business services across the supply chain or in parts of the supply chain such as e-procurement,

logistics, stock control, ordering, payments and distribution.

E-business also includes the organisation of collaboration platforms that allows different organisations to share information and knowledge for mutual benefit, i.e. the organisation of e-marketplaces that bring organisations together for buying and selling products and services or providing an online business support service.

The most high profile types of e-business involve those that sell products or services to customers. The business-to-consumer (B2C) sector has attracted the highest number of entrants as well as some of the most successful e-business ventures such as Amazon.com, e-Bay and Friends Reunited. The latter two also incorporate a consumer-to- consumer (C2C) element to their service by bringing consumers together for specific purposes.

Most organisations now have a website that is used for promoting the activities of the business or marketing their products and services. More and more traditional firms are creating their own e-business and e-commerce websites to offer an additional sales channel for their customers (Tesco.com, marksandspencer.com).

There is a large industry sector that supports e-business, including Internet Service Providers (ISPs) such as Yahoo!, Google and AOL. These organisations run a number of services including internet access and search engines and have built up enormous databases of websites that form the basis of their search engine.

Organisations who want to have their websites on the search engine pay an amount relative to the prominence on the list. Other organisations specialise in providing applications software for facilitating e-business or sell hardware such as computers and modems (Dell, Compaq, IBM).

There are many thousands of businesses that specialize in maintaining and supporting e-businesses, including computer analysts, IT specialists, software consultants, applications consultants, computer trainers, security consultants and so on. The development and maintenance of the network infrastructure is a vital industry for ensuring high quality access to internet services and includes some of the world's biggest and most complex organisations such as BT and Cisco.

The most significant factor that transformed the internet into a global communications phenomenon was the development of the World Wide Web (WWW) in the early 1990s. This extended the functionality of the internet by introducing hypertext that linked documents on the internet servers. This facilitated access to particular parts of documents or even to other relevant documents held on other servers. This was called the hypertext transfer protocol (HTTP) and derived from a mark-up language called hypertext markup language (HTML). Within the servers, each document, or pages within documents, are given a unique address. The addresses are termed universal resource locators (URL's). The ability to access pages, documents and servers from many different websites created a network of interconnectivity and gave rise to the term the World Wide Web

The Web was the catalyst for huge changes in the business environment as more and more firms sought to integrate their traditional business models with those online. By the mid 1990s firms'born on the net' emerged, whose function was to exploit the opportunities in the marketplace by using the internet. However, the key driver of the phenomenal rise of the internet was the rapid increase in the use of computers with access to the internet and the Web by the public.

From 1993 to 1996 the number of computer users with access to the internet and the Web rose from zero to 10 million. In 2004 the figure stood at around half a billion. Also, the number of websites appearing on the Web has increased exponentially from 1993 onwards. In the months following the releases of HTTP and HTML there were less than 50 websites in existence. By the end of the decade there were countless millions available.

Since the commercialization of the internet in the mid 1990s demand for its use has increased hugely each year. In fact, the growth of the internet has been such that there are fears that the existing infrastructure may be unable to sustain demand into the future. The internet has had a profound effect at so many different levels including individuals, society, business, governments, education, health, security services, entertainment, news services, financial markets and many others.

To comprehend the staggering growth of the internet many analysts turn to the prediction of the founder of Intel and inventor of the chip, Gordon Moore. In the mid 1960s Moore predicted that the number of components that could be located on a single chip would double every twenty-four months.

In the twenty years between 1974 and 1994 the Intel 8080 chip increased the number of transistors from 5000 to over 5 million. This exponential growth phenomenon became known as Moore's law and can easily be related to the growth witnessed in demand for access to information technology in general, and the internet in particular. The internet has created a new communications channel and provides an ideal medium for bringing people together cheaply, efficiently and for a wide range of different reasons. It has also presented opportunities and challenges for the business community.

As consumers become more knowledgeable about using the internet to service their needs and wants so the business community has been boosted by the potential the internet presents for extending markets, developing new products and services and achieving a competitive advantage and profitability. New markets quickly emerged based on applications of the internet, most prominently the business-to-consumer (B2C) and business-to-business (B2B) sectors.

One of the key characteristics of e-commerce is the ease of entry for firms. The cost of entry and exit is low relative to traditional industries, as firms do not require large sales teams, costly investment in infrastructure or high sunk costs in order to compete effectively. Rising connectivity rates among potential customers ensures increasing competition among e-commerce firms as more are attracted to the source of potential revenue. Importantly, the internet does away with geographical boundaries thereby increasing yet further the extent of competitive rivalry. Intense competition is a characteristic of the internet economy and has spread across all e-business and e-commerce sectors.

Framework for business models

Business models are designed to help firms add value to customers and achieve their stated objectives. To succeed, firms need to under- stand their external environment, utilise their resources effectively and build distinctive capabilities that leverage competitive advantage over rivals. Figure 3 illustrates the process linking a business model with competitive advantage.

Developing and implementing business models help firms to compete in a marketplace.

Analyzing the business model helps firms identify what activities in the value chain contribute to profit and help create a competitive advantage. The effectiveness of a business model is determined by the ability of firms to exploit market opportunities, match or exceed customer expectations and achieve stated aims and objectives. Lee (2001) sets out the key characteristics of a viable e-commerce model.

Firms must:

- Design programs that take advantage of the internet network effects and other disruptive attributes to achieve a critical mass of installed customer base;
- Leverage on a single set of digital assets to provide value across many different and disparate markets;
- Build trust relationships with customers through e-business communities to increase their costs of switching to other vendors;
- Transform value propositions and organisational structures for enhanced value creation; and generate synergy effects on e-commerce product and service offerings.
- In developing and implementing an e-business model firms must meet three critical success factors.
- Understand and exploit the e-market space characteristics;
- add value to customers and achieve economic viability.

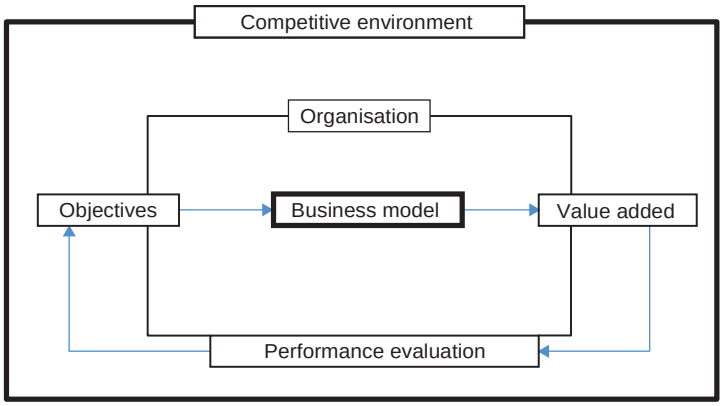


Figure 3. A framework for analysing e-business models

What is E-commerce? Explain advantages and disadvantages of E-Commerce.

Electronic commerce, better known as E-commerce, refers to the commercial activities—such as on-line shopping and payment transactions—carried out using computers and the Internet.

Advantages and disadvantages of E-Commerce:

E-commerce covers the global information economy, which includes electronic trading goods and services, electronic fund transfer, online procurement, direct marketing and electronic Billing. E-commerce provides the procedures or the ways for generating profits by increasing the number of transactions.

Some of the main advantages of E-commerce are as follows:

Increased access:

E-commerce has made it easier for businesses to reach people around the world and run their operation without approaching their suppliers directly. E-commerce businesses provide access to the consumers and the other businesses all over the world

Reduces competitive gap:

E-commerce reduces marketing and advertising expenses. So, smaller companies can also compete on quality, price and availability of goods with the bigger companies.

Reduced sale cycle:

The customers access the product listing and the pricing directly from the Internet without any phone calls and e-mails.

Reduced cost of business:

E-commerce reduces the effort required to do business. It reduces the amount of manpower required, inventory costs, purchasing costs and order processing costs associated with faxing, phone calls and data entry.

Easy business administration:

With the use of efficient software, most of the business-related tasks can be done automatically. Business processes like storing of inventory levels, shipping and receiving logs and other business administration processes are automatically stored.

Better payment system:

With the advancement in payment technologies, E-commerce allows encrypted and secure payment facilities on-line.

Reduced burden on staff:

E-commerce simplifies the customer service and sales support tasks , thus relieving the staff from one of their job responsibilities.

Medium to grow business:

E-commerce serves as a medium for start-up, small- and medium-sized companies to reach the global market.

Network production:

E-commerce allows parceling of the production process to the contractors who are geographically separated but are connected through the Internet. This helps in selling of add-on products, services and new systems.

Disadvantages:

E-commerce has helped customers to find the required product in an easy way. But, there are some difficulties that exist in the use of E-commerce. Some of the most common difficulties are as follows:

It is difficult to decide the criteria on which taxes should be charged on the selling of goods over the Internet in case the business and the customer are in different states. It would be unfair to collect taxes from businesses whose products are not marketed over the Internet and to allow businesses selling their products over the Internet not to pay any tax

The issue of security is another major area of concern on E-Commerce. The security issues concerning personal and financial information about a customer still exists even with the improvement of data encryption techniques.

The cost that is involved in the development and deployment of the E-commerce application is very high.

Some protocols are required to develop some specific E-commerce applications that are not standardized around the world. The deployment of such applications over the Internet required that these protocols should be available on the client side.

The integration of E-commerce infrastructure with the present organizational Information technology system is difficult. The technologies used in the development of an E-commerce application in an organization may be different from that of the presently existing application used in -the organization.

Explain the Architecture of E-Commerce.

E-commerce is based on the client-server architecture.A client can be an application, which uses a Graphical User Interface (GUI) that sends request to a server for certain services.The server is the provider of the services requested by the client.

In E-commerce, a client refers to a customer who requests for certain services and the server refers to the business application through which the services are provided.

The business application that provides services is deployed on a Web' server.

The E - Commerce Web server is a computer program that provides services to "other computer programs and serves requested Hyper Text Mark-up Language (HTML) pages or files. In client-server architecture, a machine can be both a client as well as a server.

There are two types of client server architecture that E-commerce follows: two-tier and three-tier.

E- Commerce System Architecture: Two-tier architecture:

In two-tier client-server architecture the user interface runs on the client and the database is stored on the server. The business application logic can either run on the client or the server. The user application logic can either run on the client or the server. It allows the client processes to run separately from the server processes on different computers.

The client processes provide an interface for the customer that gather and present the data on the computer of the customer. This part of the application is known as presentation layer. The server processes provide an interface with the data store of the business.

this part of the application is known as data layer. The business logic, which validates data, monitors security and permissions and performs other business rules, can be kept either on the client or the server. The following Figure shows the e commerce system two-tier architecture diagram.

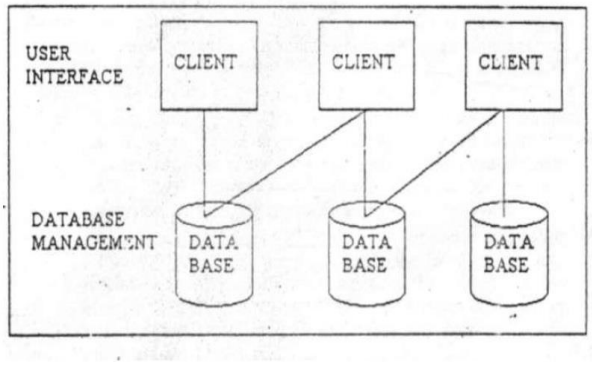


Figure 1 Architecture diagram

Components of E-Commerce.

The technology and infrastructure used to develop the E-commerce application is the key to its success.The hardware and software must be selected in such a way that they can fulfill the needs of the E-commerce application.

The following figure shows the components involved in

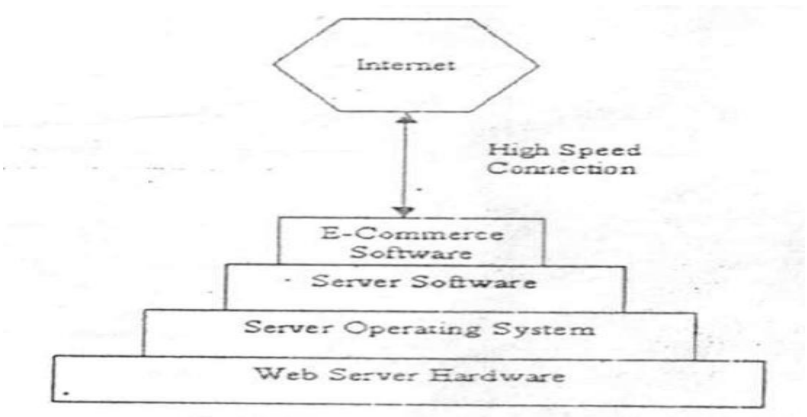


Figure 2. E-commerce infrastructure.

Hardware:

A Web server hardware platform is one of the major components of the Ecommerce infrastructure on which the performance of the whole E-commerce application depends.While selecting Web server hardware, the software that will run on the server of the E-commerce transactions to be processed must be considered.

The amount of the storage capacity and the computing power required depend on the volume of the E-commerce transaction to be processed.

If the exact requirements are not known in advance, then the hardware configuration should be highly scalable so that they can be upgraded to meet the requirements.

E - Commerce Softwares

Software is the main component that implements the E-commerce services and functionality. Software for E-commerce can be categorized in the following two types

Web server software:

Web server software is required in addition to the Web server operating system software.

It is used to implement some extra functionality such as security and identification and retrieval and sending of Web pages.

Web server software creates a Web log file that identifies things such as the URL of the visitor, the length of the visit and the search engine and the key words used to find the site.

Web server software includes website development tools such as HTML editor and Web pages.

E-commerce softwares:

With the growth of E-commerce, many applications have emerged— for example, the electronic shopping cart that tracks the items selected for purchase and their costs.

Typical E-commerce software must support the following processes:

Catalog management:
It is required to deliver the customized content to the screen or the GUI used by the customer.

The software used for catalog management combines the different product data formats into a standard format for viewing, aggregating and interacting catalog data into a central store.

Product configuration:
The Web-based product configuration software allows the user to build the product to their specifications without the intervention of the salespeople.

For example, Dell Computers and CISCO systems use configuration software to sell build-to-order and network processes to their customers over the Internet.

Shopping cart

A model known as shopping cart is used by Ecommerce sites to track the items that are selected for purchase; the shopping cart allows customers to view all the items selected by them.

The customers can add new items and remove the previously selected items from the shopping cart.

Transaction processing:
E-commerce transaction processing is used to process the data received from the. Shopping cart and to calculate the total cost of the purchase.

Explain different applications of E-Commerce.

Advantages of using e commerce in business are motivating lot of businesses to use E-Commerce for their business. Various business areas such as retail, wholesale and manufacturing are using E-Commerce.

The most common Applications of E-commerce are as follows:

Retail and wholesale:

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.

Marketing:
Another application e-commerce is Marketing.

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.

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.

Another application of E-commerce is on-line stock trading. Many Websites provide access to news, charts, information about company profile and analyst rating on the stocks.

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.

EDI

Electronic Data Interchange (EDI) is the computer-to-computer exchange of business documents in a standard electronic format between business partners.

Business-to-business (B2B) exchanges or marketplaces provide dramatic opportunities to automate collaborative business processes with customers and suppliers, generate internal efficiencies, and reach new markets at minimal cost. The landscape is littered with hundreds of B2B exchanges that have failed, demonstrating that success is far from automatic. But many are still operating. They have learned how to take advantage of the opportunities and avoid the pitfalls of this dynamic new marketing channel.

B2B exchanges are online marketplaces for businesses to buy and sell good and services from other businesses. Automated business-to-business transactions are not an entirely new concept. Large organizations have been using automated systems for a number of years, and some have been programmed to exchange business transactions with other automated systems as far back as the early nineties. For example, General Electric's Aircraft Engines division had a system with which a customer could order a part, initiate the shipping process, be invoiced, and pay for the part, all without a single piece of paper and within a span of 45 minutes.

However, these systems needed dedicated, expensive data communication facilities and required significant investments in large, complex software to be developed from the ground up before they even started working. The Internet brought down the cost and the technological barriers.

The simpler business-to-consumer (B2C) model beat B2B to the punch in wide availability and visibility. Business based on the B2C model, in which the customer browses through an electronic catalog to select items for purchase, is well established at this time. Yet, the potential in terms of dollar volume and number of transactions, however, is far higher for B2B even than B2C.

This is because a chain of transactions involving material suppliers and service providers lies behind every product that reaches the consumer. B2B transactions typically involve long, complex processes including searching for vendors, requests for quotation, evaluating different proposals, negotiation, supply chain planning, shared product design, document exchange, billing, payment

and extensive data analysis. As a result, B2B exchanges can go far beyond simply streamlining buying and selling: They can create customer-driven value chains that substantially reduce costs for both buyer and seller, better align the entire supply chain with the customer's needs. They can also make it possible to enter new global markets at minimal cost and substantially reduce the time required to respond to changes in demand patterns.

Types of exchanges

B2B exchanges can generally be divided into three basic categories. Consortia are typically formed by a group of leading vendors in a particular industry, like Global Food Exchange. Public exchanges such as Commerce One are run by a third party, and are open to all companies that meet the standards defined by the exchange. Private marketplaces are run by a single company and its key suppliers, such those sponsored by Walmart and Dell. Another way to classify exchanges is as either vertical--which specialize in serving one particular industry -- or horizontal -- servicing a broad range of industries, like PurchasePro.

Most of the first generation of B2B exchanges were open, public marketplaces whose business model was based on a small percentage fee on all transactions conducted. Wall Street did the math, noting that the total B2B marketplace is perhaps 10 times larger than the consumer marketplace because of all the intermediate transactions that are involved in bringing products to market. The result was that money from venture capital and even initial public offerings flowed freely--resulting in a large number of start-ups.

But many of these companies quickly failed because they were not able to attract paying suppliers and customers. The research firm IDC says that of the approximately 1,000 B2B marketplaces that were launched only about 700 are currently active. There are two main reasons. First, the adoption of e-commerce has generally been somewhat slower than expected. Even more important, major players in most industries have formed their own exchanges rather than giving up a percentage of their sales. The exchanges that have been successful have largely been private exchanges that gain their revenues through a variety of different means Transaction fees are still a factor, but they are usually at a much lower rate than originally expected and are often in effect paid by companies to themselves as the owners of the exchange. Other revenue sources include membership fees paid for access to the marketplace's members and fees paid for the software that is necessary to connect to some of the exchanges.

Basic development options

The ideal development strategy is deeply influenced by whether the exchange is started by a new company or to serve an established firm. A start-up company does not inherit any business rules and complex processes; some of these may exist more for historical than purely business reasons. It is able to develop the application in a cleaner fashion, and implement it on a single, most effective platform. A start-up is also under heavy pressure to bring its offering to the market quickly to gain the first-mover advantage. The clean slate that it starts with also means that the knowledge of the intricacies of the business process of the industry is not available for the company to build on. In the B2B space, no application can stand entirely on its own: it must exchange data and transactions with other, related systems. A start-up does not have such a base of interrelated systems to count on. It must therefore build the application in such a way that it can interface with a wide variety of existing systems. While the application is built on a clean business model, it must also build generalized interfacing capabilities.

An innovative example

Another example of an innovative e-business exchange initiative is TexYard.com, the online sourcing solution for the European apparel industry. TexYard.com brings buyers and suppliers together in a neutral trading environment to make the process of apparel sourcing easier, faster and more efficient. Buyers can put their complete sourcing process online to lower their administrative costs, obtain the best possible price and accelerate the time to market. Buyers can also use a comprehensive database to find, investigate, and start working with new suppliers from around the world. Suppliers can gain access to major European retailers, expand their customer base, and increase their business opportunities. Suppliers can market their services and products, and lower their cost of doing business. Accommodating both forward and reverse auctions, the exchange allows buyers to define full details of an upcoming production contract--from technical specifications and quality measures, through to shipping and delivery instructions--and get bids on these contracts.

The time spent communicating requests, comparing quotes, and negotiating prices is drastically reduced.The team that developed TexYard.com used Cold Fusion with an Oracle database to develop the application. This application is believed to provide the most sophisticated RFQ (Request For Quotation) process ever created by a trading exchange. It was needed to account for the many complexities involved in purchasing textiles. The project was managed and developed by a global team in five locations with 35 members including a project manager, six business and systems analysts, two XML developers, 25 application programmers and a test and a production support professional.

This arrangement allowed for an around-the-clock project schedule that dramatically reduced time to value. The developers in India handed off the code for testing at the end of their day and, by the time they came in the next morning, the testing group had a new set of issues for them to address. As a result, the exchange got to market early with relatively low development costs. It has been successful in attracting customers and suppliers and recently obtained a new round of financing.

What is the future of B2B exchanges? We foresee an environment in which buyers and sellers are interconnected by exchanges that provide instantaneous information to decision-makers in enterprises as well as consumers. Consider the potential impact on the economy. Most recessions are caused by inventory buildups that in turn are caused by lack of information about the intentions of purchasers as well as the time lag involved in passing information up and down the decision supply.

Business data traveling over a public network such as the Internet can be intercepted on the way. To secure the data against such theft, it is coded before transmission and decoded when received. The encryption/decryption is implemented with public key systems in which each party has a pair of related keys -- a public key that is published to all partners and a private key that is kept secret. The public and private keys are mathematically related to each other in such a way that computing the private key from the public key requires so much computing power as to make it impossible for all practical purposes. One approach is to establish a secure communications channel by using one of several protocols such as secure sockets layer (SSL) that operate as a layer above the standard Internet TCP protocol.

Another approach to ensuring the privacy of communications, which can be used in place of or in combination with a secure protocol, involves transmitting a message in a secure form so that it

cannot be opened or read by another party. Public key infrastructures (PKIs) provide the supporting services that are needed when public-key-based technologies are used on a large scale. A PKI deployment might typically consist of a certificate authority that creates the certificates and a certificate repository to provide distributed access to certificates.

What is Telnet?

- A program that allows one system to log in to a remote host on a TCP/IP network.
- Users must have valid user names and passwords before accessing the remote system.
- Telnet sends all messages in clear text and has no specific security mechanisms.

Distinguish between Internet and Intranet.

Internet

1. Internet is wide network of computers and is open for all.
2. Internet itself contains a large number of intranets.
3. The number of users who use internet is Unlimited.
4. The Visitors traffic is unlimited.
5. Internet contains different source of information and is available for all.

Intranet

1. Intranet is also a network of computers designed for a specific group of users.
2. Intranet can be accessed from Internet but with restrictions.
3. The number of users is limited.
4. The traffic allowed is also limited.
5. Intranet contains only specific group information.

What is the main purpose of E-mail.

Email is a Store and Forward mail service allows users to communicate throughout the network, requiring only a target address and a point of access.

Write down the applications of E-commerce?

1.Electronic fund transfer.
2.Enterprise integration.
3.computer supported collaborative work.
4.Government regulatory data interchanges

10.Write down the benefits of Electronic web commerce

1.Reduced costs to buyers from increased competition.
2. reduced costs to suppliers by electrically accessing on-lne databases of bid opportunites.
3. Reduced errors, time and overhead costs in information processing by eliminating requirements for reentering data.
4. Creation of new markets through the ability to easily and cheaply reach potential customers,

11.What are the open issues related to E-commerce?
1.Taxation
2.Customs
3.Regulation
4.Fraud
5.security.

12. Mention the types of software packages that make up an EDI terminal on a PC?
1. Application software.
2.Message Translator.
3.Routing manager.
4.Communication handler.

13.Give the modes of Electronic commerce
1.Business to business
2.Business to consumer.
3.consumer to consumer.

14.Mention the revenue opportunities for web commerce?
1.Technical and consulting services.
2.Merchandising products information.
3.Transport services.
4.directory services.
5.Content creation.
6.Subscriptions
7.Access services.
8.Advertising services.
9.Hosting of web sites.

What are the additional applications of E-commerce.
1.Retail & wholesale.
2.Marketing.
3.Finance.
4.Manufacturing.
5.Auctions

List the common elements of B2B exchange?
1.based around a specific industry sectors-Petroleum industry is an example. Those help buyers source goods and services that are largely specific to industries.
2.based around products and services-Examples include the marketplaces for maintenance, repair and operating (MRO) goods such as safety and office supplies.
3.focused on the functions-HR departments manage employee benefits; help companies dispose of excess inventory and so on.

Give any TWO examples of B2C model.

1.Facebook
2.Amazon
3.Twitter
4.Uber

Define Intranet.

- An intranet is a secure and private enterprise network that shares data of application resources via Internet Protocol (IP).
- An Intranet differs from the internet, which is a public network.
- Intranet, which refers to an enterprise's internal website or partial IT infrastructure, may host more than one private website and is a critical component for internal communication and collaboration.

19.Define Gopher.

- Gopher is an Internet service that allows the user to browse Internet resources using lists and menus.
- Gopher groups information resources by category.
- This is a tree branch approach to information searching
- While most conferences are completely open to the public,an increasing number are moderated that is the messages cannot be directly posted to the conference ,but are instead posted to a human moderator who chooseswhich message to display Where does ebusiness take place?

Ebusiness is offered to all users via the internet

- to internal users via an intranet (similar to the Internet, e.g (WWW)
- an intranet is a smaller network of computers usually within a single organization),
- E.g LAN, WAN,MAN
- specified users via an extranet
- (an intranet partially accessible to specified users from outside an organization via a valid username and password).

Who uses extranet?

- An **extranet** is a controlled, private network **that uses** the internet for secure collaboration and information sharing among internal team members,
- as well as a company's external contacts, such as customers, suppliers, partners, and other third parties.

What are the types of network software?

- **Network software** for communications includes email, instant message, teleconferencing and video conferencing applications.

Network software for security includes antivirus, spam filtering, firewall and data-access management applications

Differentiate the features in intranet and extranet

- A **local area network** (**LAN**) is a collection of devices connected together in one physical location, such as a building, office, or home.

Difference between Web 1.0, Web 2.0 and Web 3.0

Web 1.0

- the first generation of the web
- the websites built during this time was very very simple
- text and images doesn't have a high resolution
- internet speed is not as fast as what we have today web 1.0
- lasted from 1989 to 2005
- it was considered a read-only website
- actually it was known to be a static website,
  - where webmasters or web developer just published their content
  - online and users just passively received information
- writing your opinions about the post is not possible in web 2.0
-
- so the interaction between the web sites and
- the users were very very limited web 1.0
- search doesn't have the opportunity to make some comments with reactions or any kind of feedback

Web 2.0

Second phase of web development users are now able to interact not only on the website but also interaction among users web 2.0 facilitated the sharing of contents this feature flooded the world wide web with all types of contents things like fashion food, travel cooking music lifestyle fitness and health online courses history politics dominating when it comes to content

few examples of web 2.0 are Facebook ,Wikipedia,Twitter ,WordPress , Instagram and so web 2.0 users are now more involved to information being published in the Internet data that can be published in web 2.0 is more robust they not only text in images but also large files as videos can now easily be shared and circulated

Web 3.0

Web 3.0 is the third generation of **internet** services for websites and applications that will focus on using a machine-based understanding of data to provide a data-driven and

semantic **web**. The ultimate goal of **Web 3.0** is to create more intelligent, connected and open websites.

- Based on user's behavioral pattern your preferred products and services those things that you prefer will be on top of the list see unlike web 2.0
  - the things that are on top of your search result are basically the things that are most searched by most users on the Internet
- Web 3.0 is characterized by machine learning automation and artificial intelligence

Why domain name is used for?

- Domain names serve to identify Internet resources, such as computers, networks, and services,
- with a text-based label that is easier to memorize than the numerical addresses used in the Internet protocols.

A domain name may represent entire collections of such resources or individual instances.

What are the examples of domain?

- 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).

When a company (or a person) purchases a **domain** name, they're able to specify which server he **domain** name points to.

SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE
www.sathyabama.ac.in

SCHOOL OF MANAGEMENT STUDIES

•

UNIT II -MANAGING EBUSINESS – SBAA 7033

A firewall is a network security device that monitors incoming and outgoing network traffic permits or blocks data packets based on a set of security rules. Its purpose is to establish a barrier between your internal network and incoming traffic from external sources (such as the internet) in order to block malicious traffic like viruses and hackers.

Al analyzes incoming traffic based on pre-established rules and filter traffic coming from unsecured or suspicious sources to prevent attacks. Firewalls guard traffic at a computer's entry point, called ports, which is where information is exchanged with external devices. For example, "Source address 172.18.1.1 is allowed to reach destination 172.18.2.1 over port 22."

Think of IP addresses as houses, and port numbers as rooms within the house. Only trusted people (source addresses) are allowed to enter the house (destination address) at all then it's further filtered so that people within the house are only allowed to access certain rooms (destination ports), depending on if they're the owner, a child, or a guest. The owner is allowed to any room (any port), while children and guests are allowed into a certain set of rooms (specific ports).

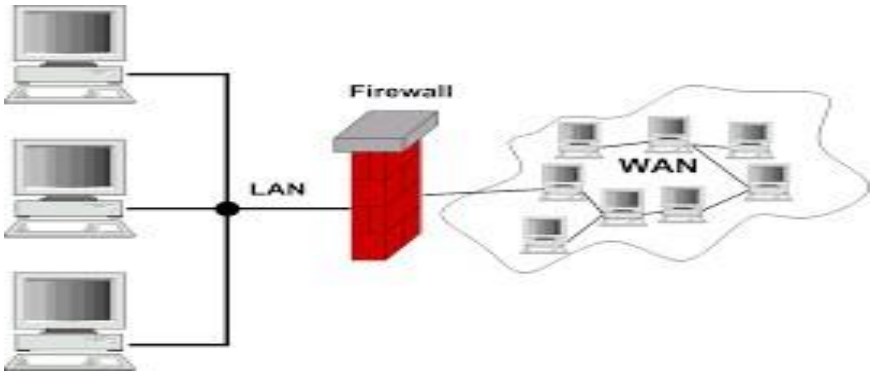


Figure 1 . Firewall encryption

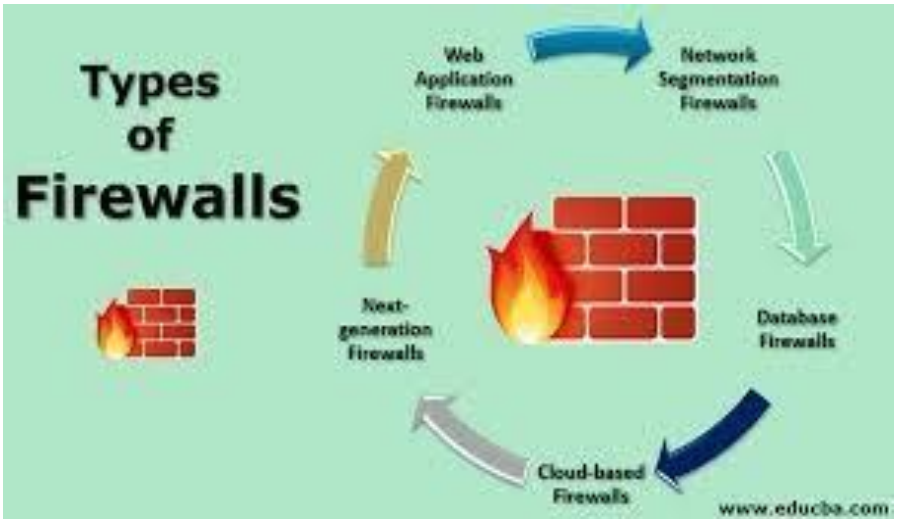


Figure 2 types of firewalls

All data packets entering or leaving the internal network pass through the firewall, which examines each packet and blocks those that do not meet the specified security criteria.

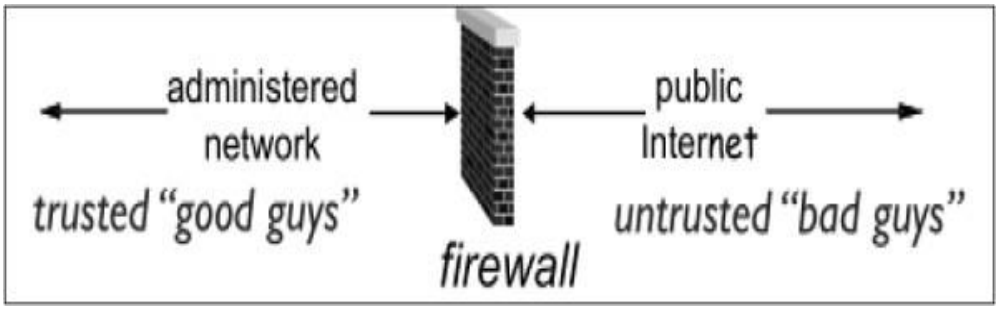


Figure 3 Firewall Encryption

Deploying firewall at network boundary is like aggregating the security at a single point is analogous to locking an apartment at the entrance and not necessarily at each door.

- Firewall is considered as an essential element to achieve network security for the following reasons −
- Internal network and hosts are unlikely to be properly secured.
- Internet is a dangerous place with criminals, users from competing companies, disgruntled ex-employees, spies from unfriendly countries, vandals, etc.
- To prevent an attacker from launching denial of service attacks on network resource.

To prevent illegal modification/access to internal data by an outsider attacker.

TYPES OF FIREWALL

Firewalls can either be software or hardware. A software firewall is a program installed on each computer and regulates traffic through port numbers and applications. While a physical firewall is a piece of equipment installed between your network and gateway.

- **Packet-filtering** firewalls.
- Circuit-level gateways.
- Stateful inspection firewalls.
- Application-level gateways (a.k.a. proxy firewalls)
- Next-gen firewalls.
- Software firewalls.
- Hardware firewalls.
- Cloud firewalls.

STATEFUL VS STATELESS.

Packet-filtering firewalls are divided into two categories: stateful and stateless.

- Stateless firewalls examine packets independently of one another and lack context, making them easy targets for hackers.
- In contrast, stateful firewalls remember information about previously passed packets and are considered much more secure.

In this type of firewall deployment, the internal network is connected to the external network/Internet via a router firewall.

The firewall inspects and filters data packet-by-packet. **Packet-filtering firewalls** allow or block the packets mostly based on criteria such as source and/or destination IP addresses, protocol, source and/or destination port numbers, and various other parameters within the IP header.The decision can be based on factors other than IP header fields such as ICMP message type, TCP SYN and ACK bits, etc.

Next-generation firewalls (NGFW)

- combine traditional firewall technology with additional functionality,
  - such as encrypted traffic inspection, intrusion prevention systems,
  - anti-virus, and more.
  - Most notably, it includes deep packet inspection (DPI).
  - While basic firewalls only look at packet headers, deep packet inspection examines the data within the packet itself,
    - enabling users to more effectively identify, categorize, or stop packets with malicious data

Proxy firewalls

Filter network traffic at the application level. Unlike basic firewalls, the proxy acts an intermediary between two end systems. The client must send a request to the firewall,

where it is then evaluated against a set of security rules and then permitted or blocked. Most notably, proxy firewalls monitor traffic for layer 7 protocols such as HTTP and FTP, and use both stateful and deep packet inspection to detect malicious traffic.

Network Address translation firewalls

- allow multiple devices with independent network addresses to connect to the internet using a single IP address,
- Keeping individual IP addresses hidden.
- NAT firewalls are similar to proxy firewalls in that they act as an intermediary between a group of computers and outside traffic.

Stateful multilayer inspection (SMLI) firewalls

- filter packets at the network, transport, and application layers, comparing them against known trusted packets.
- Like NGFW firewalls, SMLI also examine the entire packet and only allow them to pass if they pass each layer individually.
- These firewalls examine packets to determine the state of the communication
- (thus the name) to ensure all initiated communication is only taking place with trusted sources.

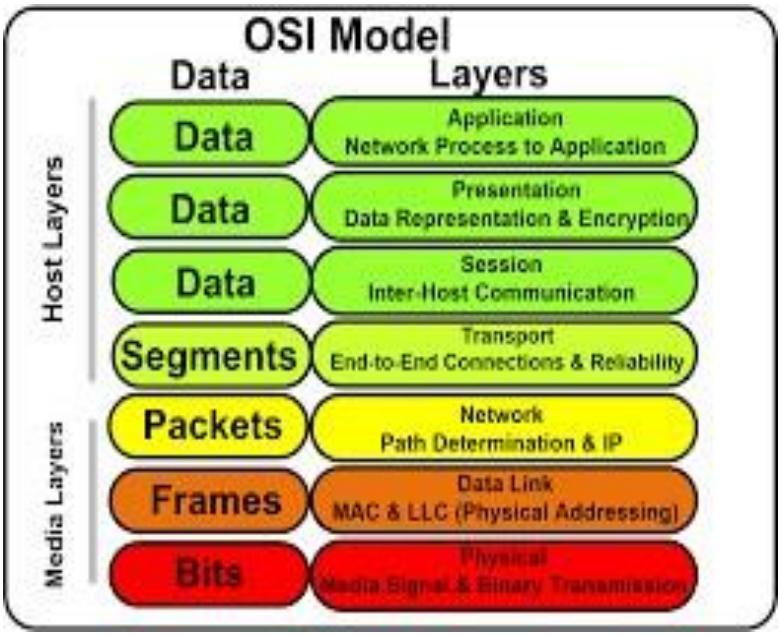


Figure 4 Protocol Layers

Email Protocols - POP3, SMTP and IMAP

Post Office Protocol version 3 (POP3) is a standard mail protocol used to receive emails from a remote server to a local email client. POP3 allows you to download email messages on your local computer and read them even when you are offline.

The Internet Message Access Protocol (IMAP) is a mail protocol used for accessing email on a remote web server from a local client. IMAP and POP3 are the two most commonly used Internet mail protocols for **retrieving emails**. Both protocols are supported by all modern email clients and web servers. While the POP3 protocol assumes that your email is being accessed only from one application, IMAP allows simultaneous access by multiple clients. This is why IMAP is more suitable to access mail from different locations or messaged are managed by multiple users.

By default, the IMAP protocol works on two ports:

- **Port 143** – this is the default IMAP non-encrypted port;
- **Port 993** – this is the port you need to use if you want to connect using IMAP securely.

Simple Mail Transfer Protocol (SMTP) is the standard protocol for **sending emails** across the Internet.By default, the SMTP protocol works on three ports:

- **Port 25** – this is the default SMTP non-encrypted port;
- **Port 2525** – this port is opened on all SiteGround servers in case port 25 is filtered (by your ISP for example) and you want to send non-encrypted emails with SMTP;

- **Port 465** – this is the port used if you want to send messages using SMTP securely.

Network Policies are sets of conditions, constraints and settings that

- allow you to designate who is authorized to connect to the **network**
- and the circumstances under which they can or cannot connect.

- During the authentication process,
- NPS verifies the identity of the user or computer that is connecting to the **network**.

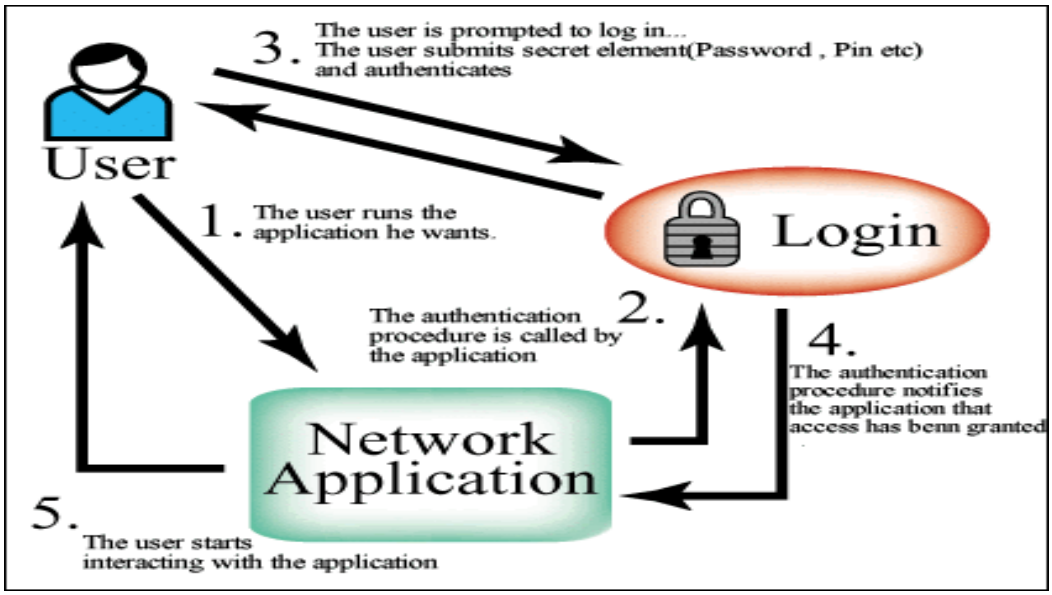


Figure 5 network application process

Security means safety as well as the measures taken to be safe or protected. Often this word is used in compounds such as a **security** measure, **security** check or **security** guard.

CIA Triad: These three letters stand for **confidentiality**, **integrity**, and **availability**,

Otherwise known as the CIA Triad. Together, these three principles form the cornerstone of any organization's security infrastructure.In fact; they (should) function as goals and objectives for every security program.

Encryption is a process which transforms the original information into an unrecognizable form. This new form of the message is entirely different from the original message. That's why a hacker is not able to read the data as senders use an encryption algorithm. Encryption is usually done using key algorithms. Data is encrypted to make it safe from stealing. Known companies also encrypt data to keep their trade secret from their competitors.

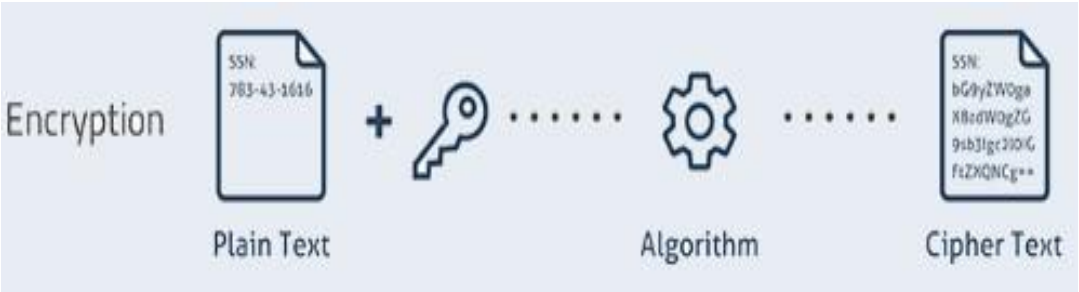


Figure 6 Encryption Process

KEY DIFFERENCE:

Encryption is a process of converting normal data into an unreadable form whereas Decryption is a method of converting the unreadable/coded data into its original form.Encryption is done by the person who is sending the data to the destination, but the decryption is done at the person who is receiving the data. The same algorithm with the same key is used for both the encryption-decryption processes.

Why Encryption:

Helps you to protect your confidential data such as passwords and login id. Provides confidentiality of private information. Helps you to ensure that that the document or file has not been altered. Encryption process also prevents plagiarism and protects IP. Helpful for network communication (like the internet) and where a hacker can easily access unencrypted data. It is an essential method as it helps you to securely protect data that you don't want anyone else to have access.

Why Cryptography

It is used to secure and protect data during communication. Encryption is a process which transforms the original information into an unrecognizable form. Decryption is a process of converting encoded/encrypted data in a form that is readable and understood by a human or a computer. Encryption method helps you to protect your confidential data such as passwords and login id. Public, Private, Pre-Shared and Symmetric are important keys used in cryptography. An employee is sending essential documents to his/her manager are an example of an encryption method. he manager is receiving the essential encrypted documents from his/her employee and decrypting it is an example of a decryption method.

Symmetric Key:

- Symmetric-key encryptions are algorithms which use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext.

Asymmetric Key:

Asymmetric encryption uses 2 pairs of key for encryption. Public key is available to anyone while the secret key is only made available to the receiver of the message. This boots security.

Public Key:

- Public key cryptography is an encryption system which is based on two pairs of keys. Public keys are used to encrypt messages for a receiver.

Parameter	Encryption	Decryption
What is	It is a process of converting normal data into an unreadable form. It helps you to avoid any unauthorized access to data	It is a method of converting the unreadable/coded data into its original form.

Process	Whenever the data is sent between two separate machines, it is encrypted automatically using a secret key.	The receiver of the data automatically allows you to convert the data from the codes into its original form.
Location of Conversion	The person who is sending the data to the destination.	The receiver receives the data and converts it.
Example	An employee is sending essential documents to his/her manager.	The manager is receiving the essential documents from his/her employee.
Use of Algorithm	The same algorithm with the same key is used for the encryption-decryption process.	The only single algorithm is used for encryption and decryption with a pair of keys where each use for encryption and decryption.
Major function	Transforming humanly understandable messages into an incomprehensible and obscure form that can not be interpreted.	It is a conversion of an obscure message into an understandable form which is easy to understand by a human.

Human being from ages had two inherent needs.(a) to communicate and share information and (b) to communicate selectively. These two needs gave rise to the art of coding the messages in such a way that only the intended people could have access to the information. Unauthorized people could not extract any information, even if the scrambled messages fell in their hand. The art and science of concealing the messages to introduce secrecy in information security is recognized as cryptography. The word 'cryptography' was coined by combining two Greek words, 'Krypto' meaning hidden and 'graphene' meaning writing.

The art of cryptography is considered to be born along with the art of writing. As civilizations evolved, human beings got organized in tribes, groups, and kingdoms. This led to the emergence of ideas such as power, battles, supremacy, and politics. These ideas further fueled the natural need of people to communicate secretly with selective recipient which in turn ensured the continuous evolution of cryptography as well. The roots of cryptography are found in Roman and Egyptian civilizations.The first known evidence of cryptography can be traced to the use of 'hieroglyph'. Some 4000 years ago, the Egyptians used to communicate by messages written in hieroglyph.This code was the secret known only to the scribes who used to transmit messages on behalf of the kings. One such hieroglyph is shown below.

In steganography, an unintended recipient or an intruder is unaware of the fact that observed data contains hidden information. In cryptography, an intruder is normally aware that data is being communicated, because they can see the coded/scrambled message.

Figure 7 embedding data

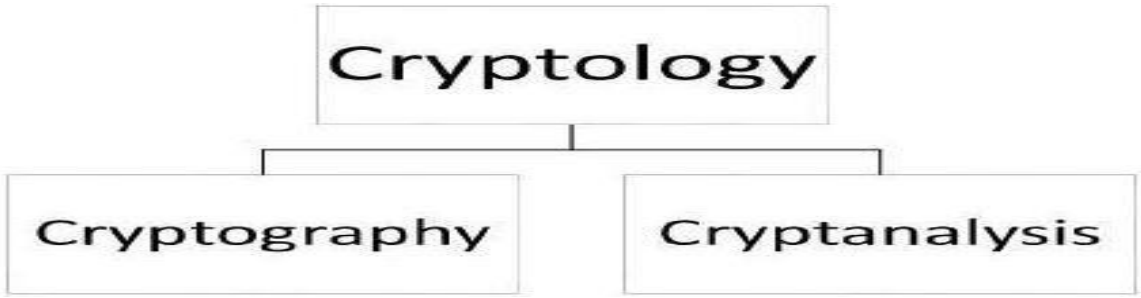


Figure 8 Crptosystem

Cryptography is the art and science of making a cryptosystem that is capable of providing information security. Cryptography deals with the actual securing of digital data. The art and science of breaking the cipher text is known as cryptanalysis. Cryptanalysis is the sister branch of cryptography and they both co-exist. The cryptographic process results in the cipher text for transmission or storage.

It involves the study of cryptographic mechanism with the intention to break them. Cryptanalysis is also used during the design of the new cryptographic techniques to test their security strengths. **Note** − Cryptography concerns with the design of cryptosystems,

while cryptanalysis studies the breaking of cryptosystems.

The primary objective of using cryptography is to provide the following four fundamental information security services.

- Confidentiality
- Data Integrity
- Authentication
- Non-repudiation

Confidentiality is the fundamental security service provided by cryptography. It is a security service that keeps the information from an unauthorized person. It is sometimes referred to as **privacy** or **secrecy**.

It is security service that deals with identifying any alteration to the data. The data may get modified by an unauthorized entity intentionally or accidently. Integrity service confirms that whether data is intact or not since it was last created, transmitted, or stored by authorized user. Data integrity cannot prevent the alteration of data, but provides a means for detecting whether data has been manipulated in an unauthorized manner.

Authentication provides the identification of the originator. It confirms to the receiver that the data received has been sent only by an identified and verified sender.

Message authentication identifies the originator of the message without any regard router or system that has sent the message

Entity authentication is assurance that data has been received from a specific entity, say a particular website.

Nonrepudiation provides an assurance that the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.

Figure 9. Nonrepudiation

The Data Encryption

Standard (DES /ˌdiːˌiːˈɛs, dɛz/) is a symmetric-key algorithm for the encryption of digital

data. A.its short key length of 56 bits makes it too insecure for applications; it has been highly influential in the advancement of cryptography. DES is insecure due to the relatively short 56-bit key size. In computing, 56-bit encryption refers to a key size of fifty-six bits, or seven bytes, for symmetric encryption. While stronger than 40-bit encryption, this still represents a relatively low level of security in the context of a brute force attack.

In cryptography, key size or key length is the number of bits in a key used by a cryptographic algorithm (such as a cipher). Key length defines the upper-bound on an algorithm's security (i.e. a logarithmic measure of the fastest known attack against an algorithm), since the security of all algorithms can be violated by brute-force attacks

The byte is a unit of digital information that most commonly consists of eight bits. the byte was the number of bits used to encode a single character of text in a computer. it is the smallest addressable unit of memory in many computer architectures. To disambiguate arbitrarily sized bytes from the common 8-bit definition, network protocol documents such as The Internet Protocol (1981) refer to an 8-bit byte as an octet.

Substitution Ciphers. Substitution ciphers encrypt the plaintext by swapping each letter or symbol in the plaintext by a different symbol as directed by the key. Perhaps the simplest substitution cipher is the Caesar cipher, named after the man who used it.

What are Substitution Ciphers?

Simple Substitution Ciphers (or Monoalphabetic Substitution Ciphers) ...

Keyword Generators. ...

The Atbash Cipher. ...

The Caesar Cipher. ...

The Pigpen Cipher (Freemasons Cipher) ...

Digraph Substitution Ciphers. ...

Breaking The Code. ...

Polyalphabetic Substitution Ciphers.

Substitution cipher, data encryption scheme in which units of the plaintext (generally single letters or pairs of letters of ordinary text) are replaced with other symbols or groups of symbols.

SUBTITUTION CIPHERS.

SIMPLE SUBTTTUION CIPHERS:

In simple substitution (or monoalphabetic) ciphers, each character of the plaintext is replaced with a corresponding character of ciphertext. A single one-to-one mapping function (*f*) from plaintext to ciphertext character is used to encrypt the entire message using the same key (k); such that

Ek(M)=f(m1)f(m2)….. f(mN)=C

Where N: is the length of the message.

M: is plaintext message given by M= (m 1, m2 mN).

C: is ciphertext message given by C=(c1, c2,….,cN)

Simple substitution ciphers are often called monoalphabetic ciphers, figure (2-2) represents two concentric rings of which the outer is free to rotate and represent the ciphertext while the inner one represent the plaintext. If the outer one is moved to a certain position then the plaintext letters could be enciphered by replacing each letter by the one out side it. The letter frequency distribution is preserved in the ciphertext. Several forms of f can be used in simple substitution, such as:

Shifted alphabet (Caesar cipher):

f(mi) - (mi + k) mod n

Where k is the number of positions to be shifted, mi is a single character of the

alphabet, and n is the size of the alphabet.

If k = 3 then we can encrypt the following message as:

M: R E N A I S S A N C E Ek(M): U H Q D L V V D Q F H

Multiplication based (decimation):

f(mi) = mi * k mod n

where k and n are relatively prime in order to produce a complete set of residues.

Example: k = 9; then the above message can encrypted as: M: R E N A I S S A N C E

Ek(M):X K N A U G G A N S K

If k and n are not prime, several letters will encipher to the same ciphertext letter, and not all letters will appear in the ciphertext.

Home work: try it when k = 13

Addition and multiplication (affine) :

f(mi)= (mi * k1+k0) mod n Where k1 and n are relatively prime.

Simple substitution ciphers does not hide the underlying frequencies of the different letters of the plaintext, and hence it can be easily broken.

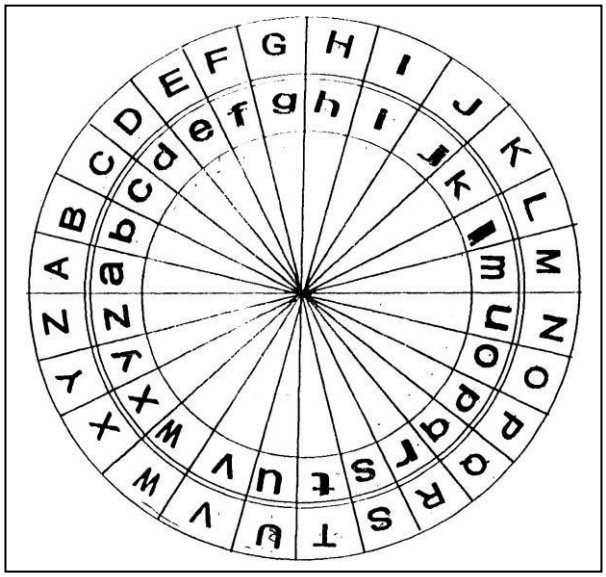


Figure (2-2) simple substitution dis

POLYALPHABETIC SUBSTITUTION CIPHER:

A Polyalphabetic cipher means a sequence of monoalphabetic ciphers, which are often referred to as its substitution alphabets or just alphabet. In another meaning; it is made of multiple simple substitutions. The sequence of the substituting alphabet may have fixed length (d) and is denoted as its period.

Given a period d, cipher alphabet (C1, ..., C2, and fi : A Ci be a mapping from a plaintext A to its ciphertext C, and M

=m1,…,md,md+1,…,m2d,... is enciphered by repeating the sequence of mapping f1,…,fd every d characters.

Ek(M)=f1(m1),…,fd(md) , f1(md+1),….,fd(m2d) For d=1 ,the cipher is monoalphabetic

A popular form of periodic substitution ciphers is the Vigenere cipher. The key is specified by a sequence of letters, K= k1,k2,…,kd , then Vigenere cipher system is defined as:

fi (mi) = (mi +ki) mod n for i=1,2, , d

Example: . ' M: C O D E B R E A K I N G

K: r a d i o r a d i o r

a C: T O G M P I E D S W E G

Another periodic cipher, is Beaufort cipher, which is similar to Vigenere but using subtraction instead of addition, and defined as :

fi (mi) = (ki - mi) mod n

HOMOPHONIC SUBSTITUTION CIPHER:

Homophonic substitution ciphers maps each character (a) of the plaintext alphabet into a set of ciphertext elements f(a) called homophone. Thus the mapping function f from plaintext to ciphertext is of the form: f:A 2c . Example of such ciphers are Beale , and High order

homophonic ciphers.

BEALE CIPHERS:

A plaintext message M=m1 m2... .... is encrypted as C = c1 c1 ... .

where ci is picked at random from the set of homophones f(mi).

Example: English letters are enciphered as integers (0 - 99), a group of integers are assigned

to a letter proportional to the relative frequency of the letter, as follows:

Letter	Homophones
A	17 19 34 4 56 60 67 83
I	08 22 53 65 88 90
L	03 44 76
N	02 09 15 27 32 40 59
0	01 11 23 28 42 54 70 80
P	33 91
T	05 10 20 29 45 58 64 78 99

M= P L A I N P I L 0 T C= 91 44 56 65 59 33 08 76 28 78

Homophonic substitution ciphers are more complicated than simple substitution ciphers, but still do not obscure all of the statistical properties of the plaintext language.

HIGER-ORDER HOMOPHONICS:

It is possible to construct higher-order homophonic ciphers such that an intercepted ciphertext will decipher into more than one meaningful message under different keys. To construct 2nd - order homophonic cipher, (lie number (1 - n2) are randomly inserted into (n * n) matrix K, whereas columns and rows correspond to the characters of the plaintext alphabet (A). For each character a , row a defines one set of homophones f1(a), and column a defines another set of homophones f2(a). There are two keys (mapping) f1, and f2. The ciphertext is selected from the intersection f1(mi),and f2(xi).

Ci = [mi , xi].

Where M = ml m2 ..... Message,

X = xl x2 ... . Dummy message.

Example : if n= 5, 5 *5 matrix for the alphabet [E, I, L, M, S]:

E I L M S

E	10	22	18	02	11
I	12	01	25	05	20
L	19	06	23	13	07
M	03	16	08	24	15
S	17	09	21	14	04

Then the message (smile) is enciphered as:

M: S M I L E X: L I M E S C: 21 16 05 19 11

POLYGRAM SUBSTITUTION CIPHER:

Polygram cipher systems are ciphers in which group of letters are encrypted together, and includes enciphering large blocks of letters. Therefore, permits arbitrary substitution for groups of characters. For example the plaintext group "ABC" could be encrypted to "RTQ", "ABB" could be encrypted to "SLL", and so on. In another meaning, encryption includes substitution of a block of multiple letters from plaintext with the corresponding group of ciphertext. Example of such ciphers are Playfair, and Hill ciphers.

PLAYFA1R CIPHER:

playfair cipher is a digram substitution cipher, the key is given by a 5*5 matrix of 25 letters (j was not used), as described in figure 11.

Each pair of plaintext letters are encrypted according to the following rules:

l. if m1 and m2 are in the same row, then c1 and c2 are to the right of m1 and m2 , respectively. The first column is considered to the right of the last column.

if m1 and m2 are in the same column, then c1 and c2 are below m1 and m2 respectively. the first row is considered to be below the last row.

if m1 and m2 are in different rows and columns, then c1 and c2 are the other two corners of the rectangle.

If m1=m2 a null letter is inserted into the plaintext between m1 and m2 to eliminate the double.

If the plaintext has an odd number of characters, a null letter is appended to the end of the plaintext.

H	A	R	P	S
I	C	O	D	B
E	F	G	K	L
M	N	Q	T	U
V	W	X	Y	Z

Figure 11 Key for Playfair cipher

Example:
M = RE NA IS SA NC EX Ek(M) = HG WC BH HR WF GV

HILL CIPHER:

Hill cipher performs linear transformation on d plaintext characters to get d cipher text characters. If d = 2, M= m1 m2 , then C = Ek(M) = C1 C2 where:

C1 =(k11 m1 + k12 m2) mod n C2 =(k21 m1 + k22 m2) mod n

Expressing M and C as column vectors:

C = Ek(M) = KM where K is matrix of coefficients:

K11 k12 that is c1 = k11 k12 m1 mod n K21 k22
c2 k21 k22 m2

Deciphering is done using the inverse matrix K-1 Dk =(C)= K-1C mod n = K-1 K M mod n =M

Where K K-1 mod n =I , I is 2*2 identity matrix.

Example : To encipher the message EG :

Let k = 3 2)

Where k * k-1 mod 26 = 1 0)

0 1

Then k-1 = $\begin{pmatrix} 15 & 20 \\ 17 & 9 \end{pmatrix}$

" by using Gauss elimination "

$$C = k * M \bmod 26 = \begin{pmatrix} 4 & 2 \\ 3 & 5 \\ & 6 \end{pmatrix} * \begin{pmatrix} 3 \\ 1 \end{pmatrix} \bmod 26 = \begin{pmatrix} 24 \\ \end{pmatrix}$$

Then the C = YQ

Transposition Cipher is a cryptographic algorithm where the order of alphabets in the plaintext is rearranged to form a cipher text. In this process, the actual plain text alphabets are not included.

Example

A simple example for a transposition cipher is columnar transposition cipher where each character in the plain text is written horizontally with specified alphabet width. The cipher is written vertically, which creates an entirely different cipher text.

Consider the plain text hello world, and let us apply the simple columnar transposition technique as shown below

h	e	l	l
o	w	o	r
l	d		

The plain text characters are placed horizontally and the cipher text is created with vertical format as : holewdlo lr. Now, the receiver has to use the same table to decrypt the cipher text to plain text.

Code

The following program code demonstrates the basic implementation of columnar transposition technique −

```
def split_len(seq, length):
   return [seq[i:i + length] for i in range(0, len(seq), length)]

def encode(key, plaintext):
   order = {
      int(val): num for num, val in enumerate(key)
   }
```

```
ciphertext = ''

for index in sorted(order.keys()):

   for part in split_len(plaintext, len(key)):

      try:ciphertext += part[order[index]]

         except IndexError:

            continue

   return ciphertext

print(encode('3214', 'HELLO'))
```

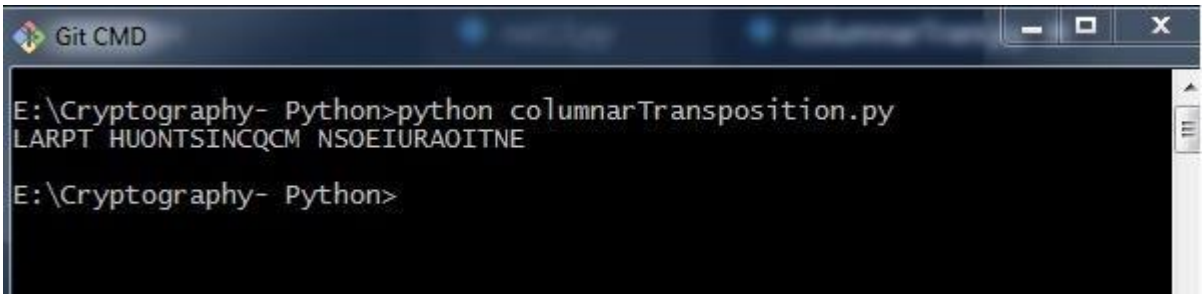
Explanation

Using the function split_len(), we can split the plain text characters, which can be placed in columnar or row format.

encode method helps to create cipher text with key specifying the number of columns and prints the cipher text by reading characters through each column.

Output

The program code for the basic implementation of columnar transposition technique gives the following output −



Note − Cryptanalysts observed a significant improvement in crypto security when transposition technique is performed. They also noted that re-encrypting the cipher text using same transposition cipher creates better security.

Transposition Cipher is a cryptographic algorithm where the order of alphabets in the plaintext is rearranged to form a cipher text. In this process, the actual plain text alphabets are not included.

Example

A simple example for a transposition cipher is columnar transposition cipher where each character in the plain text is written horizontally with specified alphabet width. The cipher is written vertically, which creates an entirely different cipher text.

Consider the plain text hello world, and let us apply the simple columnar transposition technique as shown below

h	e	l	l
o	w	o	r
l	d		

The plain text characters are placed horizontally and the cipher text is created with vertical format as : holewdlo lr. Now, the receiver has to use the same table to decrypt the cipher text to plain text.

Code

The following program code demonstrates the basic implementation of columnar transposition technique −

```
def split_len(seq, length):

   return [seq[i:i + length] for i in range(0, len(seq), length)]

def encode(key, plaintext):

   order = {

      int(val): num for num, val in enumerate(key)

   }

ciphertext = ''



for index in sorted(order.keys()):
```

```
    for part in split_len(plaintext, len(key)):
      try:ciphertext += part[order[index]]
        except IndexError:
          continue
    return ciphertext
print(encode('3214', 'HELLO'))
```

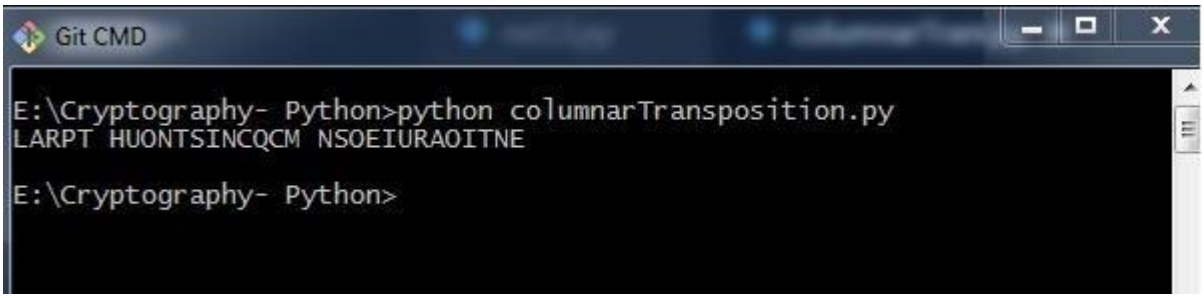
Explanation

Using the function split_len(), we can split the plain text characters, which can be placed in columnar or row format.

encode method helps to create cipher text with key specifying the number of columns and prints the cipher text by reading characters through each column.

Output

The program code for the basic implementation of columnar transposition technique gives the following output −



Note − Cryptanalysts observed a significant improvement in crypto security when transposition technique is performed. They also noted that re-encrypting the cipher text using same transposition cipher creates better security.

Generating RSA keys

The following steps are involved in generating RSA keys −

Create two large prime numbers namely p and q. The product of these numbers will be called n, where n= p*q

Generate a random number which is relatively prime with (p-1) and (q-1). Let the number be called as e.

Calculate the modular inverse of e. The calculated inverse will be called as d.

Algorithms for generating RSA keys

We need two primary algorithms for generating RSA keys using Python − Cryptomath module and Rabin Miller module.

Cryptomath Module

The source code of cryptomath module which follows all the basic implementation of RSA algorithm is as follows −

```
def gcd(a, b):
   while a != 0:
      a, b = b % a, a
   return b


def findModInverse(a, m):
   if gcd(a, m) != 1:
      return None
   u1, u2, u3 = 1, 0, a
   v1, v2, v3 = 0, 1, m


   while v3 != 0:
      q = u3 // v3
         v1, v2, v3, u1, u2, u3 = (u1 - q * v1), (u2 - q * v2), (u3 - q * v3), v1, v2, v3
```

```
  return u1 % m
```

RabinMiller Module

The source code of RabinMiller module which follows all the basic implementation of RSA algorithm is as follows −

```
import random

def rabinMiller(num):
  s = num - 1
  t = 0

  while s % 2 == 0:
    s = s // 2
    t += 1
  for trials in range(5):
    a = random.randrange(2, num - 1)
    v = pow(a, s, num)
    if v != 1:
      i = 0
      while v != (num - 1):
        if i == t - 1:
          return False
        else:
          i = i + 1
          v = (v ** 2) % num
```

```
        return True
def isPrime(num):
    if (num 7< 2):
        return False
    lowPrimes = [2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61,
    67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151,
    157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241,
    251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313,317, 331, 337, 347, 349,
    353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449,
    457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 541, 547, 557, 563, 569,
    571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661,
    673, 677, 683, 691, 701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787,
    797, 809, 811, 821, 823, 827, 829, 839, 853, 857, 859, 863, 877, 881, 883, 887, 907,
    911, 919, 929, 937, 941, 947, 953, 967, 971, 977, 983, 991, 997]

    if num in lowPrimes:
        return True
    for prime in lowPrimes:
        if (num % prime == 0):
            return False
    return rabinMiller(num)
def generateLargePrime(keysize = 1024):
    while True:
```

```
    num = random.randrange(2**(keysize-1), 2**(keysize))
    if isPrime(num):
      return num
```

The complete code for generating RSA keys is as follows −

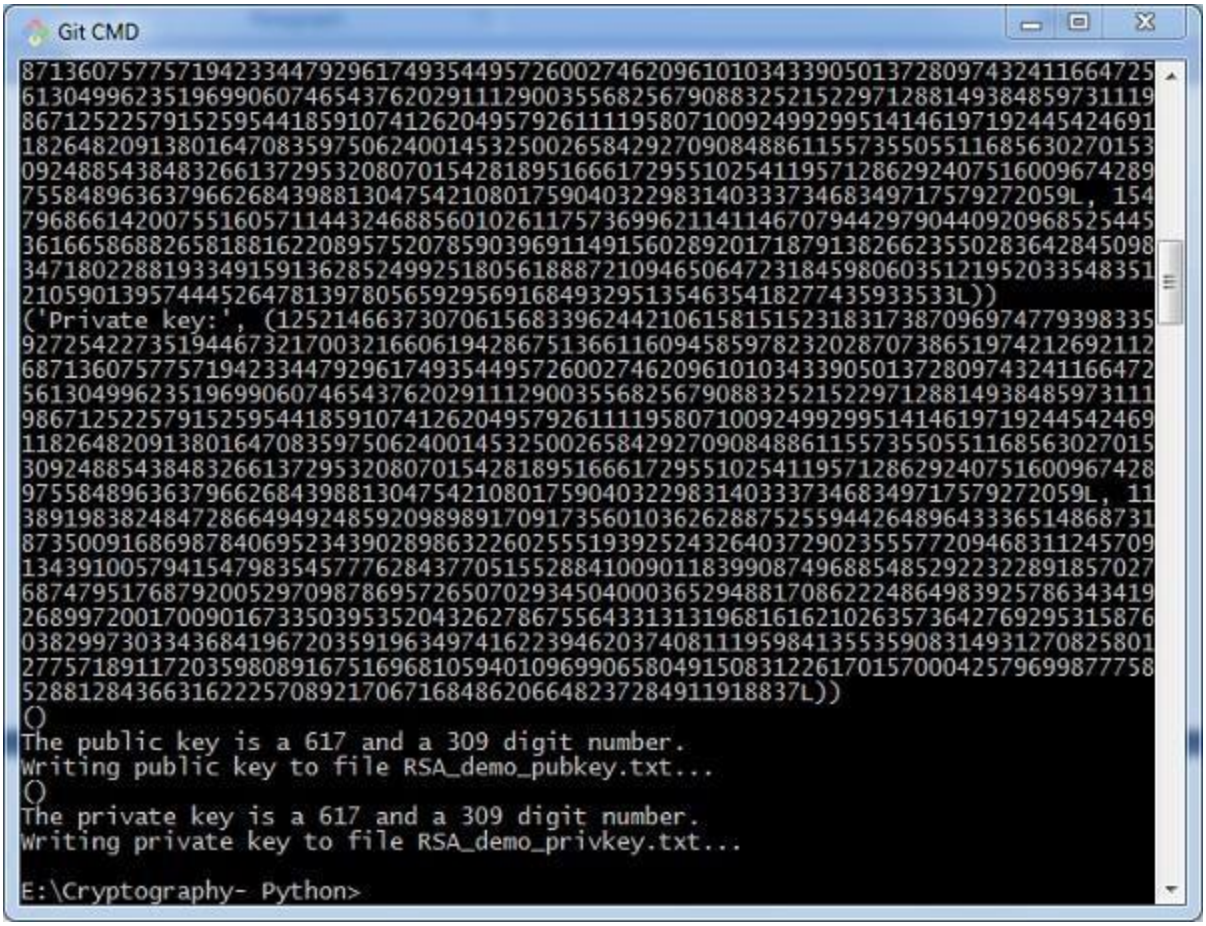
```
import random, sys, os, rabinMiller, cryptomath

def main():
  makeKeyFiles('RSA_demo', 1024)

def generateKey(keySize):
  # Step 1: Create two prime numbers, p and q. Calculate n = p * q.
  print('Generating p prime...')
  p = rabinMiller.generateLargePrime(keySize)
  print('Generating q prime...')
  q = rabinMiller.generateLargePrime(keySize)
  n = p * q

  # Step 2: Create a number e that is relatively prime to (p-1)*(q-1).
  print('Generating e that is relatively prime to (p-1)*(q-1)...')
  while True:
    e = random.randrange(2 ** (keySize - 1), 2 ** (keySize))
    if cryptomath.gcd(e, (p - 1) * (q - 1)) == 1:
      break
```

```
    # Step 3: Calculate d, the mod inverse of e.
    print('Calculating d that is mod inverse of e...')
    d = cryptomath.findModInverse(e, (p - 1) * (q - 1))
    publicKey = (n, e)
    privateKey = (n, d)
    print('Public key:', publicKey)
    print('Private key:', privateKey)
    return (publicKey, privateKey)


def makeKeyFiles(name, keySize):
    # Creates two files 'x_pubkey.txt' and 'x_privkey.txt'
        (where x is the value in name) with the the n,e and d,e integers written in them,
    # delimited by a comma.
    if os.path.exists('%s_pubkey.txt' % (name)) or os.path.exists('%s_privkey.txt' % (name)):
        sys.exit('WARNING: The file %s_pubkey.txt or %s_privkey.txt already exists! Use a
different name or delete these files and re-run this program.' % (name, name))
    publicKey, privateKey = generateKey(keySize)
    print()
    print('The public key is a %s and a %s digit number.' % (len(str(publicKey[0])),
len(str(publicKey[1]))))
    print('Writing public key to file %s_pubkey.txt...' % (name))


    fo = open('%s_pubkey.txt' % (name), 'w')
```

```
        fo.write('%s,%s,%s' % (keySize, publicKey[0], publicKey[1]))

    fo.close()

    print()

    print('The private key is a %s and a %s digit  number.' % (len(str(publicKey[0])),
len(str(publicKey[1]))))

    print('Writing private key to file %s_privkey.txt...' % (name))



    fo = open('%s_privkey.txt' % (name), 'w')

    fo.write('%s,%s,%s' % (keySize, privateKey[0], privateKey[1]))

    fo.close()

# If makeRsaKeys.py is run (instead of imported as a module) call

# the main() function.

if__name__== '_main_':

    main()
```

Output

The public key and private keys are generated and saved in the respective files as shown in the following output.



Q &A

1. Write the Goals of Security

1. Privacy
2. Integrity
3. Authentication
4. Availability

2. What is Firewall?

- A firewall is software used to maintain the security of a private network.
- Firewalls block unauthorized access to or from private networks and are often employed to prevent unauthorized Web users or illicit software from gaining access to private networks connected to the Internet.
- A firewall may be implemented using hardware, software, or a combination of both.

3. Define Encryption.

Encryption is the process of using an algorithm to transform information to make it unreadable for unauthorized users.

- This cryptographic method protects sensitive data such as credit card numbers by encoding and transforming information into unreadable cipher text.
- Also called ciphering.

4.How can we authorize the payment through online?

We can authorize the payment through online by using 1.public key cryptography
2. digital signatures

5.Expand ISP, NSP, ADSL and PSTN

ISP-Internet Service providers
NSP-Network service Providers
PSTN-Public Switched Telephone network
ADSL-Asymetric Digital Subsciber line.

6.Expand FTP,WAIS,CGI,HTTP

FTP-File Transfer Protocol.
WAIS-Wide Area Information server.
CGI-common Gateway Interface
HTML-HyperTextMarkup Language.

7.What is CGI?

CGI is the common Gateway Interface protocol for processing user-suppled informaton through server scripts and applications ,including SQL queries.

8. What are security strategies? List Down.

- Security strategies are that can be utilized to combat the threats.
- Basic Security strategies are

1. Access control
2.integrity.
3. Confidentiality
4.authentication.

9. Name some companies that support secure transaction.

1.Biznet Technologies.
2.CommerceNet
3.Cybercash
4.Digicash.
5.First virtual holdings.

6.Net cash
7.Terisa systems.
8.open market
9. Net cheque.
10. RSA data security.

10. Write the difference between network security and computer security.
computer security:

- Measures needed to protect data against unauthorized disclosure,modification,utilization,restriction,incapacitation or destruction.

Network security:

- Measures needed to protect data during transmission ie while transporting data between the user and computer and between computers.

11. What is meant by secure transaction.

- Transactions done over the internet between internet vendors with high security of payments is called secure transactions.
- Secure transaction can be done with the help of security payment protocols such as SET.

12. What is SET?

- SET is a combination of an application level protocol and recommended procedures for handling credit card transactions over the internet.
- SET covers certification of all parties involved in a purchase as well as encryption and authentication procedures.

13. Define computer virus.

- A virus is a program that can infect other programs by modifying them to include a copy of itself.
- It is possible that any program that comes in contact with virus will become infected with the virus.
- It can alter data in files, change disk assignments, create bad sectors, destroy FAT...etc....

14. What is need for computer security

- Collection of tools designed to protect data is computer security.

15. What is meant by Cryptography?

- Cryptography involves creating written or generated codes that allow information to be kept secret.
- Cryptography converts data into a format that is unreadable for an unauthorized user, allowing it to be transmitted without unauthorized entities decoding it back into a readable format, thus compromising the data.
- Cryptography also allows senders and receivers to authenticate each other through the use of key pairs.

- Cryptography is also known as cryptology.

16. Define Verisign.

- Verisign is offering its digital signature technology for authenticating users as a component separate from encryption,which allows for export of stronger authentication.

17. Define Digi cash.

- Digi cash is a software company whose products allow users to purchase goods over the Internet without using a credit card.
- Digicash is a software-only electronic cash system that provides complete privacy.
- The benefit of the Digi cash model is its ability to hold larger amounts of money than a credit card amount.

18. Define Net Cash

- Netcash is the Internet's answer to traveler's checks.
- To use NetCash users must enter their checking account or credit card numbers into an on-screen form and e-mail it to the NetCash system.
- This entitles the users to purchase electronic coupons from Net Cash for their face value plus a 2 percent commission.

19. Write down the commercial electronic payment schemes

1.Netscape.
2.Microsoft
3.Checkfree.
4.CyberCash.
5.Verisign
6.Digicash
7.First virtual Holdings.
8.Bank America/Lawrence Livermore Labs
9.Commerce Net
10.Netcash

20. What is decryption?

- The translation of encrypted text or data(called cipher text) into original text or data (call clear text).
- Also called deciphering.

21. What is private Key?

- One of the two keys used in a symmetric encryption system.
- For secure communications,the private key should be known only by its creator.

22. What is public Key?

- One of the two keys used in a symmetric encryption system.
- The public key is made public,to be used in conjunction with a corresponding private key.

23. Define proxy?

- A software agent that acts on behalf of a user.
- Typical proxies accept a connection from a user, make a decision as to whether or notthe user or client IP address is permitted to use the proxy, perhaps do additional authentication,and then complete a connection behalf of the user to a remote destination.

24. What is RLogin?

- A tool that allows one system to log in to a remote UNIX host.
- Users do not have to have valid user names or passwords to access the system,as is required when using Telnet.

25. What do you mean by authentication?

- The process of determining the identity of a user that is attempting to access a system.

26.What do you mean by authorization?

- The process of determining what types of activities are permitted.
- Usually authorization is in the context of authentication; once you have authenticated a user, that user may be authorized for different types of access or activity.

27. Define Worm

- Program that can replicate itself and send copies from computer to computer across network connections.
- Upon arrival, the worm may be activated to replicate and propagate again.
- In addition to propagation, the worm usually performs some unwanted function.

28. Define Trojan horse.

A software entity that appears to do something normal but which, in fact, contains a trapdoor or attack program

SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE
www.sathyabama.ac.in

SCHOOL OF MANAGEMENT STUDIES

UNIT - III MANAGING EBUSINESS – SBAA 7033

TRADITIONAL TRANSACTIONS

The transaction approach is the concept of deriving the financial results of a business by recording individual revenue, expense, and other purchase transactions. These transactions are then aggregated to see if a business has earned a profit or a loss.

The Transaction approach emphasizes the medium of exchange function of money only. On the other hand, the Cash Balance approach stresses equally the store of value function of money. Therefore, this approach is consistent with the broader definition of money which includes demand deposits.

Traditional transactions provide more richness in terms of face-to-face interaction including visual and aural cues. Online transactions does not have this but however overcomes the limitations of reach providing complex info to a global audience.

- The definition of a **transaction** is an exchange, or an instance where business is done or something is bought or sold.

When you go to the store and buy something, this is an **example of a transaction**.

Transaction is the main concept of the New Institutional Theory (NIT).According to specialists (R. Coase, O. Williamson etc.), transactions can be described by the following characteristics: asset specificity, uncertainty, frequency, transformation costs and transaction costs.

What are the three primary functions performed by the Transaction Processing System?

Transaction processing systems perform input, output, storage, and **processing functions**

Types of Accounting Transactions based on the Exchange of Cash. Based on the exchange of cash, there are few types of accounting transactions, namely cash transactions,

- **non**-cash transactions,
- and credit transactions.
- In computer programming, a **transaction** usually means a sequence of information exchange and related work (such as database updating), that is treated as a unit for the purposes of satisfying a request and for ensuring database integrity.
- Deposit: Add funds to an account by any method.
- Online: Withdraw funds through a web-based store or online **banking** service.

- POS: Withdraw funds through a point-of-sale **transaction** (typically a cash or debit card purchase).
- Transfer: Move funds from one account to another

Different types of online financial transactions are

- **National Electronic Fund Transfer** (**NEFT**)
- Real Time Gross Settlement (**RTGS**)
- Electronic Clearing System (**ECS**)
- **Immediate Payment Service (IMPS**)

The four important characteristics of a TPS are:

RAPID RESPONSE- Fast **performance** with a rapid response is critical.Input must become output in seconds so customers don't wait. Reliability - Organisations rely heavily on their TPS with failure possibly stopping business.

The DBMS is a software system that explains the **four types of actions** which are defining, constructing, manipulating and sharing **databases** among various users and applications.

There are various types of information systems, for example:

- transaction processing systems,
- **decision support systems**
- knowledge management systems,
- learning management systems,
- database management systems,
- office information systems

An **information system** (**IS**) is a formal, socio technical, organizational system designed to collect, process, store, and distribute information. In a socio technical perspective, information systems are composed by four components: task, people, structure (or roles), and technology. A computer information system is a system composed of people and computers that processes or interprets information. The term is also sometimes used to simply refer to a computer system with software installed.

A Transaction Processing System is a set of information which processes the data transaction in database system that monitors transaction programs. The system is useful when something is sold over the internet. It allows for a time delay between when an item is being sold to when it is actually sold. Transaction processing systems provide an execution environment that ensures the integrity, availability, and security of data. They also ensure fast response time and high transaction throughput.

Organizations expect their TPS to accomplish a number of specific objectives such as: Process data generated by and about transactions. The primary objective of TPS is

- to capture, gather, process, and store transactions
- to produce useful documents related to routine business activities to managers.

The TPS can process large amount of data in real time or batches.The use of TPS in organizations is a key feature in improving customer service and satisfaction.

A TPS allows for the user/customer to have a level of reliability and confidence during transactions.

Components of a Transaction System • The user of the information system is the person belonging to the organization that owns the **transaction system**. Participants are the people who conduct the information **processing**.

OFFLINE AND ONLINE TRANSACTIONS

Online transactions are familiar to most people. Examples include: ATM machine transactions such as **deposits**, withdrawals, inquiries, and transfers. Supermarket payments with debit or credit cards.

The terms refer to the two distinct ways in which debit payments are processed: online and offline.

Online debit transactions call for customers to endorse payments by submitting their personal identification numbers (PINs) at the point of sale, while offline transactions require shoppers to sign sales receipts.

Online Payments occurs when a customer's funds are transferred to your payment account right after your customer confirms the payment.

Online customers often will pay through Credit Card, Debit Card ,etc, Offline Payments indicates that money is transferred at a later date. Offline methods don't charge customers right away. Instead, offline payments are meant to store the customer information for processing manually.

Online Payments occurs when a customer's funds are transferred to your payment account right after your customer confirms the payment. Online customers often will pay through Credit Card, Debit Card, etc

Offline Payments indicates that money is transferred at a later date. Offline methods don't charge customers right away. Instead, offline payments are meant to store the customer information for processing manually.

Offline payments are transactions processed asynchronously. Offline payments are made via cash, checks, bank transfers, postal orders, or any other offline means besides online payment methods such as cards, online wallets, etc.

What is an offline transaction?

Offline Transaction Processing, also known as a signature debit **transaction**, is a payment method that uses a debit card to transfer funds from a checking account to a merchant across a digital credit card network.

The differences between traditional banking and Internet banking on the basis of presence, time, accessibility, security, finance control, expensive, cost, customer service and contact are differentiated as follows.

Basis of Difference	Traditional Banking	Internet Banking
Time	It consumes a lot of time as customers have to visit banks to carry out bank transactions like — checking bank balances, transferring money from one account to another.	It does not consume time as customers do not have to visit banks to check bank balances or to transfer money from one account to another. Customers can access their

		account readily from anywhere with a computer and internet access.
Accessibility	**People have to visit banks only during the working hours.**	**Internet banking is available at any time and it provides 24 hours access.**
Security	**Traditional banking does not encounter e-security threats.**	**Online banking is the tempting target for hackers. Security is one of the problems faced by customers in accessing accounts throu h internet.**
Finance Control	**Customers who often travel abroad cannot pay close attention and control of their finances.**	**Customers who often travel abroad can have greater control over their finances.**
Expensive	**Customers have to spend money for visiting banks.**	**Customers do not have to spend money for visiting banks. They can avoid bank charges that may be charged for certain teller transactions or when they pay bills electronically — directly from their account to the**

		merchant. It helps to save money on postal charges.
Cost	**The cost incurred by traditional banks includes a lot of operating and fixed costs.**	**Such costs are eliminated as the banks do not have physical presence.**
Customer Service	**ln traditional banks, the employees and clerical staff of the bank can attend only few customers at a time.**	**In online banking, the customers do not have to stand in queues to carry out certain bank transactions.**
Contact	**Customers can have face to face contact in traditional banking.**	**Customers can have only electroonic contacts.**
Presence	**Banks exist physically for serving the customers,**	**Internet banks do not have physical presence as services are provided online.**

Offline payment works much the same as online payment. When the merchant swipes a customer's credit the payment details processed by the point of sale (POS) terminal are transferred via a payment gateway (a secure connecting technology) to an acquirer or acquiring bank.

The acquirer checks with the card issuer (cardholder's bank or the bank that issued the card) to confirm that there are sufficient funds for the payment to be made.

Once the issuer confirms that the payment can be made, the acquirer approves the payment and the terminal indicates to the merchant that the payment has been successful.

Difference between Traditional Commerce and E- Commerce

Points of Distinction	Traditional Commerce	E-Commerce
Interaction	Direct interaction between buyer and seller is present in traditional commerce.	Interaction between buyer and seller is indirect through internet or web.
Suitability	It is suitable for products needed to convince to the customers.	It is suitable for the standard products, low-value products, intangible products, and digital products.
Identity Verification	In traditional commerce, customer can verify the identity of the seller and their physical location.	In case of e-commerce, customer cannot identify the seller, his / her location and many other things.
Transaction Processing	Transactions are processed manually.	Business transactions are processed in automated manner.
Scope	The scope of business is generally limited to particular region.	The scope of business in world-wide.
Level of Competition	The level of competition is generally low.	Because of the wide scope of business, the level of competition is relatively high.

Electronic commerce is very much like traditional commerce. It also involves and exchange of goods. But the exchange of goods is conducted online. Technologies such as email, electronic data interchange and electronic fund transfer are used to track transactions and receive payments. Some of the differences between electronic commerce and traditional commerce are explained briefly below.

1.Cost effective

E-commerce is very cost effective when compared to traditional commerce. In traditional commerce, cost has to be incurred for the role of middlemen to sell the company's product. The cost incurred on middlemen is eliminated in e-commerce as there is a direct link between the business and the customer. The total overhead cost required to run e-business is comparatively less, compared to traditional business.

For example, in running an e-business, only a head office is required. Whereas in traditional method, a head office with several branches are required to cater to the needs of customers situated in different places. The cost incurred on labour, maintenance, office rent can be substituted by hosting a website in e-business method.

2. Time saving

It takes a lot of time to complete a transaction in traditional commerce. E-commerce saves a lot of valuable time for both the consumers and business. A product can be ordered and the transaction can be completed in few minutes through internet.

3. Convenience

E-commerce provides convenience to both the customers and the business. Customers can browse through a whole directories of catalogues, compare prices between products and choose a desired product any time and anywhere in the world without any necessity to move away from their home or work place.

E-commerce provides better connectivity for its prospective and potential customers as the organization's website can be accessed virtually from anywhere, any time through internet. It is not necessary to move away from their work place or home to locate and purchase a desired product.

4. Geographical accessibility

In traditional commerce, it may be easy to expand the size of the market from regional to national level. Business organizations have to incur a lot of expenses on investment to enter international market. In e-commerce it is easy to expand the size of the market from regional to international level.

Introduction of new products

In traditional commerce, it takes a lot of time and money to introduce a new product and analyze the response of the customers. Initially, cost has to be incurred to carry out pilot surveys to understand the taste of the customers.

In e-commerce, it is easy to introduce a product on the website and get the immediate feedback of the customers. Based on the response, the products can be redefined and modified for a successful launch.

6. Profit

E-commerce helps to increase the sales of the organization. It helps the organization to enjoy greater profits by increasing sales, cutting cost and streamlining operating processes.

The cost incurred on the middlemen, overhead, inventory and limited sales pulls down the profit of the organization in traditional commerce.

7. Physical inspection

E-commerce does not allow physical inspection of goods. In purchasing goods in e-commerce, customers have to rely on electronic images whereas in traditional commerce, it is possible to physically inspect the goods before the purchase.

8. Time accessibility

Business is open only for a limited time in traditional commerce. Round the clock (24 x 7) service is available in e-commerce.

9. Product suitability

E-commerce is not suitable for perishable goods and high valuable items such as jewellery and antiques. It is mostly suitable for purchasing tickets, books, music and software. Traditional commerce is suitable for perishables and touch and feel items. Purchasing software, music in traditional commerce may appear expensive,

10. Human resource

To operate in electronic environment, an organization requires technically qualified staff with an aptitude to update themselves in the ever changing world. E-business has difficulty in recruiting and retaining talented people.

Traditional commerce does not have such problems associated with human resource in non electronic environment.

11. Customer interaction

In traditional commerce, the interaction between the business and the consumer is a “face-to-face”.

In electronic commerce, the interaction between the business and the consumer is “screen-to-face”. Since there is no personal touch in e-business, companies need to have intimate relationship with customers to win over their loyalty.

12. Process

There is an automated processing of business transactions in electronic commerce. It helps to minimize the clerical errors.

There is manual processing of business transactions in traditional commerce. There are chances of clerical errors to occur as human intervention takes place.

13. Business relationship

The business relationship in traditional commerce is vertical or linear, whereas in electronic commerce the business relationship is characterized by end-to-end.

14. Fraud

Lot of cyber frauds take place in electronic commerce transactions. People generally fear to give credit card information. Lack of physical presence in markets and unclear legal issues give loopholes for frauds to take place in e-business transactions.

Fraud in traditional commerce is comparatively less as there is personal interaction between the buyer and the seller.

By hosting a website, by placing advertisements on the internet and satisfying certain legal norms, a business can penetrate into global market. It is quite easy to attract customers from global markets at a marginal cost.

DIGITAL CURRENCIES - VIRTUAL CURRENCY, CRYPTO CURRENCY

Virtual Currency is different than digital currency since digital currency is simply currency issued by a bank in digital form. Virtual currency is unregulated and therefore experiences dramatic price movements since the only real force behind trading is consumer sentiment.

Virtual currency is a type of unregulated digital currency that is not issued or controlled by a central bank. Examples include Bitcoin, Litecoin, and XRP. Virtual currency can be either centralized or decentralized

Note:

- XRP is known as a Real Time Gross Settlement System which is a 'currency exchange and remittance network' that independent servers validate. The currency traded is known as XRP and transfer times are immediate.

  Cryptocurrency is a type of virtual currency that utilizes cryptography to validate and secure transactions that are digitally recorded on a distributed ledger, such as a blockchain.

  A Crypto currency is a digital or virtual currency that is secured by cryptography, which makes it nearly impossible to counterfeit or double-spend. Many crypto currencies are decentralized networks based on block chain technology—a distributed ledger enforced by a disparate network of computers.

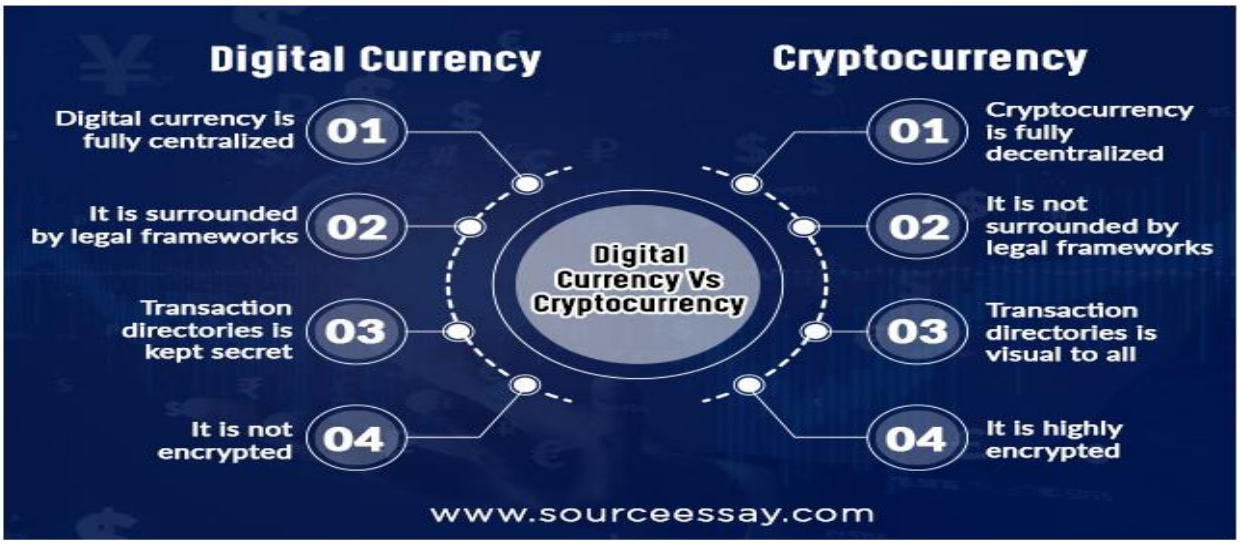


Figure 1.Digital Currency vs Crypto

Crypto currency is a subset of digital currency but not its identical twin. From the fastest port of transaction to the development of blockchain technology; cryptocurrencies ensure a high degree of privacy and secure transactions. Nonetheless, many economists didn't approve cryptocurrency as it fluctuates widely.

Plastic money is a term used to represent the hard plastic cards used in day to day life in place of actual banknotes. They come in several forms such as debit cards, **credit cards**, store cards and pre-paid cash cards

- **Four types of money and why they matter**
- **Representative** currencies (gold) The most important and widely-used money throughout history has been gold. ...
- **Fiat** currencies (USD) **Fiat** money is one that is declared legal tender. ...
- Cryptocurrencies (Bitcoin) ...
- Corporate currencies (Libra)

PAYMENT SYSTEM -CREDIT CARD, DEBIT CARD, ELECTRONIC FUND TRANSFER - CREDIT CARD BASICS.

A cardholder begins a credit card transaction by presenting his or her card to a merchant as payment for goods or services. The acquiring bank (or its processor) captures the transaction information and routes it through the appropriate card network to the cardholder's issuing bank for approval.

A payment processor is a company that handles transactions so that your customers can buy your products. That means the payment processing company communicates and relays information from your customer's credit or debit card to both your bank and your customer's bank.

- Types of Electronic Payment Systems
- Automated clearing house.
- Wire transfers.
- Item processing.
- Remote deposit capture.
- FedLine Access Solutions.
- Automated Teller Machines.
- Card Services (ATM, credit, debit, prepaid)
- Mobile payments.

Merchants send batches of authorized transactions to their payment processor. The payment processor passes transaction details to the card associations that communicate the appropriate debits with the issuing banks in their network. The issuing bank charges the cardholder's account for the amount of the transactions.

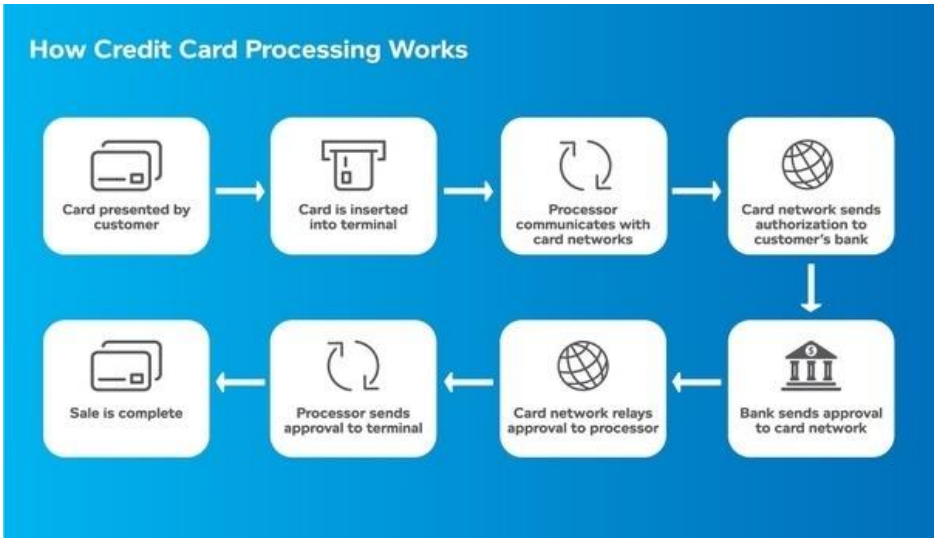


Figure 1credit card Pocess

Chase Paymentech, the payment processing arm of the largest bank in the U.S., authorizes and processes payments in more than 130 currencies. And like its peers, it offers analytics, fraud detection, and security solutions.

A typical Master card transaction involves five parties: besides the payments processor itself, the event includes a consumer or account holder and his or her issuer bank, as well as a merchant and his or her acquirer bank. Typically, an account holder uses a Master card-branded card to make a purchase with a merchant.

Here's how online payment processing works:

The customer picks up an item and pulls out their card. The merchant submits a transaction.
The payment gateway securely sends the transaction to the processor.

The Address Verification Service (AVS) is a tool provided by credit card processors and issuing banks to merchants in order to detect suspicious credit card transactions and prevent credit card fraud. This is done as part of the merchant's request for authorization of the credit card transaction.

The lifecycle of each specific card payment transaction can vary depending on a variety of factors but a few steps in the credit card transaction lifecycle are fixed in place: authorization, batching, clearing and settlement.

- Customer data protection at the point of purchase, through the transmission of data, and when information is stored.Utilization of point-to-point Encryption and Tokenization when sending sensitive client data such as card numbers• Provision of Europay,

Mastercard, and Visa (EMV) protection. EMV chip technology produces a unique code each time. it is used vs. a magnetic strip holding a static amount of data making

- it easier for criminals to skim your card and use the data to create their own
- Secure support in both card present and card-absent environments
- Multipronged fraud-reducing approach

Debit cards deduct money directly from your bank account. Credit cards offer better consumer protection through warranties and fraud protection but are costlier. Newer debit cards offer more credit-card-like protection, while many credit cards no longer charge annual fees. Prepaid refers to the scheme in which you buy credit in advance before availing services.

Postpaid is defined as a scheme in which the customers are billed at the end of the month for the services availed by them. Plans of postpaid SIM costs higher than prepaid SIM. E-Money transactions refer to situation where payment is done over the network and the amount gets transferred from one financial body to another financial body without any involvement of a middleman.

E-money transactions are faster, convenient, and saves a lot of time.Online payments done via credit cards, debit cards, or smart cards are examples of emoney transactions. Another popular example is e-cash.In case of e-cash, both customer and merchant have to sign up with the bank or company issuing e-cash.

Security is an essential part of any transaction that takes place over the internet. Customers will lose his/her faith in e-business if its security is compromised.

Following are the essential requirements for safe e-payments/transactions −

- Confidentiality − Information should not be accessible to an unauthorized person.
- Integrity − Information should not be altered during its transmission over the network.
- Availability − Information should be available wherever and whenever required within a time limit specified.

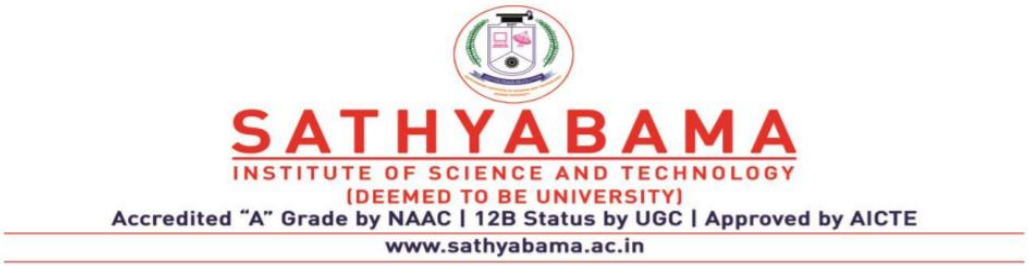
  Authenticity − There should be a mechanism to authenticate a user before giving him/her an access to the required information.

- 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.

Secure Socket Layer (SSL)-It is the most commonly used protocol and is widely used across the industry. It meets following security requirements –Authentication Encryption Integrity Non-reputability. "https://" is to be used for HTTP urls with SSL, where as "http:/" is to be used for HTTP urls without SSL.



SCHOOL OF MANAGEMENT STUDIES

•

UNIT - IV- MANAGING EBUSINESS – SBAA 7033

Virtual Internet Payment System

Virtual has created a payment system, the Internet Payment System, to be used exclusively for the sale of information over the Internet, rather than for products or services. The first virtual Internet payment system is more formally defined by Green Commerce Model and the simple Green Commerce Protocol

ACCOUNT SETUP AND COSTS – There are two ways to setup as a seller on first virtual Internet payment system:

Pioneer and Express.

The Pioneer sellers' program is designed for people who want to start selling their information over Internet without establishing themselves as traditional sellers requiring a credit check. The pioneer application process is simple online application. After application is received and processed,

FIrst virtual will e-mail a 12-digit application number and instructions to seller on how to send bank account information to first virtual via postal mail?
The Express seller program is for those sellers who already have a credit card merchant available to accept credit card payments.

Each buyer and seller must have an e-mail connection to Internet, but transactions can be completed through first virtual World Wide Web site or through a remote terminal session with their system.

Cyber cash has been described as Federal Express of Internet payment business, since it offers safe, efficient and inexpensive delivery of payments across Internet. Cyber cash makes available the software and services needed to exchange payments securely across the Internet with its Secure Internet Payment Service.

Using a procedure that incorporates encryption and digital signatures, cyber cash gives consumers a "digital wallet", and merchants a conduit to Internet payment processing through their own banks.

Cybercash can very much help with the commodification of information and operation of b-web alliances. This, after all, is money as software, thus endowed with high-tech capabilities which no previous money form possessed.

The high-tech nature of cybercash will surely pose unique management problems, such as new (especially reputational and legal) risks, sharp volume fluctuations, complexities in the asset backing of cybercash supplies, convertibility with other money forms, and disruption of online payments systems.

But that same quality will also allow digital money to become embedded in our online economy in entirely new ways. Money flows will surely carry with them large amounts of information facilitating the conduct of transactions and settlement of contractual obligations.

CyberCash, Inc. was an internet payment service for electronic commerce, headquartered in Reston, Virginia. It was founded in August 1994 by Daniel C. Lynch (who served as chairman), William N. Melton (who served as president and CEO, and later chairman), Steve Crocker (Chief Technology Officer), and Bruce G. Wilson.

The company initially provided an online wallet software to consumers and provided software to merchants to accept credit card payments. Later, they additionally offered "CyberCoin," a micropayment system modeled after the NetBill research project at Carnegie Mellon University, which they later licensed.

At the time, the U.S. government had a short-lived restriction on the export of cryptography, making it illegal to provide encryption technology outside the United States. CyberCash obtained an exemption from the Department of State, which concluded that it would be easier to create encryption technology from scratch than to extract it out of Cyber-Cash's software.

In 1995, the company proposed RFC 1898, CyberCash Credit Card Protocol Version 0.8. The company went public on February 19, 1996, with the symbol "CYCH" and its shares rose 79% on the first day of trading. In 1998, CyberCash bought ICVerify, makers of computer-based credit card processing software,and in 1999 added another software company to their lineup, purchasing Tellan Software.[4] In January 2000, a teenage Russian hacker nicknamed "Maxus" announced that he had cracked CyberCash's ICVerify application; the company denied this, stating that ICVerify was not even in use by the purportedly hacked organization.

On January 1, 2000, many users of CyberCash's ICVerify application fell victim to the Y2K Bug, causing double recording of credit card payments through their system. Although CyberCash had already released a Y2K-compliant update to the software, many users had not installed it.

Advantages:• CyberCash uses strong encryption for transporting payment information. – They claim to be the only Internet payment company granted an export license to use RSAs 786 bit encryption algorithm. The Merchant does not see the buyers credit card number.

A web payment processing service from CyberCash, Inc., Oakland, CA that allowed merchants to process credit cards and initiate direct transfers from customer checking accounts. Merchant transactions were sent to CyberCash servers which accessed the credit card networks and Automated Clearing House (ACH).

Performing a Single CyberCash Transaction

To access the CyberCash Transaction page, navigate to Virtual Terminal -> Single Transaction.

1. Be sure to enter information for all fields denoted by an asterisk.

2. Select a Transaction Type from the drop-down menu. For detailed information, refer to Transaction Types.

3. Enter an Order ID. An Order ID is an alphanumeric code you create to identify the transaction. Later on, you can perform secondary actions such as Delayed Capture, Credit, and Void based on the Order ID you specify here.

4. Specify a Credit Card Number that will be billed for the transaction.

5. Specify the Expiration Date of the card.

5. Enter the Amount of the transaction. Use a positive number with no monetary ($) sign and include a decimal point and cents (00 if no cents are involved). For example, 42.00.

6. If you are processing an Voice Authorization transaction, specify the Voice Authorization Number.

7. Enter the Customer Information for the transaction. Use the name as it appears on the credit card, and the address information associated with the card.

8. For Transaction Mode, select Live or Test transaction from the drop-down menu.

9. Verify the information and click Submit.

The CyberCash payment system consists of "CC user software" on the user's machine, "CC merchant software" on the merchant's machine, and the CyberCash server (CC server). The user invokes the CC user software, provides his credit card information, and authorizes the sale for a specific amount.

Customers are able to authorize payments out of their digital wallets. The payments are signed and encrypted, then sent through the merchant bank to cyber cash, which in turn passes the transaction to the merchant's bank for processing.

The digital wallet initially supported only credit cards, but now supports digital cash transfers for small dollar amounts for products and services that are too expensive to justify using a credit card.

What are digital currencies?

*Digital currencies are money used on the Internet.*Digital money exists only in the digital form. It doesn't have any physical equivalent in the real world. Nevertheless, it has all the characteristics of traditional money. Just as classic fiat money, you can obtain, transfer or exchange it for another currency. You can use it to pay for the goods and services, such as mobile and Internet communication, online stores and others. Digital currencies don't have geographical or political borders; transactions might be sent from any place and received an any point in the world. Actually, digital accounts and wallets may be regarded as bank deposits.

What are cryptocurrencies?

Cryptocurrencies are a variety of digital currencies. Cryptocurrency is an asset used as a means of exchanging. It is considered reliable because it's based on cryptography.

One of the cryptography's primary objectives is communications and how to make them secure. It creates and analyzes the algorithms and protocols so no information is changed or interrupted during the conversation by third parties. Cryptography is a mix of a large number of different sciences, with mathematics as the basic. It's math that attaches the severity and reliability to algorithms and protocols.

Cryptocurrencies use Blockchain and a decentralized ledger. It means that no supervisory authority controls all the actions in the network. This comes at the expanse of all the users.

What are the core differences between the two?

Though cryptocurrency is a type of digital currency, there are some fundamental differences.

Structure. Digital currencies are centralized; there is a group of people and computers that regulates the state of the transactions in the network. Cryptocurrencies are decentralized, and the regulations are made by the majority of the community.

Anonymity. Digital currencies require user identification. You'll need to upload a photo of yourself and some documents issued by the public authorities. Buying, investing and any other processes with cryptocurrencies do not need require any of that. Nevertheless, cryptocurrencies are not fully anonymous. Though the addresses don't contain any confidential information such as name, residential address, etc., each transaction is registered, the senders and the receivers are publicly known. Thus, all the transactions are tracked.

Transparency. Digital currencies are not transparent. You cannot choose the address of the wallet and see all the money transfers. This information is confidential. Cryptocurrencies are transparent. Everyone can see any transactions of any user, since all the revenue streams are placed in a public chain.

Transaction manipulation. Digital currencies have a central authority that deals with issues. It can cancel or freeze transactions upon the request of the participant or authorities or on suspicion of fraud or money-laundering. Cryptocurrencies are regulated by the community. It's very unlikely that the users will approve the changes in the Blockchain, although there were some precedents such as the hack of The DAO. However, the amount of money was significant, and the decision was uncertain.

Legal aspects. Most countries have some legal framework for digital currencies, i.e., Directive 2009/110/EC in the European Union, or Article 4A of the Uniform Commercial Code in the US. We cannot say the same about cryptocurrencies at the moment. In most countries, their official status is not defined. The establishment of the legal framework is only in the process.

What are the strengths and weaknesses of digital money?
Most distinctions can be considered as both advantages and disadvantages.
In a centralized system, there is a group of people responsible for the state of the whole system. If you made a mistake in a transaction, you can make a request to the company and rely on the successful outcome. You cannot do this in the decentralized system. On the other hand, centralized networks keep a lot of confidential information about the users. This data may get lost, hacked or be transferred to law enforcement agencies at court request. Decentralized networks do not have these problems. The same goes for a transaction cancellation. If the system is revocable, you can make changes to a transaction. At the same time, it opens room for fraudulent activities.

Virtual Transaction Process – Info Haus–Cyber Cash Model.

Cyber cash acts as a conduit for transactions among Internet, merchants, consumers and banking networks. Merchants wishing to use cyber cash to securely process credit card transactions must establish a merchant account with a bank offering cyber cash PAY button.When the customer completes a purchase and begins a cyber cash transaction by

Clicking on the cyber cash PAY button of a merchant's World Wide Web site, the merchant receives information about the customer's order, as well as an encrypted message from the customer's cyber cash client.

The payments are signed and encrypted then sent through merchant bank to cyber cash, which in turn passes the transaction to merchant's bank for processing. The digital wallet initially supported only credit cards, but now for small dollar amounts for products and services that are too expensive to justify using a credit card.

With cyber cash the wallet is used to manage your credit cards.In a sense cyber cash

process electronically presents your credit card payments to the merchant in the process just like the last time we physically pulled the card out of our wallet and presented it to a merchant.

Cyber cash uses a combination of RSA public key and DES secret key technologies to protect and guarantee data through encryption and digital signatures. It uses full 768-bit RSA as well as 56-bit DES encryption of messages. All transactions are authenticated with MD5 a message digest procedure and RSA digital signatures.While FTP-only sites used to be fairly common, they are becoming less common as more sites move their published data to web sites, or at least to web interfaces.

FTP may be implemented very much like a windows file manager program, including drag-and- drop file copying. Telnet, a remote terminal session application, is less frequently used. It is included with complete TCP/IP packages.

Open market transaction model

1. Request price and purchase information (consumer –
2. content server)

3. Send price and purchase information (content server – consumer)

4. Begin transaction with the specified transaction server (consumer-transaction server)

5. Send consumer transaction information to authorization entity and request authorization (transaction server-financial processing network)

6. Respond with authorization [denied or allowed] (financial processing network-transaction server)

7. Send sales confirmation on confirmed transaction (transaction server-consumer)

8. Request product with confirmation from transaction server (content consumer-server)

9. Deliver product to consumer (content server-consumer)

Using ecash :To get a copy of ecash software, participants filled out a request form with their name, e-mail address, and information about their systems and their intended use for each client and waited for digicash to reply with user-name and password.The first step when first running ecash is to accept the digicash license agreement followed by entering

personal information. Using ecash once the software is set up Clients click on icons to interact with ecash.

There are 3 options:

- withdraw from ecash bank account
- deposit to ecash bank account
- wit hdraw from credit card Consumers Benefits:

Safe, private and easy to use. Protected by the highest allowed levels of Internet encryption with assured authentication. Use existing Visa, MasterCard, American Express or Discover. No special credit cards are necessary. Complete on-line payments. CyberCash is a system which uses public-key cryptography to leverage credit cards onto the Internet, and CyberCoin is an extension of CyberCash to allow small-value transactions.

CyberCash is a system which uses public-key cryptography to leverage credit cards onto the Internet. CyberCoin is an extension of CyberCash to allow small-value transactions.

PGP use a public key cryptosystem RSA (Rivest-Shamir-Adleman, to exchange a private key and to provide a signature for each message. That private key will be used to encrypt message by sender and to decrypt ciphertext by receiver.

With RSA privacy and eletronic signature are easy to achieve.

Credit cards Another simple model for electronic commerce is to use a credit card to pay for the purchase. Customers have credit cards; vendors register with credit card companies;

Customers give their credit card number to vendors; vendors contact their credit card companies for payment; the credit card companies handle the accounting and billing. There are established methods for ensuring secure transmission of the client's credit card number to the vendor. since every purchase involves communication to a centralized credit card transaction service, it is expensive

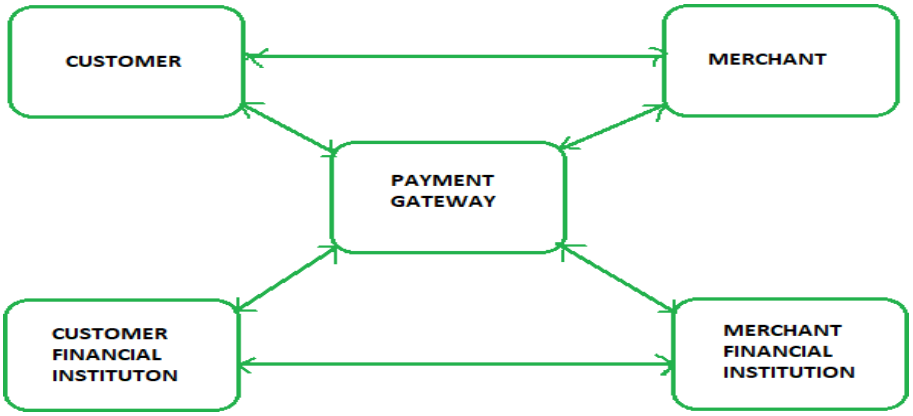
Digital cash is normally issued by a central trusted entity (like a bank). The integrity of digital cash is guaranteed by the digital signature of the issuer, so that counterfeiting digital cash is extremely hard. However, it is trivial to duplicate the bit pattern of the digital cash to produce and spend identical (and equally authentic) cash. In an online digital cash scheme, when a vendor receives digital cash, he must contact the issuer to see if it is valid and not already spent.

Secure Electronic Transaction or SET is a system which ensures security and integrity of electronic transactions done using credit cards.

SET is not some system that enables payment but it is a security protocol applied on

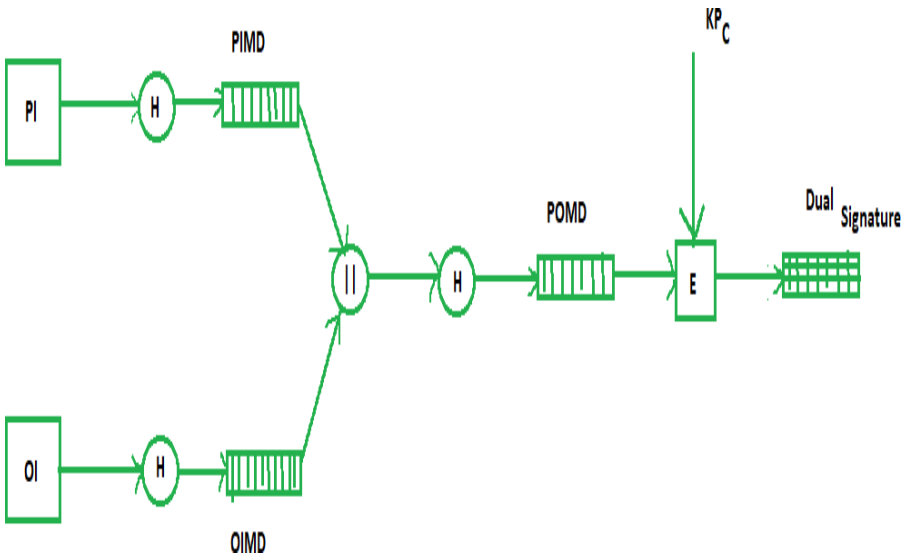
those payments.

- It uses different encryption and hashing techniques to secure payments over internet done through credit cards.
- SET protocol was supported in development by major organizations like Visa, Mastercard, Microsoft which provided its Secure Transaction Technology (STT) and NetScape which provided technology of Secure Socket Layer (SSL).



- SET protocol has important requirements
  - It has to provide mutual authentication i.e., customer (or cardholder) authentication by confirming .if the customer is intended user or not and merchant authentication.
  - It has to keep the PI (Payment Information) and OI (Order Information) confidential by appropriate encryptions.

    Dual Signature :
    The dual signature is a concept introduced with SET, which aims at connecting two information pieces meant for two different receivers : **Order Information (OI) for merchant**
  - **Payment Information (PI) for bank**



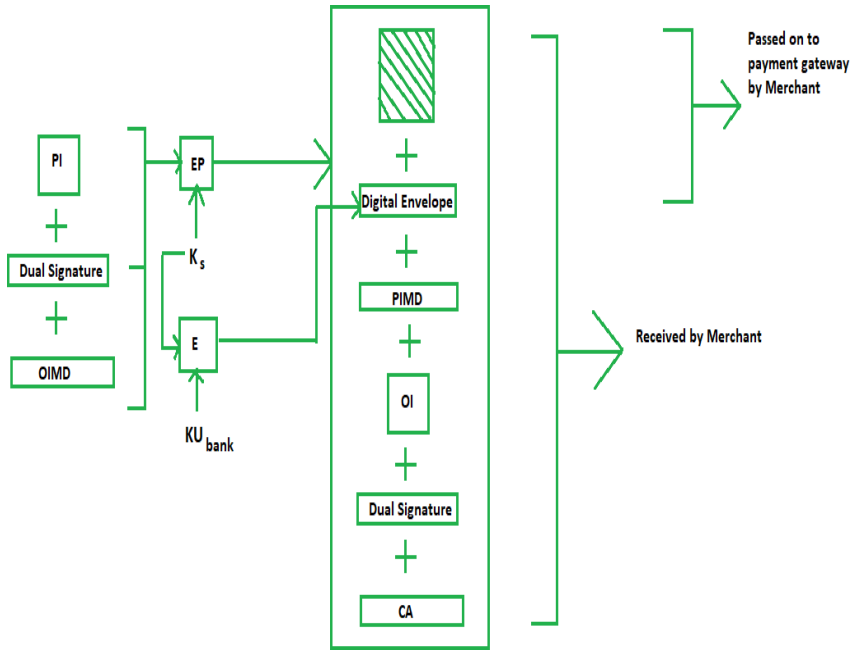

```
Where,

   PI stands for payment information
   OI stands for order information
   PIMD stands for Payment Information Message Digest
   OIMD stands for Order Information Message Digest
   POMD stands for Payment Order Message Digest
   H stands for Hashing
   E stands for public key encryption
   KPc is customer's private key
   || stands for append operation
   Dual signature, DS= E(KPc, [H(H(PI)||H(OI))])
```

Purchase Request Generation

- The process of purchase request generation requires three inputs:
- Payment Information (PI)
- Dual Signature

- Order Information Message Digest (OIMD)

  The purchase request is generated as follows:



Here,

PI, OIMD, OI all have the same meanings as before.

The new things are :

EP which is symmetric key encryption

Ks is a temporary symmetric key

KUbank is public key of bank

CA is Cardholder or customer Certificate

Digital Envelope = E(KUbank, Ks)

Payment Authorization and Payment Capture

Payment authorization as the name suggests is the authorization of payment information by merchant which ensures payment will be received by merchant.

Payment capture is the process by which merchant receives payment which includes again generating some request blocks to gateway and payment gateway in turn issues payment to merchant.

SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE
www.sathyabama.ac.in

SCHOOL OF MANAGEMENT STUDIES

UNIT - V MANAGING EBUSINESS – SBAA 7033

MOBILE COMMERCE

Mobile Commerce - Introduction, Mobile Payments - Direct Mobile Billing, Mobile Web Payment, Direct Operator Billing, Mobile Wallets, Wireless Application Protocol - WAP transaction Model, WAP Architecture.

Buying and selling products and services through mobile devices are the new trend. A housewife can purchase her kitchen appliances from the comfort of her living room, a busy person can order lunch from office, one can use mobile platforms to sell goods and services − all with a few clicks.

What is M-Commerce?

Mobile commerce or simply M-Commerce means engaging users in a buy or sell process via a mobile device. For instance, when someone buys an Android app or an iPhone app, that person is engaged in m-commerce. There are a number of content assets that can be bought and sold via a mobile device such as games, applications, ringtones, subscriptions etc.

How does M-Commerce Work?

Decide Where to Sell

Before you sell your products or services via m-commerce, you need to decide what type of outlets or stores suit your business best. Let us suppose you have created ringtones − you can sell them either at specific third-party outlets or to independent aggregators who charge you a commission for the service.

You can also sell your ringtones on mobile stores or app stores such as Android marketplace or App store (Apple). These stores are frequently visited by many buyers and hence ideal for making sales easily and efficiently. Finally, you can also sell via your own mobile store by creating a mobile website specifically for sales or as by setting-up an m-commerce page on your main website.

Set up Mobile Billing

Once you have decided where to sell, the next step is to set up your merchant account. For instance, you can use third-party services such as PayPal. This is ideal for small businesses or

also large companies. A third-party application makes it really easy for you as well as your customers to make the payments, but then they do charge commission on the transaction.

You can also set-up your own billing and payment gateway, but make sure that you make it really easy for users. Mobile users do not use keyboards or a mouse so make sure that the design of your m-commerce site is intuitive, with easy navigation tools and the right display sizes. Basically, make your m-commerce site optimized for Smartphone users.

Benefits of M-Commerce

The major benefit of engaging in m-commerce is the sheer size of potential sales. The probability of your potential customers owning a Smartphone is very high, so you can safely assume that you will get much more positive response from mobile devices than your website. M-commerce is recommended for every business irrespective of its type, scale, and size.

Mobile devices help users to navigate the world. Customers use mobile devices for all aspects of their needs. They act on the information they see. So advertisers need to extend online advertising and should strive to be seen on mobiles.

Mobile Users − Statistics

As per the survey carried out by Google in partnership with Ipsos OTX MediaCT on 5000+ users, 89% use smartphones throughout the day.

Out of this −

- 89% stay connected
- 82% research and read news
- 75% navigate
- 65% entertain
- 45% manage and plan
- 70% uses mobile devices to make purchase
- 82% notice ads on mobile devices of which around 42% go ahead and click on ads

Advertisers should use location-based services to be easily accessible. Owning a responsive website is a must now.

Ways to Know Your Mobile Audience

You can use the following methods to understand more about your mobile audience −

- Measure user recordings − Here every gesture of user is captured. This makes it easy to trap users' behavior.
- Heat maps give you a breakdown of users' action. You can see where they tap more and the need to change your UI.
- Real-time In-App analytics give an insight into the user's psyche and all the actions they do on their screens.

Return on Investment or simply ROI is the calculation of the profit earned on investment. The formula to calculate ROI is as follows −

ROI =

Return – Investment

To understand the ROI from Mobile Marketing, let's assume −

Customer Lifetime Value (CLV)

CLV = Avg. Revenue per customer × Avg. No. of visits

Say, $100 per customer × 10 visits = $1,000

Calculate allowable Cost of Customer Acquisition (COCA) as −

COCA = CLV × (% allocated to new customer)

Say, $1000 × 10% = $100

Now, reallocate your mobile marketing budget by dividing them into 'Branding' and 'Direct Response'. For example, allocate 20% of your budget to direct response −

Say, direct response budget = $200,000

20% of $200,000 = $40,000

Hence, mobile marketing budget is $40,000.

Now, calculate the number of estimated customers from new mobile marketing campaign.

CLV= $1,000

Budget= $200,000

COCA= $100

Customers acquisition = budget ÷ COCA

Hence, $200,000 ÷ 100 = 2,000

Therefore, new customers = 2,000

Direct response (of new customers) = 2,000

Mobile marketing new customers = 400

Conclusion − On 20% investment, you will gain 20% new customers.

WIRELESS APPLICATION PROTOCOL

Wireless Applications Protocol (WAP) is a standard that transfers data and information to wireless devices. The WAP rollout in 2000 was the first effective standard specifically aimed at mobile devices using a stripped down version of HTML called 'Wireless Markup Language'

(WML). WML is designed for making data, information and limited graphics legible on small hand-held devices such as mobile phones.

The standard protocol for sending data between wireless devices is the Wireless Application Protocol (WAP). WAP uses a version of HTML called Wireless Markup Language (WML) and are designed specifically for small devices such as mobile phones and PDAs. WML allows text to be readable on mobile devices that would be indecipherable using HTML. Users of WAP-enabled devices have to accept some compromises compared to fixed networks.

First, the band- width is much narrower. Although it is possible to broaden bandwidth on mobile devices, it is at the expense of battery life. Second, HTTP messages do not translate well on mobile devices since they are written in human-readable text that is too bulky for wireless-enabled devices.

When wireless technology was first rolled out in the early 1990s, mobile phones operated on the Global System for Mobile Communication (GSM) standard that offered a minimum transmission speed of 9.6 k/bits per second. By 2000, GSM speed was increased to 64 k/bits per second by aggregating channels in a scheme called High-Speed Circuit Switched Data (HSCSD). This brought mobile devices into line with transmission speeds of fixed networks.

There quickly followed a further initiative called the General Packet Radio Service (GPRS).This standard offered a minimum transmission speed of 43 k/bits per second and potentially 170 k/bits per second. GPRS works by combining packets of data from different calls in order to optimise use of capacity. The evolution of standards has continued at a rapid pace since 2000. The GSM standard has subsequently been enhanced by Enhanced Data Rates for Global Evolution (EDGE) at 384 k/bits per second and third generation (3G)Universal Mobile Telecommunications System (UMTS) with a possible 2000 k/bits per second.

For telecommunications firms such as Nokia, Eriksson, BT and Orange, the importance of acquiring a license to operate on frequencies for mobile phones cannot be underestimated. Across Europe, and including the UK, telecommunications firms had to bid for the rights to own a license in a closed auction.

WAP stands for Wireless Application Protocol. It is a protocol designed for micro-browsers and it enables the access of internet in the mobile devices. It uses the mark-up language WML (Wireless Markup Language and not HTML), WML is defined as XML 1.0 application. It enables creating web applications for mobile devices. In 1998, WAP Forum was founded by Ericson, Motorola, Nokia and Unwired Planet whose aim was to standardize the various wireless technologies via protocols.

WAP protocol was resulted by the joint efforts of the various members of WAP Forum. In 2002, WAP forum was merged with various other forums of the industry resulting in the formation of Open Mobile Alliance (OMA).

Internet protocol

Internet protocol (IP) is a system that facilitates the convergence of voice and video with existing forms of internet communication (e-mail, databases, etc.). IP is linked to a common infrastructure that unifies the computer and IT infrastructure of organisations. This allows workers to communicate with anyone else in any part of the globe using a choice of

communications media including video conferencing, mobile phones or laptop computers. IP also extends to mobile communications. Beyond 3G technology comes mobile IP-based network developments that allow users to access any other network using mobile telephones. This will form part of the next generation of mobile phone technology (4G).

VOIP

A challenge to mobile telecoms companies is the prospect of the development of internet telephony, and in particular, voiceover internet protocol (voip). Voip is a means of making telephone calls over the internet and is set to have a considerable impact on the telecoms market. Internet telephony works by breaking down the voice call (in similar fashion to the dismantling of data for online contact), sending it over the internet and then reassembling it at the receiver's end.

VOIP offers free telephone calls by allowing broadband users to download software on to their computers and call other broadband users with exactly the same software anywhere in the world. Free calls are, of course, only available to those users who share the same technology. Nevertheless, voip has attracted the interest of some of the biggest names in telecoms and internet industries including Wanadoo (www.wanadoo.com) and AOL (www.aol.co.uk/ aim). In January 2005 BT (www.bt.com/btcommunicator) announced a £9 billion investment in upgrading its network to facilitate the voip delivery system.

Internet Service Providers (ISPs) can see opportunities by encouraging their customers to switch to internet telephony. Google, one of the world's most high profile ISPs has introduced a strategy to increase its revenues by offering broadband internet users access to cheap phone calls over the internet. By providing a telephony service Google would also gain a greater insight into the customers who use their website. This valuable information could be used to improve the service they provide for their advertisers. The firm also intends to introduce new services such as 'click-to-dial'. This is where an advertiser's web page has a special button that connects an internet phone call straight to a call centre.

Voip may spell the end for telephone charges per minute with the likely replacement being a monthly service charge. This has become possible because of the convergence of telecoms with computers with call traffic moving to the internet. Using the internet for telephony reduces the marginal cost of calls to zero and allows firms to offer phone calls for free. Customers pay a fixed monthly rate and can make as many local or national calls as they wish.

This has significant savings potential for businesses who use telephone services extensively throughout a normal working day. Using traditional communications infrastructure, firms require separate network connections at each of their office locations for data, video, fax and standard calls, making the whole process complex and expensive. Voip allows for voice, video or data to be transmitted using the same dedicated network. The technology also includes additional services such as voicemail, call diversion, caller display and three-way calling.

Voice recognition

A great amount of time, energy and resources has been poured into developing voice recognition technology, with IBM leading the way in both research and design. Once voice

recognition becomes widely available it will offer a further value-added dimension to communicating via fixed or mobile internet.

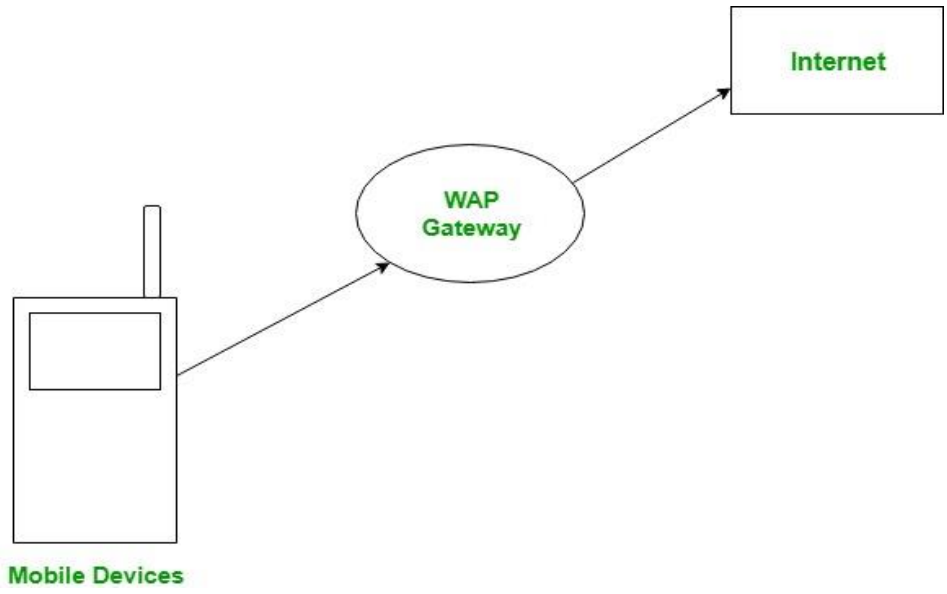
Internet television

Internet television (IPTV) enables viewers to choose from a vast archive of film and television programmes. IPTV is to be rolled out in America in 2005 and is likely to reach British shores in 2007. Internet television has been in development for over a decade with Microsoft being one of the leading firms investing in this new technology. BT has agreed a deal with Microsoft to develop the underlying technology for providing a television network delivered over phone lines.

The aim is to deliver a range of existing TV channels alongside video-on-demand services through a set-top box. Two technical factors have made this possible. Firstly, increased broadband speeds make the launch of video-based services viable. Secondly, there have been significant advances in developing television picture quality on PC screens. Previously, the fonts and pixels used to deliver text and images on a PC screen were incompatible for television. Developers of IPTV have largely solved this problem such that the picture quality on a PC resembles that of conventional televisions.

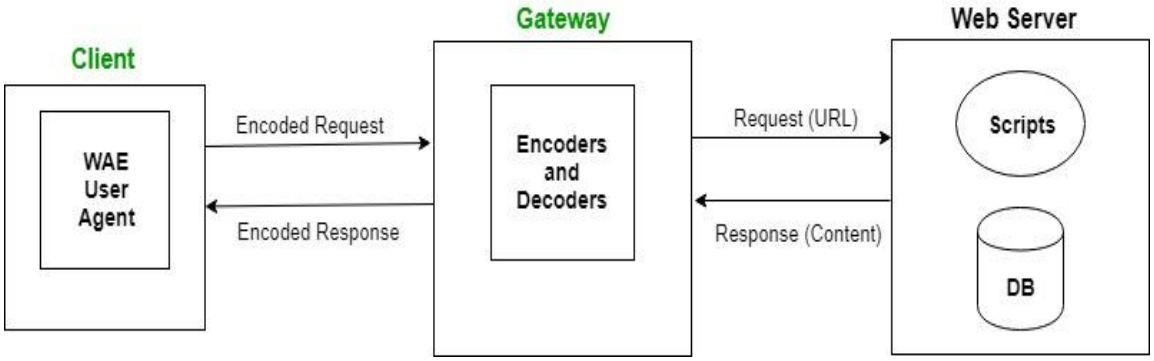
Mobile phone television

Major telecommunications businesses are involved in providing mobile television services. For example, Orange provide a mobile phone TV service in France using 3G technology. Vodaphone already provides a mobile phone TV service in Germany and intends to roll out similar services in the UK to try to boost demand for its 3G services. In Finland, Nokia have been active in experimenting with mobile TV services to determine what their customers want from the service, how they use it and how much they are willing to pay. The development of mobile phone television provides another channel for telecommunication companies, content providers, broadcasters, advertisers and other businesses to reach customers.



WAP Model:

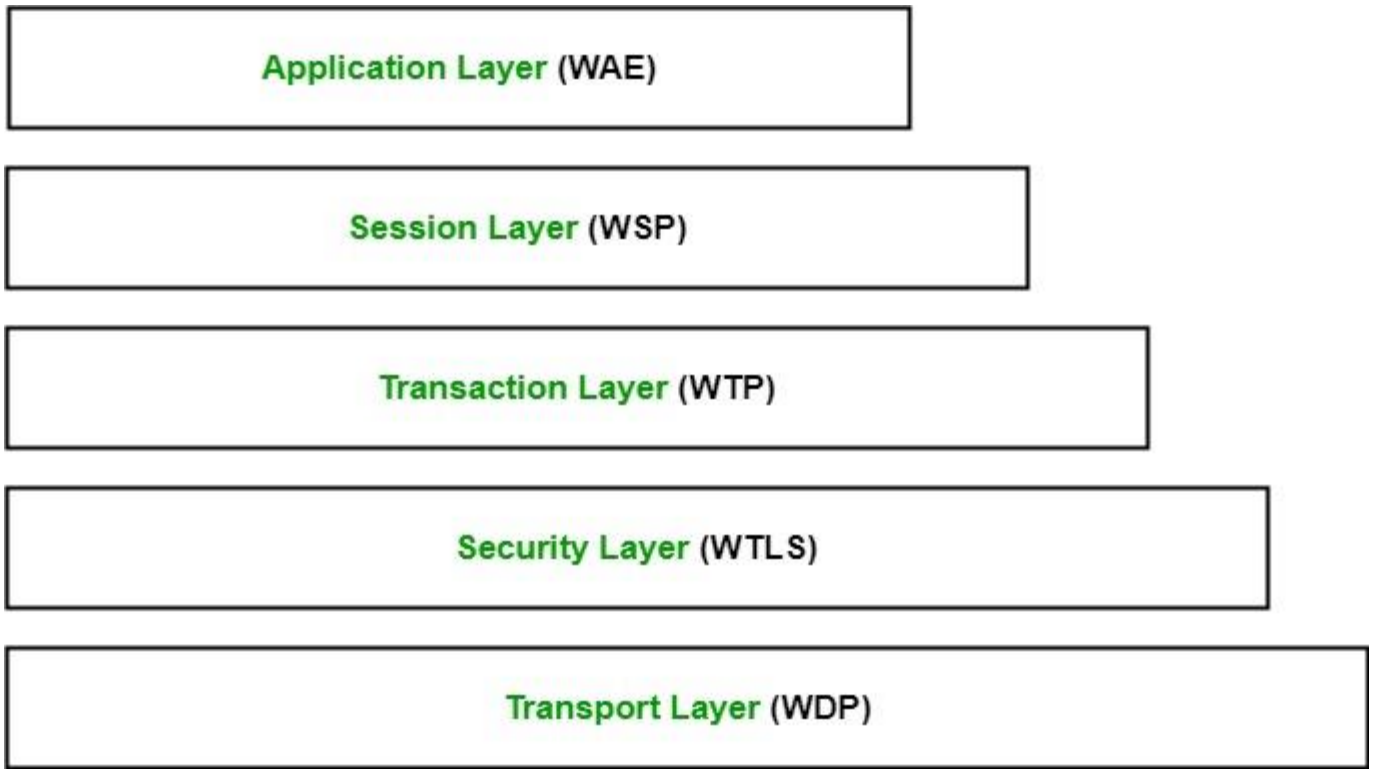
The user opens the mini-browser in a mobile device. He selects a website that he wants to view. The mobile device sends the URL encoded request via network to a WAP gateway using WAP protocol.



ADVERTISING

The WAP gateway translates this WAP request into a conventional HTTP URL request and sends it over the internet. The request reaches to a specified Web server and it processes the request just as it would have processed any other request and sends the response back to the mobile device through WAP gateway in WML file which can be seen in the micro-browser.

WAP Protocol stack:



Application Layer:
This layer contains the Wireless Application Environment (WAE). It contains mobile device specifications and content development programming languages like WML.

Session Layer:
This layer contains Wireless Session Protocol (WSP). It provides fast connection suspension and reconnection.

Transaction Layer:
This layer contains Wireless Transaction Protocol (WTP). It runs on top of UDP (User Datagram Protocol) and is a part of TCP/IP and offers transaction support.

Security Layer:
This layer contains Wireless Transaction Layer Security (WTLS). It offers data integrity, privacy and authentication.

Transport Layer:
This layer contains Wireless Datagram Protocol. It presents consistent data format to higher layers of WAP protocol stack.

WAP is designed in a layered fashion, so that it can be extensible, flexible, and scalable. As a result, the WAP protocol stack is divided into five layers −

Layers of WAP Protocol

Application Layer

Wireless Application Environment (WAE). This layer is of most interest to content developers because it contains among other things, device specifications, and the content development programming languages, WML, and WMLScript.

Session Layer

Wireless Session Protocol (WSP). Unlike HTTP, WSP has been designed by the WAP Forum to provide fast connection suspension and reconnection.

Transaction Layer

Wireless Transaction Protocol (WTP). The WTP runs on top of a datagram service, such as User Datagram Protocol (UDP) and is part of the standard suite of TCP/IP protocols used to provide a simplified protocol suitable for low bandwidth wireless stations.

Security Layer

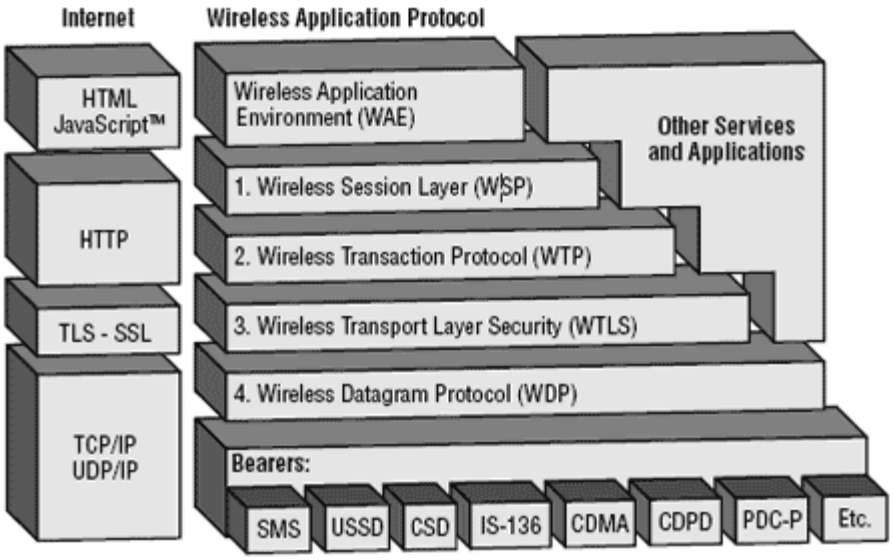
Wireless Transport Layer Security (WTLS). WTLS incorporates security features that are based upon the established Transport Layer Security (TLS) protocol standard. It includes data integrity checks, privacy, service denial, and authentication services.

Transport Layer

Wireless Datagram Protocol (WDP). The WDP allows WAP to be bearer-independent by adapting the transport layer of the underlying bearer. The WDP presents a consistent data format to the higher layers of the WAP protocol stack, thereby offering the advantage of bearer independence to application developers.

Each of these layers provides a well-defined interface to the layer above it. This means that the internal workings of any layer are transparent or invisible to the layers above it. The layered architecture allows other applications and services to utilise the features provided by the WAP-stack as well. This makes it possible to use the WAP-stack for services and applications that currently are not specified by WAP.

The WAP protocol architecture is shown below alongside a typical Internet Protocol stack.



Note that the mobile network bearers in the lower part of the figure above are not part of the WAP protocol stack.

Wireless Application Environment (WAE), the uppermost layer in the WAP stack, provides an environment that enables a wide range of applications to be used on the wireless devices. We have earlier discussed about the WAP WAE programming model. In this chapter, we will focus on the various components of WAE.

Components of WAE

Addressing Model

A syntax suitable for naming resources stored on servers. WAP use the same addressing model as the one used on the Internet that is Uniform Resource Locators (URL).

Wireless Markup Language (WML)

A lightweight markup language designed to meet the constraints of a wireless environment with low bandwidth and small handheld devices. The Wireless Markup Language is WAP's analogy to HTML used on the WWW. WML is based on the Extensible Markup Language (XML).

WMLScript

A lightweight scripting language. WMLScript is based on ECMAScript, the same scripting language that JavaScript is based on. It can be used for enhancing services written in WML in the way that it to some extent adds intelligence to the services; for example, procedural logic, loops, conditional expressions, and computational functions.

Wireless Telephony Application (WTA, WTAI)

A framework and programming interface for telephony services. The Wireless Telephony Application (WTA) environment provides a means to create telephony services using WAP.

Hardware and Software Requirement

At minimum developing WAP applications requires a web server and a WAP simulator. Using simulator software while developing a WAP application is convenient as all the required software can be installed on the development PC.

Although, software simulators are good in their own right, no WAP application should go into production without testing it with actual hardware. The following list gives a quick overview of the necessary hardware and software to test and develop WAP applications −

- A web server with connection to the Internet
- A WML to develop WAP application
- A WAP simulator to test WAP application
- A WAP gateway
- A WAP phone for final testing.

Microsoft IIS or Apache on Windows or Linux can be used as the web server and Nokia WAP Toolkit version 2.0 as the WinWAP simulator.

Please have look at WAP - Useful Resources to find out all the above components.

Configure Web Server for WAP

In the WAP architecture, the web server communicates with the WAP gateway, accepting HTTP requests and returning WML code to the gateway. The HTTP protocol mandates that each reply must include something called a Multi-Purpose Internet Mail Extensions (MIME) type.

In normal web applications, this MIME type is set to text/html, designating normal HTML code. Images on the other hand could be specified as image/gif or image/jpeg for instance. With this content type specification, the web browser knows the data type that the web server returns.

In WAP applications a new set of MIME types must be used, as shown in the following table −

File type	MIME type
WML (.wml)	text/vnd.wap.wml
WMLScript (.wmls)	text/vmd.wap.wmlscript

WBMP (.wbmp)	image/vnd.wap.wbmp

In dynamic applications, the MIME type must be set on the fly, whereas in static WAP applications, the web server must be configured appropriately.

.

The topmost layer in the WAP architecture is made up of WAE (Wireless Application Environment), which consists of WML and WML scripting language.

WML scripting language is used to design applications that are sent over wireless devices such as mobile phones. This language takes care of the small screen and the low bandwidth of transmission. WML is an application of XML, which is defined in a document-type definition.

WML pages are called decks. They are constructed as a set of cards, related to each other with links. When a WML page is accessed from a mobile phone, all the cards in the page are downloaded from the WAP server to mobile phone showing the content.

WML commands and syntaxes are used to show content and to navigate between the cards. Developers can use these commands to declare variables, format text, and show images on the mobile phone.

WAP Program Structure

A WML program is typically divided into two parts − the document prolog and the body. Consider the following code −

```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.2//EN"
"http://www.wapforum.org/DTD/wml12.dtd">
<wml>
  <card>

  ...
  </card>
  ...more cards...
</wml>
```

The first line of this text says that this is an XML document and the version is 1.0. The second line selects the document type and gives the URL of the document type definition (DTD). This DTD gives the full XML definition of WML. The DTD referenced is defined in WAP 1.1, but this header changes with the versions of the WML. The header must be copied exactly so that the tool kits automatically generate this prolog.

The body is enclosed within a <wml>...</wml> tag pair as shown above. The body of a WML document can consist of one or more of the following −

- Deck

- Card
- Content to be shown
- Navigation instructions

WML Commands

The commands used in WML are summarized as follows −

Formatting

Command	Description
<p>	Paragraph
<b>	Bold
<big>	Large
	Emphasized
<I>	Italicized
<small>	Small
	Strongly Emphasized
<u>	Underlined
 	Line Break

Inserting Images

```
<img src="image-path/image - name" alt="Picture not available" />
```

Using Tables

Command	Description
<table>	Definition of a table
<tr>	Defining a row
<td>	Defining a column
<Thead>	Table header

Variables

Declared as −

```
<setvar name="x" value="xyz"/>
```

Used as −

```
$ identifier or
$ (identifier) or
$ (Identifier; conversion)
```

Forms

Command	Description
<select>	Define single or multiple list
<input>	Input from user
<option>	Defines an option in a selectable list
<fieldset>	Defines a set of input fields
<optgroup>	Defines an option group in a selectable list

Task Elements

Command	Description
<go>	Represents the action of switching to a new card
<noop>	Says that nothing should be done
<prev>	Represents the action of going back to the previous card
<refresh>	Refreshes some specified card variables.

Events

The various events are as follows −

Command	Description
<do>	Defines a do event handler
<onevent>	Defines an onevent event handler
<postfield>	Defines a postfield event handler
<ontimer>	Defines an ontimer event handler
<onenterforward>	Defines an onenterforward handler
<onenterbackward>	Defines an onenterbackward handler
<onpick>	Defines an onpick event handler

Sample WML Program

Keep the following WML code into info.wml on your server. If your server is WAP enabled then you can access this page using any WAP device.

```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.2//EN"
"http://www.wapforum.org/DTD/wml12.dtd">
<!-- WML prolog.declaration of file type and version>

<wml>
<!-- Declaration of the WML deck>
<card id="info" newcontext="true">
<!-- declaration of a card in deck>
<p align="center"><b>Information Center</b></p>
<!--paragraph declaration to display heading>
<p>
<!--paragraph declaration to display links>
<a href="Movie.wml">1. Movies info.</a>
<a href="Weather.wml">2. Weather Info.</a>
<!--declaration of links for weather and movies>
</p>
</card>
<!-- card end>
</wml>
<!-- program end>
```