RGPVNOTES.IN

Subject Name: **Web Engineering**

Subject Code: **CS-7003**

Semester: **7th**

Unit-V

E- Commerce: E Commerce stands for electronic commerce and caters to trading in goods and services through the electronic medium such as internet, mobile or any other computer network. It involves the use of Information and Communication Technology (ICT) and Electronic Funds Transfer (EFT) in making commerce between consumers and organizations, organization and organization or consumer and consumer. With the growing use of internet worldwide, Electronic Data Interchange (EDI) has also increased in humungous amounts and so has flourished e-commerce with the prolific virtual internet

bazaar inside the digital world, which is righty termed as e-malls. We now have access to almost every knick-knack of our daily lives at competitive prices on the internet. No matter one is educated or illiterate, an urbane or a fellow citizen, in India or in U.K; all you need is an internet connection and a green bank account. With e-commerce then, you can buy almost anything you wish for without actually touching the product physically and inquiring the salesperson n number of times before placing the final order. Here is a beautiful picture depicting how has human life evolved to adapt to the digital world and hence trading over the internet. As seen, from pizza and potted plant to pair of shoes, we have everything on sale on the internet available in tempting offers..!! Snapdeal.com, Amazon, eBay, Naaptol, Myntra, etc are some of the most popular e-commerce websites. E-Commerce or Electronics Commerce business models can generally categorized in following categories.

Business Models

- Business - to - Business (B2B)
- Business - to - Consumer (B2C)
- Consumer - to - Consumer (C2C)
- Consumer - to - Business (C2B)
- Business - to - Government (B2G)
- Government - to - Business (G2B)
- Government - to - Citizen (G2C)

Business - to - Business (B2B) - Website following B2B business model sells its product to an intermediate buyer who then sells the product to the final customer. As an example, a wholesaler places an order from a company's website and after receiving the consignment, sells the end product to final customer who comes to buy the product at wholesaler's retail outlet.

1. **Features**
2. E-Commerce provides following features-

3. **Non-Cash Payment** – E-Commerce enables use of credit cards, debit cards, smart cards, electronic fund transfer via bank's website and other modes of electronics payment.
4. **24x7 Service availability** – E-commerce automates business of enterprises and services provided by them to customers are available anytime, anywhere. Here 24x7 refers to 24 hours of each seven days of a week.
5. **Advertising / Marketing** – E-commerce increases the reach of advertising of products and services of businesses. It helps in better marketing management of products / services.
6. **Improved Sales** – Using E-Commerce, orders for the products can be generated anytime, anywhere without any human intervention. By this way, dependencies to buy a product reduce at large and sales increases.
7. **Support** – E-Commerce provides various ways to provide pre sales and post sales assistance to provide better services to customers.
8. **Inventory Management** – Using E-Commerce, inventory management of products becomes automated. Reports get generated instantly when required. Product inventory management becomes very efficient and easy to maintain.
9. **Communication improvement** – E-Commerce provides ways for faster, efficient, reliable communication with customers and partners.

Business - to - Business B2B

Website following B2B business model sells its product to an intermediate buyer who then sells the product to the final customer. As an example, a wholesaler places an order from a company's website and after receiving the consignment, sells the product to final customer who comes to buy the product at wholesaler's retail outlet.

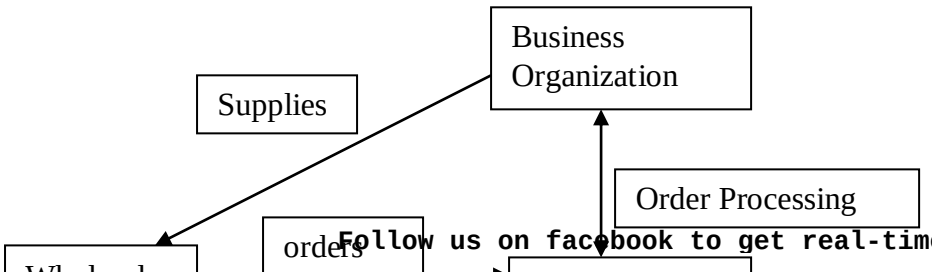

Fig-5.1

Business - to - ConsumerB2C-Business-to-consumer e-commerce, or commerce between companies and consumers, involves customers gathering information; purchasing physical goods (i.e., tangibles such as books or consumer products) or information goods (or goods of electronic material or digitized content, such as software, or e-books); and, for information goods, receiving products over an electronic network. It is the second largest and the earliest form of e-commerce. B2C e-commerce is even more attractive because it saves firms from factoring in the additional cost of a physical distribution network. Moreover, for countries with a growing and robust Internet population, delivering information goods becomes increasingly feasible Website following B2C business model sells its product directly to a customer. A customer can view products shown on the website of business organization. The customer can choose a product and order the same. Website will send a notification to the business organization via email and organization will dispatch the product/goods to the customer.

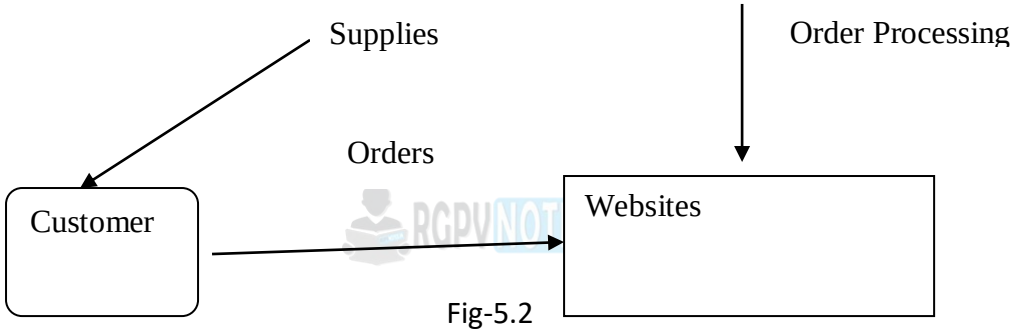

Fig-5.2

Consumer - to - Consumer C2C

Consumer-to-consumer e-commerce or C2C is simply commerce between private individuals or consumers. This type of e-commerce is characterized by the growth of electronic marketplaces and online auctions, particularly in vertical industries where firms/businesses can bid for what they want from among multiple suppliers.16 It perhaps has the greatest potential for developing new markets.

This type of e-commerce comes in at least three forms:

- auctions facilitated at a portal, such as eBay, which allows online real-time bidding on items being sold in the Web;
- peer-to-peer systems, such as the Napster model (a protocol for sharing files between users used by chat forums similar to IRC) and other file exchange and later money exchange models; and
- Classified ads at portal sites such as Excite Classifieds and wanted, Pakwheels.com (an interactive, online marketplace where buyers and sellers can negotiate and which features “Buyer Leads & Want Ads”).

Website following C2C business model helps consumer to sell their assets like residential property, cars, motorcycles etc. or rent a room by publishing their information on the website. Website may or may not charge the consumer for its services. Another consumer may opt to buy the product of the first customer by viewing the post/advertisement on the website.

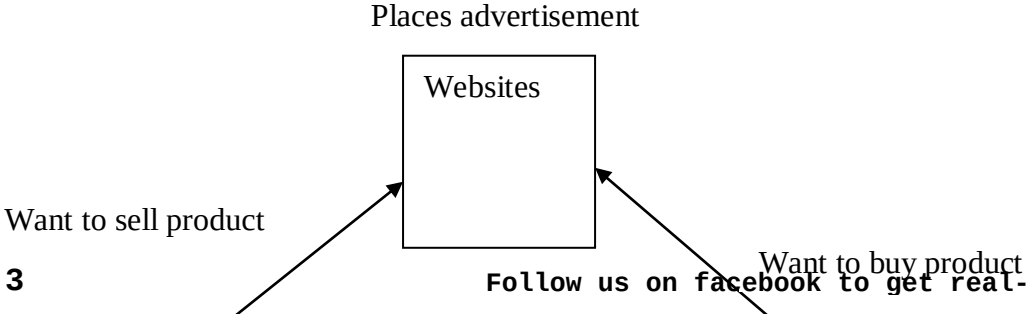

Fig-5.3

Advantages of C2C sites- Consumer to consumer e-commerce have many benefits. The primary benefit to consumers is reduction in cost. Buying ad space on other e-commerce sites is expensive. Sellers can post their items for free or with minimal charge depending on the C2C website. C2C websites form a perfect platform for buyers and sellers who wish to buy and sell related products. The ability to find related products leads to an increase in the visitor to customer conversion ratio. Business owners can cheaply maintain C2C websites and increase profits without the additional costs of distribution locations. A good example of a C2C e-commerce website is Esty, a site that allows consumers to buy and sell handmade or vintage items and supplies including art, photography, clothing, jewelry, food, bath and beauty products, quilts, knick-knacks, and toys.

Disadvantages of C2C sites- There are a couple of disadvantages to these types of sites as well. Doing transaction on these types of websites requires co-operation between the buyer and seller. It has been note many times that these two do not co-operate with each other after a transaction has made. They do not share the transaction information, which may be via credit or debit card or internet banking. This can result in online fraud since the buyer and seller is not very well verse with each other. This can lead to lawsuit being impose either on ends or also on the site if it has not mentioned the disclaimer in its terms and conditions. This may also hamper the c2c website's reputation.

Consumer - to - Business C2B- In this model, a consumer approaches website showing multiple business organizations for a particular service. Consumer places an estimate of amount he/she wants to spend for a particular service. For example, comparison of interest rates of personal loan/ car loan provided by various banks via website. Business organization that fulfils the consumer's requirement within specified budget approaches the customer and provides its services.

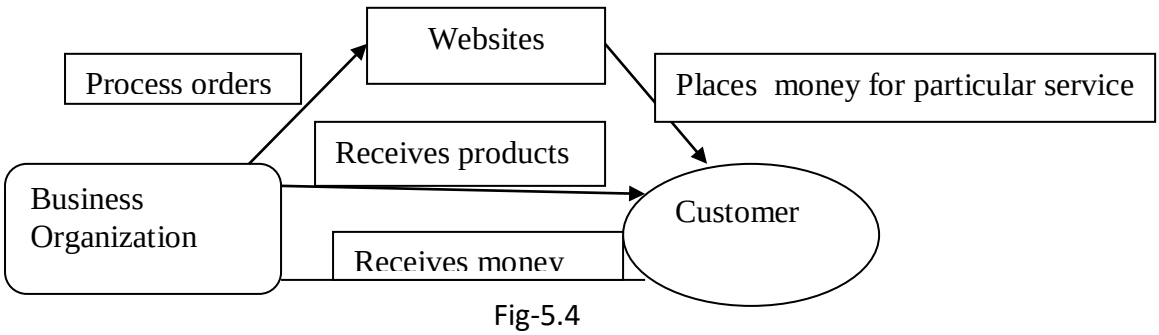

Fig-5.4

Business - to - Government B2G- Business-to-government e-commerce or B2G is generally defined as commerce between companies and the public sector. It refers to the use of the Internet for public procurement, licensing procedures, and other government-related operations. This kind of e-commerce has two features: first, the public sector assumes a pilot/leading role in establishing e-commerce; and second, it is assume that the public sector has the greatest need for making its procurement system more effective. Web-based purchasing policies increase the transparency of the procurement process (and reduce the risk of irregularities). To date, however, the size of the B2G e-commerce market, as a component of total e-commerce is insignificant, as government e-procurement, systems remain undeveloped. B2G model is a variant of B2B model. Such websites are used by government to trade and exchange information with various business organizations. Such websites are accrediting by the government and provide a medium to businesses to submit application forms to the government.

Fig-5.5

Government - to - Business G2B

Government uses B2G model website to approach business organizations. Such websites support Auctions, tenders and application submission functionalities

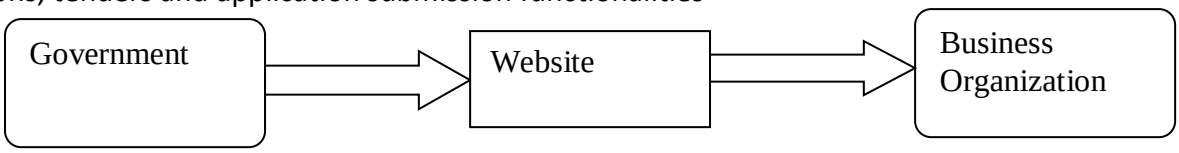

Fig-5.6

Government - to - Citizen G2C

Government uses G2C model website to approach citizen in general. Such websites support auctions of vehicles, machinery or any other material. Such website also provides services like registration for birth, marriage or death certificates. Main objectives of G2C website are to reduce average time for fulfilling people requests for various government services.

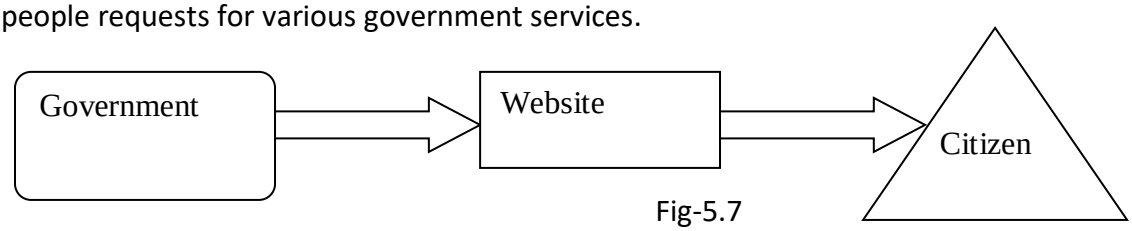

Fig-5.7

Internet relevant to e-commerce

The Internet allows people from all over the world to get connected inexpensively and reliably. As a technical infrastructure, it is a global collection of networks, connected to share information using a common set of protocols. Also, as a vast network of people and information, the Internet is an enabler for e-commerce as it allows businesses to showcase and sell their products and services online and gives potential customers, prospects, and business partners access to information about these businesses and their products and services that would lead to purchase.

Infrastructure-Every business requires an infrastructure to support its customers and operations. This includes facilities, equipment, and processes to support all the functional areas of your business. Choosing the correct infrastructure to match your business strategies enables your operations to run efficiently. Conversely, if an element of your infrastructure is uncoordinated with your strategies, you will likely feel the pain in every aspect of your business.

Here are seven important infrastructure decisions that ecommerce businesses face.

1.**Marketing** - Of all the infrastructure elements, marketing may be the most important. To succeed, your website must be found. Once visitors are on your site, you need to keep them there and compel them to buy from you. That's the job of your marketing team. Whether it's website design, social media, search marketing, merchandising, email, or other forms of advertising, it's all about marketing. To effectively manage marketing activities in-house is very challenging. Most small ecommerce businesses outsource some element of marketing.

2.**Facilities** - A key competitive advantage that ecommerce businesses have over brick-and-mortar stores is the investment in their physical offices and warehouses. In many cases, you can host your business out of a home office and your basement or garage. If you drop ship or outsource fulfilment, you may be able to do that for a long period. Even when you grow to have many employees, you can set up your offices in class B or C space, as you have no need for a fancy store in the right location. A word of advice is to keep your options flexible. Try to find an office park that has a wide variety of spaces in different sizes. You may be able to start in a smaller space and move up to a larger one without penalty, as your needs change.

3.**Customer Service** - There are many choices today for delivering high-quality customer service. You can

manage those activities in-house or outsource to a third party. Basic customer service for sales and post-sales activities can be handled using email, and by providing an 800 number for more extensive phone support. A customer-management system will make those activities easier, but for smaller companies it is not a requirement. Live chat will affect your operations, as someone needs to be available during specified hours of operation. Be sure to gauge the impact of that on your organization, if you decide to handle those activities in house.

4.**Information Technology** - Choosing the right ecommerce platform is one of the most important decisions you will make in your business. Do you want to build and host your own system, outsource the development and then manage the system going forward, or use a hosted, software-as-a-service platform that is more turnkey and externally managed?

If you build and host your own system, you may need more cash up front and skilled administrators and developers on your staff. By using a SaaS platform, you will not need to host or manage the system in-house, but you may still need web developers on staff. Choosing to outsource the development and hosting will reduce your staffing costs, but you will incur higher costs for any future enhancements or changes to your websites. There are pros and cons to any approach. Just be sure to think through the impacts on both your staffing and your cash flow and bottom line before you move forward.

5.**Fulfilment** - Another key decision is whether you will manage your own inventory or outsource those activities to a fulfilment house or through drop shipping arrangements with your suppliers.

6.**Finance and Administration** - As with other business operations, you will need to decide if you want to manage your finance and administration activities in-house, outsource, or a hybrid of the two. If your ecommerce platform is tightly integrated to your accounting system, you may have very little need for an in-house bookkeeper. If you use separate systems for your website, order management and accounting, you may need more help for data entry and making sure that the information is properly managed many ecommerce companies use outside services for vendor payments, payroll, and other basic accounting activities. They decide to focus on the sales, marketing, and customer service. On the administration side, you need a leadership team and provide direction to them. Good communication is important, whether you have 3 or 100 employees. Whether you choose to be more authoritative or democratic in your management style is up to you. But choose a style and stay consistent. Be sure that everyone understands their roles, as well as the overall business strategies. You may need to adjust your approach as your business evolves.

7.Human Resources - Many small-business owners avoid the human resources function. Recruiting, setting up compensation, maintaining compliance and other HR activities are specialized and time consuming. You may choose to bring the resources in-house to manage those activities, but also evaluate outsourcing them. There are many individuals and agencies well equipped to take on your HR activities.

Environment and Opportunities- Electronic commerce includes all forms of business transactions, such as the purchase of goods or services, undertaken through electronic means, such as telephones, televisions, computers, and the Internet. It is believe to be the means through which most business will conduct in the future. With the growing numbers of people connecting to the Internet, electronic commerce is gaining rapid acceptance. Many people think of electronic commerce in terms of shopping on the Internet, or shopping on-line, but it is really much more than that. Electronic commerce affects our lives in more ways than we realize.

- A manufacturer-checking inventory on parts at a supplier's warehouse through the Internet in evolved in electronic commerce.
- A direct deposit transaction, such as the direct deposit of a paycheck or a tax refund into a bank account, is an electronic commerce transaction.
- A person advertising a seldom used exercise bike on-line is engaging in electronic commerce.
- Each time someone takes money out of an ATM, or uses a debit or credit card to purchase goods or services, that person is taking part in electronic commerce.
- A catalogue shopper placing an order over the telephone is also participating in electronic commerce.

Electronic commerce may be in the form of business-to-business activities, business to consumer, or direct consumer to consumer contacts. Links to governments, educational institutions, libraries and not-for-profit organizations are all a part of the electronic commerce environment. Goods, services, and information are the content of electronic commerce; the whole world is its venue.

Modes & Approaches-

1. For real time e-commerce, the merchant establishes the internet merchant facility with their bank, integrates the payment gateway, and uses either a shopping cart or order form for information capture. From a security point of view the advantage of using a payment gateway means that the customer's details (name, address, credit card number) are not captured (or seen) by the merchant but rather are captured by the payment gateway provider only. Also the transfer of the customer's details from the merchant's website to the payment gateway is secure (encrypted) and cannot be intercepted.
2. Another approach is where the merchant uses a third party hosted solution such as Paypal, Worldpay or Pay mate who look after some or all of the key components of e-commerce. The advantage is the ease in which the Australian company can charge the customer in different currencies without having to establish dedicated currency bank accounts.
3. The last approach and the least preferred from a security perspective is where the merchant uses either a shopping cart or order form for information capture and then manually re-keys the credit card number into an EFTPOS facility they have leased from a bank. Essentially the website captures the order information and the transaction is process manually off-line. With this approach, the company does not require a payment gateway service because the transaction is not in real time.

Marketing & Advertising Concepts- Ecommerce marketing is the process of driving sales by raising awareness about an online store's brand and product offerings. Digital marketing for ecommerce applies traditional marketing principles to a multichannel, data-driven environment. Ecommerce marketing can divided into two general actions: driving website traffic and optimizing the user experience for conversion. Both are critical components to growing an online business — failure in one is all but sure to undermine any success in the other. Seasoned marketers can thrive in a digital landscape, starting with a solid foundation of common terms.

Ecommerce Marketing Channels

- **Pay-per-click Advertising (PPC)**: Effective PPC campaigns drive users with intent to purchase, making it more efficient than many traditional advertising platforms. Businesses bid on impressions for paid listings at the top of search engine results, paying on a per-click basis. Impressions are determined by user search query, with strategy revolving around which keyword bids yield the highest ROI.
- **Search Engine Marketing (SEM**): Sometimes used a synonym for PPC, referring to paid advertising campaigns. SEM is often use to describe efforts on Google's AdWords platform and paid platforms on other search engines, such as Bing. This multifaceted term is also used by many marketer to describe all paid and organic efforts.
- **Search Engine Optimization (SEO)-** Unlike the paid media opportunities described above, SEO traffic comes from unpaid "organic" results on search engines such as Google and Yahoo.
- **Display Advertising-** Banners, sidebars and other predominantly visual advertisements that appear on other websites. Display ads are facilitating by ad networks such as Google Display Network.
- **Affiliate Marketing-** Referrals from other websites with industry or product-focused content such as reviews, comparisons, and testimonials. Successful affiliates have a loyal following or receive traffic from some of the above channels. They typically receive a set commission of referred sales, often determined on a case-by-case basis.
- **Email Marketing**: Newsletters, abandoned cart notifications and remarketing all use email to target past and potential customers.

Ecommerce Marketing terms

- **Google AdWords-** Google's advertising platform pioneers the PPC model and capitalizes on the company's majority share of the search market.
- **Search Engine Results Page (SERP):** The cumulative results from users executing a search engine query, comprising organic and paid listings. Having results on the first page of SERPs is critical to acquiring new customers.

- **Conversion Rate Optimization (CRO)-** The process of improving every aspect of a website so that more visitors purchase. Faster load times, fewer clicks to purchase and more enticing product descriptions/images make it easier for user's to evaluate your products and follow through to The most common metric for evaluating CRO efforts is conversion rate.
- **Conversion Funnel-** The steps taken by a prospect to become a customer begin with awareness and ending with a purchase. Higher-priced items generally have a longer sales cycle, while low-cost items can convert in a much shorter period.

Electronic Publishing issues- **Electronic publishing** is electronic commerce in digital goods and services that are intended for consumption by the human senses

It encompasses a wide range of formats, including:

- text;
- structured data;
- image, both raster/bit-map and vector;
- moving image (animation and video);
- sound; and
- Combinations of the above ('multi-media').

The following are examples of the kinds of digital goods and services that are encompassed by that definition:

- documents in electronic form, including articles and books;
- data, such as statistical tables;
- low-volatility reference information, such as dictionaries and encyclopaedias;
- high-volatility reference information, such as news, sports reports and weather forecasts;
- speeches;
- musical performances;
- cartoons;
- films and video-clips; and
- Entertainment, infotainment, edutainment and education.

A more developed and mature e-banking environment plays an important role in e-commerce by encouraging a shift from traditional modes of payment (i.e., cash, checks or any form of paper-based legal tender) to electronic alternatives (such as e-payment systems), thereby closing the e-commerce loop.

a) Benefits of e-Commerce

- Expanded Geographical Reach
- Expanded Customer Base
- Increase Visibility through Search Engine Marketing
- Provide Customers valuable information about your business
- Available 24/7/365 - Never Close
- Build Customer Loyalty
- Reduction of Marketing and Advertising Costs
- Collection of Customer Data

b) Basic Benefits of e-Business e-Commerce

- Increase sales - this is the first thing that people consider when dealing with e-commerce
  - Decreasing costs
  - Increase profits
    - Understanding that profits is not the same as sales
  - Expands the size of the market from regional to national or national to international
  - Contract the market
  - Reach a narrow market
    - Target market segmentation allows you to focus on a more
    - Select group of customers
    - And therefore have a competitive advantages in satisfying them

Ecommerce legalities and technologies- A technological innovation is followed by frequent incorporation of ethical standards into law. New forms of E-Commerce that enables new business practices have many advantages but also bring numerous risks.

Let us discuss about the ethical and legal issues related to e-business.

Ethical Issues-In general, many ethical and global issues of Information Technology apply to e-business. So, what are the issues particularly related to e-commerce.

Web tracking-E-businesses draw information on how visitors use a site through log files. Analysis of log file means turning log data into application service or installing software that can pluck relevant information from files in-house. Companies track individual's movement through tracking software and cookie analysis. The battle between computer end users and web trackers is always going on with a range of application programs.

Privacy-Most Electronic Payment Systems knows the identity of the buyer. Therefore, it is necessary to protect the identity of a buyer who uses Electronic Payment System. A privacy issue related to the employees of company is tracking. Monitoring systems are installed in many companies to monitor e-mail and other web activities in order to identify employees who extensively use business hours for non-business activities. The e-commerce activities performed by a buyer can be tracked by organizations. For example, reserving railway tickets for their personal journey purpose can be tracked. Many employees do not want to be under the monitoring system even while at work.

Disintermediation and Reinter mediation-Intermediation is one of the most important and interesting e-commerce issue related to loss of jobs. The services provided by intermediaries are

(i) Matching and providing information.

(ii) Value added services such as consulting.

The first type of service (matching and providing information) can be fully automated, and this service is likely to be in e-marketplaces and portals that provide free services.

Legal Issues- Internet fraud and its sophistication have grown even faster than the Internet itself. There is a chance of a crime over the internet when buyers and sellers do not know each other and cannot even see each other. During the first few years of e-commerce, the public witnessed many frauds committed over the internet. Let us discuss the legal issues specific to e-commerce.

Fraud on the Internet-E-commerce fraud popped out with the rapid increase in popularity of websites. It is a hot issue for both cyber and click-and-mortar merchants. The swindlers are active mainly in the area of stocks. The small investors are lured by the promise of false profits by the stock promoters. Auctions are also conductive to fraud, by both sellers and buyers. The availability of e-mails and pop up ads has paved the way for financial criminals to have access to many people. Other areas of potential fraud include phantom business opportunities and bogus investments.

Copyright-The copyright laws protect Intellectual property in its various forms, and cannot be used freely. It is very difficult to protect Intellectual property in E-Commerce. For example, if you buy software you have the right to use it and not the right to distribute it. The distribution rights are with the copyright holder. In addition, copying contents from the website also violates copyright laws.

Domain Names- The competition over domain names is another legal issue. Internet addresses are known as domain names and they appear in levels. A top-level name is qburst.com or microsoft.com. A second level name will be qburst.com/blog. Top-level domain names are assigned by a central non-profit organization, which also checks for conflicts or possible infringement of trademarks. Problems arise when several companies having similar names competing over the same domain name.

Secure Web document, - Non-technical Issues

1. **Security Awareness-** Most opinion surveys list "insecurity of financial transactions" and "loss of privacy" among the major impediments to electronic commerce, but in fact most users have only ague ideas about the threats and risks, and a very limited understanding of the technical and legal options for minimizing their risk. As a result, all kinds of misperceptions exist.

For instance, the cardholder's risk in sending his or her credit card number over the Internet is typically overestimated. At least as of this writing payments over the Internet are treat like mail-order/telephone-order transactions, which means that the cardholder is not liable at all. All risk is with the merchant. On the other hand, the risks in sending sensitive data in an electronic mail are typically underestimated. Probably

most users of email know the mere facts: neither confidentiality nor integrity nor availability is guarantee. However, many users do not hesitate to send all kind of very personal and sensitive data to their friends or colleagues, unprotected. Unfortunately, developers of electronic commerce solutions are often as security unaware and ignorant as their prospective users. For instance, still many developers demand that “lower layers” must provide security in a "transparent" way. However, for instance, Secure Socket Layer (SSL) in “opaque socket integration" does not make any sense in most case. Security has to be an integral part of the architecture, design, and implementation.

2. **Crypto Regulations-** Several countries regulate the deployment of strong encryption technology by law. For instance, France controls the domestic use of encryption technology, in order to maintain the capability to eavesdrop on the communication of criminals. The USA prohibits the export of strong encryption products for the mass market, for the same reasons as it controls the export of munitions.

Such regulations do not discriminate between “good” and “bad” applications, and limit the security of honest citizens and companies to at least the same extent as they limit the security of terrorists and organized crime. Therefore several governments, in particular the US administration, are willing to relax their crypto regulations, provided access to the encrypted information would still be possible on demand. The idea is to introduce new “Trusted Third Parties” where secret keys must either be escrowed in advance, or can be recovered afterwards. All these proposals are heavy contested, for various technical and political reasons: The Trusted Third Parties would be “single points of failure” for everybody’s, i.e., new and extremely attractive targets for attacks. It is questionable whether any regulation of encryption technology can be effective in fighting organized crime: tools for strong encryption are publicly available, and steganography techniques can perfectly conceal the fact that cryptographic techniques are applied. Many types of commercial transactions require strong confidentiality, which cannot be satisfied in some countries, or across some borders. For instance, consider two large companies that prepare a merger. Clearly, their negotiations require top confidentiality. Even the fact that they are preparing the merger, i.e., that they are communicating intensively, will be extremely sensitive. This requires actually services for anonymous communication. Nevertheless using the appropriate cryptographic tools would be illegal in many countries. Political regulations are not subject to scientific research. However, we clearly see the need for an international agreement on a more liberal and consistent regulation of cryptography. Electronic commerce demands strong confidentiality, which can implement only by strong encryption schemes.

3. Legal Issues- Surveying the open legal problems in electronic commerce is beyond the scope of this article. The two most important security-related problems are the following:

- Liability: The financial risk of a user in a specific transaction depends on his or her liability. In principle, if a user bears no liability, there is no risk.

The main issue here is fairness: The liability of a user should correspond to the security of his or her technical equipment. For instance, if it is technically trivial to forge the digital signature of a user then this party should not held liable for his or her signatures, in general.

- Harmonization: The national laws that regulate electronic commerce over the Internet (like evidential value of digital signatures, consumer protection, and copyright protection) is not harmonized, and are contradictory. One side result is that there is no mutual recognition between national PKIs, even where comparable laws exist.

Technical Components of e-commerce Security- There are four components involved in Ecommerce Security: client software, server software, the server operating system, and the network transport. Each component has its own set of issues and challenges associated with securing them:

- Client software is becoming increasingly more security-focused; however, single-user desktop operating systems historically have had no security features implemented. Ecommerce software that relies on the security of the desktop operating system easily compromised without the enforcement of strict physical controls.
- Server software is constantly under test and attack by the user community. Although there have been cases of insecurities, a system administrator keeping up with the latest patches and vendor information can provide a high degree of confidence in the security of the server itself.

- Operating systems used for hosting Ecommerce servers are securable, but rarely shipped from the vendor in a default configuration that is secure. Ecommerce servers must protect the database of customer information accumulating on the server as well as provide security while the server is handling a transaction. If it is easier for a thief to compromise the server to obtain credit card numbers, why bother sniffing the network for individual credit card numbers.

Session transport between the client and server uses network protocols that may have little or no built-in security. In addition, networking protocols such as TCP/IP were not design to have confidentiality or authentication capabilities

Cryptography & Pretty Good Privacy (PGP)

1. The need for cryptography in electronic communications

Cryptography has been around for centuries; as long as there has been communication, there has been the need for privacy and safe, secure methods of transmission. Although many types of difficult problems can be classify as cryptography problems, what we are mostly concerned with today is the ability to keep transmissions private with data encryption techniques. This has become an even greater issue due to the changing nature of communications since the information revolution. More and more people rely on electronic communications for the transmission of sensitive or personal data; e-mail, e-commerce, FTP, and HTML are all examples of technology that have already filtered into the social consciousness as primary ways for disseminating and gathering information and for exchanging goods and services. While this technological shift has made communication faster, easier, and better in many ways, it has also brought along with it a whole host of difficult problems and social policy issues.

The main problem that comes with electronic communications is the ease with which transmissions can be eavesdropped or impersonated. Paper communications obviously have security problems as well: documents can be stolen, steamed open, have forged signatures or changed contents. However, if someone is trying to catch a specific transmission (or type of communication), it is much easier when dealing with an electronic medium. Also, since there can be (and often are) multiple copies of any given electronic transmission, it is difficult to know if someone has stolen a copy or somehow altered the original.

Secondly, there is an access control problem. Many electronic transmissions are made in a broadcast manner, as seen with cable or satellite television and wireless phones. People can install devices to intercept these transmissions, and senders usually have no way to either monitor or stop this. In order to prevent unwanted people from making free use of their services, senders must encrypt their outgoing transmissions. To their paying customers, they can give special devices to decrypt the information.

Finally, there is the problem of authentication: electronic communications are impersonal, and can be easily forged by impersonating IP addresses, changing "sender fields" in e-mail, "cloning" cellular phone numbers, and so forth. In order for people to want to - and, indeed, be able to - use electronic communication in the coming years, it is essential that these problems be resolved. Right now, advances in cryptography are the best way to address these issues. Data encryption not only provides privacy and access control by rendering communications illegible to unauthorized parties; it can provide effective authentication as well through the use of digital signatures and timestamps.

2. The primary forms of cryptography

There are two main forms of cryptography: secret-key (or symmetric) and public-key (or asymmetric).

Secret-key cryptography

Secret-key cryptography is the more traditional form, and has been used for all kinds of communications throughout the ages. In this method, one "key" is used to both encrypt and decrypt the data. A key can be anything from a secret-decoder ring found in a cereal box to a highly complex mathematical algorithm; keys really only differ in the ease with which they can be broken by third parties. In secret-key cryptography, the sender and receiver must have the same key in order for the transmission to work correctly.

Secret-key cryptography suffers from two overwhelming problems. First, any two people that want to communicate with each other must first agree on the key to use. This makes it more difficult to send information to people that you do not already know, and large-scale communication becomes much more difficult. The second, more fundamental, problem is that of "key management", which the system for

transmission and storage of keys is. In order to agree on a key, there must first be some sort of communication that occurs, and this communication itself can be eavesdropped. If some third party catches the key that is used, then all further communications between the two parties are no longer secure and private. In addition, the third party could easily impersonate communications because it is believe that no one else knows the key. This problem is exacerbating by the fact that the initial parties might have no way of knowing that the key stolen. This key management issue causes a "repudiation problem": later on, either of the parties could repudiate messages that had sent with secret-key encryption, claiming that the key had stolen and that the messages were compromised or faked. Thus, there is always an inherent lack of security and trust in a purely secret-key environment.

Public-key cryptography

The key management problem inherent to secret-key cryptography needed to be address in order for large-scale, secure use of data encryption techniques. In 1976, Whitfield Diffie, a cryptographer and privacy advocate, and Martin Hellman, an electrical engineer, working together discovered the concept of public-key encryption. Instead of having one key shared between both users of an encrypted transmission, each user has his or her own public/private key pair. A user makes the public key open and available to anyone (by publishing it on-line or registering it with a public key server), and keeps the private key hidden away where (hopefully) no one can get at it. In order to send someone a message, the sender encrypts the transmission with the receiver's public key. This can then decrypt by the receiver's private key. Thus, anyone can encrypt a message with someone else's public key, but only that person would ever be able to read it. This method solves the problems of secret-key cryptography. Because the only key information that needs to share is made public, there is no worry about some third party intercepting and possessing the key. This makes the users of the encryption surer that their transmissions are secure and private. It also solves the repudiation problem; because there is no third party that could ever be blame-each individual is responsible for safeguarding his or her own private key.

The inherent weakness of the public-key method is that the two keys are link together mathematically. If a third party figures out the exact way that an individual's private key is derive from his or her public key, the whole security of the system will be lost. The only way around this liability (so far) has been to make the derivation so incredibly complex that a brute force attempt to crack it would take a prohibitively long amount of time. It is easy to see that the quality of the method used to create keys is essential to the success of any public-key system.

Digital Signatures – The digital equivalent of a handwritten signature or stamped seal, but offering far more inherent security, a digital signature is intended to solve the problem of tampering and impersonation in digital communications. Digital signatures can provide the added assurances of evidence to origin, identity and status of an electronic document, transaction or message, as well as acknowledging informed consent by the signer.

In many countries, including the United States, digital signatures have the same legal significance as the more traditional forms of signed documents. The United States Government Printing Office publishes electronic versions of the budget, public and private laws, and congressional bills with digital signatures.

How digital signatures work

Digital signatures based on public key cryptography, also known as asymmetric cryptography. Using a public key algorithm such as RSA, one can generate two keys that are mathematically link: one private and one public. To create a digital signature, signing software (such as an email program) creates a one-way hash of the electronic data to be sign. The private key is then use to encrypt the hash. The encrypted hash -- along with other information, such as the hashing algorithm -- is the digital signature. The reason for encrypting the hash instead of the entire message or document is that a hash function can convert an arbitrary input into a fixed length value, which is usually much shorter. This saves time since hashing is much faster than signing. If the two hash values match, the message has not been Tampere with, and the receiver knows the message is from sender. Most modern email programs support the use of digital signatures and digital certificates, making it easy to sign any outgoing emails and validate digitally signed incoming messages. Digital signatures use extensively to provide proof of authenticity, data integrity and non-repudiation of communications and transactions conducted over the Internet.

FIREWALL-A firewall is a set of related programs, located at a network gateway server, that protects the resources of a private network from users from other networks. (The term also implies the security policy that is used with the programs.) An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources and for controlling what outside resources its own users have access to.Basically, a firewall, working closely with a router program, examines each network packetto determine whether to forward it toward its destination. A firewall also includes or works with a proxy server that makes network requests on behalf of workstation users. A firewall is often installed in a specially designated computer separate from the rest of the network so that no incoming request can get directly at private network resources.There are a number of firewall screening methods. A simple one is to screen requests to make sure they come from acceptable (previously identified) domain name and Internet Protocol addresses. For mobile users, firewalls allow remote access in to the private network by the use of secure logon procedures and authentication certificates. A number of companies make firewall products. Features include logging and reporting, automatic alarms at given thresholds of attack, and a graphical user interface for controlling the firewall.Computer security borrows this term from firefighting, where it originated. In firefighting, a firewall is a barrier established to prevent the spread of fire.

Cyber Crime- It could be hackers vandalizing your site, viewing confidential information, stealing trade secrets or intellectual property with the use of internet. It can also include 'denial of services' and viruses attacks preventing regular traffic from reaching your site. Cybercrimes are not limited to outsiders except in case of viruses and with respect to security, related cybercrimes that usually done by the employees of particular company who can easily access the password and data storage of the company for their benefits. Cybercrimes also includes criminal activities done with the use of computers which further perpetuates crimes i.e. financial crimes, sale of illegal articles, pornography, online gambling, intellectual property crime, e-mail, spoofing, forgery, cyber defamation, cyber stalking, unauthorized access to Computer system, theft of information contained in the electronic form, e-mail bombing, physically damaging the computer system etc.

Classifications Of Cyber Crimes: Cyber Crimes which are growing day by day, it is very difficult to find out what is actually a cybercrime and what is the conventional crime so to come out of this confusion, cybercrimes can be classified under different categories which are as follows:

1. **Cyber Crimes against Persons:**

There are certain offences which affect the personality of individuals can be defined as:

Harassment via E-Mails: It is very common type of harassment through sending letters, attachments of files & folders i.e. via e-mails. At present harassment is common as usage of social sites i.e. Facebook, Twitter etc. increasing day by day.

Cyber-Stalking: It means expressed or implied a physical threat that creates fear through the use to computer technology such as internet, e-mail, phones, text messages, webcam, websites or videos.

Dissemination of Obscene Material: It includes Indecent exposure/ Pornography (basically child pornography), hosting of web site containing these prohibited materials. These obscene matters may cause harm to the mind of the adolescent and tend to deprave or corrupt their mind.

Defamation: It is an act of imputing any person with intent to lower down the dignity of the person by hacking his mail account and sending some mails with using vulgar language to unknown persons mail account.

Hacking: It means unauthorized control/access over computer system and act of hacking completely destroys the whole data as well as computer programmes. Hackers usually hacks telecommunication and mobile network.

Cracking: It is amongst the gravest cybercrimes known till date. It is a dreadful feeling to know that a stranger has broken into your computer systems without your knowledge and consent and has tampered with precious confidential data and information.

E-Mail Spoofing: A spoofed e-mail may be said to be one, which misrepresents its origin. It shows its origin to be different from which actually it originates.

SMS Spoofing: Spoofing is a blocking through spam which means the unwanted uninvited messages. Here a offender steals identity of another in the form of mobile phone number and sending SMS via internet

and receiver gets the SMS from the mobile phone number of the victim. It is very serious cybercrime against any individual.

Crimes against Persons Property:

As there is rapid growth in the international trade where businesses and consumers are increasingly using computers to create, transmit and to store information in the electronic form instead of traditional paper documents. There are certain offences which affects person's properties which are as follows:

Intellectual Property Crimes: Intellectual property consists of a bundle of rights. Any unlawful act by which the owner is deprived completely or partially of his rights is an offence. The common form of IPR violation may be said to be software piracy, infringement of copyright, trademark, patents, designs and service mark violation, theft of computer source code, etc.

- **Cyber Squatting:** It means where two persons claim for the same Domain Name either by claiming that they had registered the name first on by right of using it before the other or using something similar to that previously. For example two similar names i.e. www.yahoo.com and www.yaahoo.com.
- **Cyber Vandalism:** Vandalism means deliberately destroying or damaging property of another. Thus cyber vandalism means destroying or damaging the data when a network service is stopped or disrupted. It may include within its purview any kind of physical harm done to the computer of any person. These acts may take the form of the theft of a computer, some part of a computer or a peripheral attached to the computer.
- **Hacking Computer System:** Hacktivism attacks those included Famous Twitter, blogging platform by unauthorized access/control over the computer. Due to the hacking activity there will be loss of data as well as computer. Also research especially indicates that those attacks were not mainly intended for financial gain too and to diminish the reputation of particular person or company.
- **Transmitting Virus:** Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worm attacks plays major role in affecting the computerize system of the individuals.
- **Cyber Trespass:** It means to access someone's computer without the right authorization of the owner and does not disturb, alter, misuse, or damage data or system by using wireless internet connection.
- **Internet Time Thefts:** Basically, Internet time theft comes under hacking. It is the use by an unauthorised person, of the Internet hours paid for by another person. The person who gets access to someone else's ISP user ID and password, either by hacking or by gaining access to it by illegal means, uses it to access the Internet without the other person's knowledge. You can identify time theft if your Internet time has to be recharged often, despite infrequent usage.

3. **Cybercrimes against Government:**There are certain offences done by group of persons intending to threaten the international governments by using internet facilities. It includes:

- **Cyber Terrorism:** Cyber terrorism is a major burning issue in the domestic as well as global concern. The common form of these terrorist attacks on the Internet is by distributed denial of service attacks, hate websites and hate e-mails, attacks on sensitive computer networks etc. Cyber terrorism activities endanger the sovereignty and integrity of the nation.
- **Cyber Warfare:** It refers to politically motivated hacking to conduct sabotage and espionage. It is a form of information warfare sometimes seen as analogous to conventional warfare although this analogy is controversial for both its accuracy and its political motivation.
- **Distribution of pirated software:** It means distributing pirated software from one computer to another intending to destroy the data and official records of the government.
- **Possession of Unauthorized Information:** It is very easy to access any information by the terrorists with the aid of internet and to possess that information for political, religious, social, ideological objectives.

4. Cybercrimes Against Society at large:

An unlawful act done with the intention of causing harm to the cyberspace will affect large number of persons. These offences include:

- **Child Pornography:** It involves the use of computer networks to create, distribute, or access materials that sexually exploit underage children. It also includes activities concerning indecent exposure and obscenity.
- **Cyber Trafficking:** It may be trafficking in drugs, human beings, arms weapons etc. which affects large number of persons. Trafficking in the cyberspace is also a gravest crime.
- **Online Gambling:** Online fraud and cheating is one of the most lucrative businesses that are growing today in the cyber space. There are many cases that have come to light are those pertaining to credit card crimes, contractual crimes, offering jobs, etc.
- **Financial Crimes:** This type of offence is common as there is rapid growth in the users of networking sites and phone networking where culprit will try to attack by sending bogus mails or messages through internet. Ex: Using credit cards by obtaining password illegally.
- **Forgery:** It means to deceive large number of persons by sending threatening mails as online business transactions are becoming the habitual need of today's life style.

Cyber Law: information technology has spread throughout the world. The computer is used in each sector wherein cyberspace provides equal opportunities to all for economic growth and human development. As the user of cyberspace grows increasingly diverse and the range of online interaction expands, there is expansion in the cyber-crimes i.e. breach of online contracts, perpetration of online torts etc. Due to these consequences there was need to adopt a strict law by the cyber space authority to regulate criminal activities relating to cyber and to provide better administration of justice to the victim of cybercrime. In the modern cyber, technology world it is very much necessary to regulate cybercrimes and most importantly cyber law should be made stricter in the case of cyber terrorism and hackers.

IT Act. - E-commerce in recent times has been growing rapidly across the world. It is a type of business model, or segment of a larger business model, that enables a firm or individual to conduct business over an electronic network, typically the internet. Electronic commerce operates in all four of the major market segments: business-to-business, business to consumer, consumer to consumer and consumer to business.

In India, there are three type of e-commerce business model are in vogue

(i) Inventory base model of e-commerce

(ii) Marketplace base model of e-commerce

(iii) Hybrid model of inventory based and market place model.

Indian Information Technology Act and E-commerce: Indian Information Technology (IT) Act gives legal recognition to electronics records and electronic signature. These are the foremost steps to facilitate paper less trading. Under this Act Ministry of Electronics & Information Technology also has Information Technology Rule, 2000 for Reasonable security practices and procedures and sensitive personal data or information. Under section 72A of IT Amendment Act, 2008, punishment for disclosure of information in breach of a lawful contract is laid down.

FDI guidelines for e-commerce by DIPP: DIPP has issued guidelines for FDI in e-commerce. In India 100%, FDI is permitted in B2B e-commerce; however, No FDI is permit in B2C e-commerce earlier. As per these new guidelines on FDI in e-commerce, 100% FDI under automatic route is permit in marketplace model of e-commerce, while FDI is not permit in inventory-based model of e-commerce.

E-commerce has become an important part of many multilateral negotiations such as Regional Comprehensive Economic Partnership (RCEP), WTO, and BRICS etc. Ministry of Electronics & Information Technology is spearheading such negotiations on e-commerce from Indian side.

Electronic Cash- IT is the debit card system of the German Banking Industry Committee, the association that represents the top German financial interest groups. Usually paired with a Transaction account or Current Account, cards with an **Electronic Cash** logo are only hand out by proper credit institutions

Electronic Payment Systems:- The electronic payment system has grown increasingly over the last decades due to the growing spread of internet-based banking and shopping. As the world advances more with technology development, we can see the rise of electronic payment systems and payment processing devices. As this increase, improve, and provide ever more secure online payment transactions the percentage of check and cash transactions will decrease.

Electronic payment methods- One of the most popular payment forms online are credit and debit cards. Besides them, there are also alternative payment methods, such as bank transfers, electronic wallets, smart cards or bit coin wallet (bit coin is the most popular crypto currency).

E-payment methods could classify into two areas, credit payment systems and cash payment systems.

Credit Payment System-

Credit Card — A form of the e-payment system which requires the use of the card issued by a financial institute to the cardholder for making payments online or through an electronic device, without the use of cash.

E-wallet — A form of prepaid account that stores user's financial data, like debit and credit card information to make an online transaction easier.

Smart card — a plastic card with a microprocessor that can be loaded with funds to make transactions; also known as a chip card.

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

- **E-check** — A digital version of an old paper check. It's an electronic transfer of money from a bank account, usually checking account, without the use of the paper check.
- **E-cash** is a form of an electronic payment system, where a certain amount of money is stored on a client's device and made accessible for online transactions.
- **Stored-value card** — A card with a certain amount of money that can be used to perform the transaction in the issuer store. A typical example of stored-value cards are gift cards.

RTGS - The acronym 'RTGS' stands for Real Time Gross Settlement, which can be defined as the continuous (real-time) settlement of funds transfers individually on an order-by-order basis (without netting). 'Real Time' means the processing of instructions at the time they are received rather than at some later time; 'Gross Settlement' means the settlement of funds transfer instructions occurs individually (on an instruction-by-instruction basis). Considering that the funds settlement takes place in the books of the Reserve Bank of India, the payments are final and irrevocable.

NEFT- National Electronic Funds Transfer (NEFT) is a nation-wide payment system facilitating one-to-one funds transfer. Under this Scheme, individuals can electronically transfer funds from any bank branch to any individual having an account with any other bank branch in the country participating in the Scheme.

RTGS is different from National Electronics Funds Transfer System (NEFT) - NEFT is an electronic fund transfer system that operates on a Deferred Net Settlement (DNS) basis, which settles transactions in batches. In DNS, the settlement takes place with all transactions received until the particular cut-off time. These transactions are netted (payable and receivables) in NEFT whereas in RTGS the transactions are settled individually. For example, currently, NEFT operates in hourly batches. [There are twelve settlements from 8 am to 7 pm on weekdays and six settlements from 8 am to 1 pm on Saturdays.] Any transaction initiated after a designated settlement time would have to wait until the next designated settlement time Contrary to this, in the RTGS transactions are processed continuously throughout the RTGS business hours.

Internet Banking- **Online banking**, also known as **internet banking**, **e-banking** or **virtual banking**, is an electronic payment system that enables customers of a bank or other financial institution to conduct a range of financial transactions through the financial institution's website. The online banking system will typically connect to or be part of the core banking system operated by a bank and is in contrast to branch banking , which was the traditional way customers accessed banking services.

Digital Certificates & Signatures- A digital signature is an electronic, encrypted, stamp of authentication on digital information such as email messages, macros, or electronic documents. A signature confirms that the information originated from the signer and has not altered

Signing certificate To create a digital signature, you need a signing certificate, which proves identity. When you send a digitally signed macro or document, you also send your certificate and public key. Certificates issued by a certification authority, and like a driver's license, can revoke. A certificate is usually valid for a year, after which, the signer must renew, or get a new, signing certificate to establish identity.

Certificate authority (CA) A certificate authority is an entity similar to a notary public. It issues digital certificates, signs certificates to verify their validity and tracks, which certificates have revoked or have expired.

Digital signature assurances

The following terms and definitions show what assurances digital signatures provide.

Authenticity-The signer is confirmed as the signer

Integrity The content has not been changed or tampered with since it was digitally signed

Non-repudiation-Proves to all parties the origin of the signed content. Repudiation refers to the act of a signer denying any association with the signed content

Notarization-Signatures in Microsoft Word, Microsoft Excel, or Microsoft PowerPoint files, which are time stamped by a secure time-stamp server, under certain circumstances, have the validity of a notarization.

To make these assurances, the content creator must digitally sign the content by using a signature that satisfies the following criteria:

1. The digital signature is valid.
2. The certificate associated with the digital signature is current (not expired).
3. The signing person or organization, known as the publisher, is trusted.

Infrastructure and Security of Electronic Payment

Secure Socket Layer (SSL) - Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols which provide secure communications on the Internet for such things as web browsing, e-mail, Internet faxing, instant messaging and other data transfers. The TLS protocol(s) allow applications to communicate across a network in a way designed to prevent eavesdropping, tampering, and message forgery. TLS provides endpoint authentication and communications privacy over the Internet using cryptography. Typically, only the server is authenticated (i.e., its identity is ensured) while the client remains unauthenticated; this means that the end user (whether an individual or an application, such as a Web browser) can be sure with whom they are communicating. The next level of security—in which both ends of the "conversation" are sure with whom they are communicating—is known as mutual authentication. Mutual authentication requires public key infrastructure (PKI) deployment to clients.

Secure Electronic Transactions (SET) - Secure Electronic Transaction (SET) is a standard protocol for securing credit card transactions over insecure networks, specifically, the Internet. SET is not itself a payment system, but rather a set of security protocols and formats that enables users to employ the existing credit card payment infrastructure on an open network in a secure fashion. SET specification lists the following business requirements for secure payment processing with credit cards over the Internet and other networks:

1. Provide confidentiality of payment and ordering information
2. Ensure the integrity of all transmitted data
3. Provide authentication that a cardholder is a legitimate user of credit card account
4. Provide authentication that a merchant can accept credit card transactions through its relationship with a financial institution
5. Ensure the use of the best security practices and system design techniques to protect all legitimate parties in an electronic commerce transaction
6. Facilitate and encourage interoperability among software and network providers

3D Secure Protocol- The 3-D Secure™ protocol was developed by Visa to improve the security of online payments. The protocol is offered with the service name Verified by Visa. MasterCard has also adapted a similar protocol called MasterCard Secure Code. Both allow authentication of cardholders by their issuers at participating merchants. The objective is to benefit all participants by providing issuers the ability to fully authenticate cardholders using a password during online purchases, cutting down the chances of credit card fraud and improving card transaction efficiency. 3-D Secure ties the financial authorization process with an online authentication. This authentication is based on a three-domain model (hence the 3-D in the name).

The three domains are:

- Acquirer domain (the merchant and the bank to which money is being paid)
- Issuer domain (the bank which issued the card being used)

- Interoperability domain (the infrastructure provided by the card scheme, credit, debit, prepaid or other type of finance card, to support the 3-D Secure protocol)

Interoperability domain includes the internet, MPI, ACS and other software providers

The protocol uses XML messages sent over SSL connections with client authentication (this ensures the authenticity of peers, the server and the client, using digital certificates). When you start a transaction using 3-D Secure, it initiates a redirection to the website of the card-issuing bank to authorize the transaction. This provides extra protection because correctly entering the security code during a purchase confirms that you are the authorized cardholder. If an incorrect security code is entering, the purchase will not complete. Even if someone knows your credit or debit card number, the purchase cannot be complete without your security code. The process works in a similar way to a PIN number for your card. A significant factor in adopting 3-D Secure is the reduction in disputed transactions and the handling and losses that come with those. Authenticated payment is expecting to eradicate a substantial proportion of fraud, charge-backs and customer complaints. Much harder to predict is the effect 3-D Secure is having on consumer confidence. Greater confidence should mean increased sales, so any steps your business takes to protect data will have a positive impact on your business. 3-D Secure is compatible with most online payment solutions although some high-risk accounts may require the addition of a 'message passing interface' (MPI). Benefits of integrating 3-D Secure:

- Minimal impact on merchant's interaction with consumer
- Customer confidence in your site's security
- Less risk of fraudulent transactions
- Fewer disputed transactions

RGPVNOTES.IN

We hope you find these notes useful.

You can get previous year question papers at https://qp.rgpvnotes.in .

If you have any queries or you want to submit your study notes please write us at rgpvnotes.in@gmail.com

LIKE & FOLLOW US ON FACEBOOK
facebook.com/rgpvnotes.in