INTERNET AND E-COMMERCE

Objectives of E-Commerce

Ecommerce business drives profitable growth with reduction is cost-to-customer, developing customer-reach, and providing a unique customer experience. It has become more than essential for B2B as well as other businesses to make the right use of ecommerce. Now, ecommerce is evolving or better say evolved into digital commerce that implies to the entire business journey from buying to delivery with an online experience. Below are the few objectives of ecommerce:

1. Reduce management costs

Businesses aim at reducing the costs incurred for the betterment of their revenue. Automating the ecommerce business can help in reducing the management cost significantly. Moreover, the right use of digital marketing can help in reducing the cost spent on driving customers to such an extent that businesses can bring customers for free of cost.

2. Developing business relations

With ecommerce as the primary use, business development can be easily achieved. The direct communication between a company and the customer, the business relationship can be boosted. Eventually, the ecommerce market shall be expanded.

3. Providing a unique customer experience

Uncountable ecommerce businesses are functioning out there in the market. When a customer searches for a certain product (for instance, shampoo), they will probably click on the first three links that are shown on the Google Search Engine Results Page. All the rest links are either avoided, never seen, or are visited by a few. This itself shows the competition in the ecommerce market. One of the best ways to stand out from the crowd is by providing a unique customer experience. This includes giving a personalized experience to each customer or visitor of your online store, website, or mobile app. Some other pointers to consider are round the clock customer service, immediate responses to the queries rose, engaging with the customers, and so on.

4. Increasing the number of loyal customers

Customers are the core of all business strategies. Therefore, ensuring the great customer experience is of prime importance for the growth of the business. You need to meet your customers where they spend their time. More than 60% of consumers look for purchasing goods

and services online. If you meet your customers where they are already active, the chances of them, interacting with your business increases two folds. You can increase the number of loyal customers by giving the best experience to your already existing customers as well as bring in newer customers.

5. Boosting the efficiency of services

With the continually evolving technology, you need to enhance the efficiency of your services. By choosing an online ecommerce platform to create an online store, you can efficiently reduce the cost of managing and selling online. You have various opportunities to boost the efficiency of your service that eventually enhances the revenue earned. By reducing the delivery time, you can witness happy customers getting back to your business two times faster. Another way is to provide your customers with automated services such as status update, invoice creating, chat support, etc. When you update your efficiency of delivering products or services to your customers, you are creating a strong online presence that helps you sell more.

6. Developing relevant target

Developing relevant traffic for an ecommerce business is a common objective. Whether an ecommerce website or an online store, building traffic is one of the most important objectives. However, you should know that not all traffic is useful for your business. If you are successfully creating traffic for your ecommerce site or store, but most of the people in the traffic do not require the products or services you provide, the traffic is not causing any good to your business. For instance, your marketing strategies were attractive enough for teenagers; your business would not be receiving any boost in sales. Therefore, along with boosting your traffic, you need to analyze your traffic. Here comes the need for collecting customer data. Collecting customer data include demographics such as age, location, and gender, customer interests, browsing history, browser history, and so on. By saving these data, you can aim in targeting the relevant market.

7. Making responsive ecommerce website

With the increasing use of smartphones for shopping online, it has become more than mandatory for ecommerce businesses to go mobile. Apart from creating a native mobile app, like the one offered from Builderfly, you need to create a responsive ecommerce website. It is one of the major objectives of all leading ecommerce businesses. By responsive, it means to create a website that can be viewed from any devices of varying screen size, equally. Studies say that

Google may next rank a website based on its mobile website. It means that any website that has a responsive design would be ranked on top of the website that does not have one. Making your ecommerce website responsive can help you optimize it. A mobile-friendly website earns more traffic than the rest.

8. Increasing sales

The objective of increasing sales will always remain continuous and constant for an ecommerce business. In order to thrive in the ecommerce industry, you need to boost your sales, constantly. All other objectives are zeroed down to make this objective happen. However, you also need to look into your past store analytics and figure out the marketing tactics that have worked well for you to increase sales. Although these objectives could help you in gaining sales, nothing can beat the tried and tested marketing tactics for your business. For instance, the products that are sold the most, ideally the best seller can be used for remarketing and grab more attention. Any marketing strategy you used earlier including the email targeting and traffic boosting tactics must be revisited and worked upon to increase sales. Based on the above-mentioned objectives and the marketing tactics that actually worked for you, you need to design your marketing plan. Only you can decide what is perfect for your business and what is not. Every business is unique, and so is yours!

Electronic payment System

E-commerce sites use electronic payment, where electronic payment refers to paperless monetary transactions. Electronic payment has revolutionized the business processing by reducing the paperwork, transaction costs, and labor cost. Being user friendly and less time-consuming than manual processing, it helps business organization to expand its market reach/expansion. Listed below are some of the modes of electronic payments −

- Credit Card
- Debit Card
- Smart Card
- E-Money
- Electronic Fund Transfer (EFT)

Credit Card

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

- **The card holder** − Customer
- **The merchant** − seller of product who can accept credit card payments.
- **The card issuer bank** − card holder's bank
- **The acquirer bank** − the merchant's bank
- **The card brand** − for example , visa or Mastercard.

Credit Card Payment Proces

Step	Description
Step 1	Bank issues and activates a credit card to the customer on his/her request.
Step 2	The customer presents the credit card information to the merchant site or to the merchant from whom he/she wants to purchase a product/service.
Step 3	Merchant validates the customer's identity by asking for approval from the card brand company.
Step 4	Card brand company authenticates the credit card and pays the transaction by credit. Merchant keeps the sales slip.

Step 5	Merchant submits the sales slip to acquirer banks and gets the service charges paid to him/her.
Step 6	Acquirer bank requests the card brand company to clear the credit amount and gets the payment.
Step 6	Now the card brand company asks to clear the amount from the issuer bank and the amount gets transferred to the card brand company.

Debit Card

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

Debit cards free the customer to carry cash and cheques. Even merchants accept a debit card readily. Having a restriction on the amount that can be withdrawn in a day using a debit card helps the customer to keep a check on his/her spending.

Smart Card

Smart card is again similar to a credit card or a debit card in appearance, but it has a small microprocessor chip embedded in it. It has the capacity to store a customer’s work-related and/or personal information. Smart cards are also used to store money and the amount gets deducted after every transaction.

Smart cards can only be accessed using a PIN that every customer is assigned with. Smart cards are secure, as they store information in encrypted format and are less expensive/provides faster processing. Mondex and Visa Cash cards are examples of smart cards.

Smart cards.

A smart card, chip card, or integrated circuit card (ICC) is any pocket-sized card with embedded integrated circuits. Smart cards are made of plastic, generally polyvinyl chloride, but sometimes polyethylene terephthalate based polyesters, acrylonitrile butadiene styrene or polycarbonate.

Smart cards can provide identification, authentication, data storage and application processing. Smart cards may provide strong security authentication for single sign-on (SSO) within large organizations

Types of smart cards:

Contact smart cards

Contact smart cards have a contact area of approximately 1 square centimeter (0.16 sq in), comprising several gold-plated contact pads. These pads provide electrical connectivity when inserted into a reader,[8] which is used as a communications medium between the smart card and a host (e.g., a computer, a point of sale terminal) or a mobile telephone. Cards do not contain batteries; power is supplied by the card reader

Contactless smart cards

A second card type is the contactless smart card, in which the card communicates with and is powered by the reader through RF induction technology. These cards require only proximity to an antenna to communicate. Like smart cards with contacts, contactless cards do not have an internal power source. Instead, they use an inductor 'to capture some of the incident radio-frequency interrogation signal, rectify it, and use it to power the card's electronics

Example of widely used contactless smart cards are London's Oyster card, Hong Kong's Octopus card, Tokyo's Suica and Pasmo cards used for public transportation

Smart Cards and Electronic Commerce:

Smart cards are turning out to be a fundamental piece of the transformation of retailing into electronic commerce. The impressive growth of the Internet is making electronic shopping at least a real possibility, if not a habit, among computer users. However, the business model used in current electronic commerce applications still cannot enjoy the full potential of the electronic medium. Moreover, concerns about the reliability of an invisible counterpart and about the safety of the Internet for credit card information increase the wariness and thereby limit the use of the electronic shopping on the part of customers.

Of the estimated 360 billion payments that took place in the United States in 1995, approximately 300 billion could not have taken place using the existing electronic media. Such transactions involved micro-payments p; i.e. payments for less than $10 p; which are virtually outside of the electronic arena for lack of a payment method compatible with such low amounts. Credit cards or checks are simply too expensive to use for micro-payments, and the e-cash currently being experimented on the World Wide Web does not seem to have the characteristics to appeal to shoppers. For this reason, smart cards could be a fundamental building block of widespread use of electronic commerce, since they are an instrument to pay at a low cost for transactions involving small amounts of money.

Another big advantage of smart cards for electronic commerce is their use for the customization of services. It is already possible to purchase tailored services on the World Wide Web p; MyYahoo and FireFly are well known examples. However, in order for the service supplier to deliver the customized service, the user has to provide each supplier with her profile p; a boring and time consuming activity. A smart card can contain a non-encrypted profile of the bearer, so that the user can get customized services even without previous contacts with the supplier.

Finally, smart cards are a key technology enabler for financial institutions. The processing power, the portability and the interactive properties of smart cards will constitute the basis for a revolution in the relationship between consumers and banks. PC-based home banking and phone banking will give way to card banking: a phone equipped with a smart card reader will be all that is needed for any kind of transaction.

Credit Cards and Smart Cards have become the most common forms of payment for e-commerce transactions. In North America almost 90% of online B2C transactions were made with this payment type. Now a days, to decrease the risk of fraud, more security steps are being taken by the government and banks to increase the use of plastic money, such as the use of the card verification number (CVN) which detects fraud by comparing the verification number printed on the signature strip on the back of the card with the information on file with the cardholder's issuing bank.

A Smart card is similar to a credit card a popular smart card initiative is the VISA Smart card. Using the VISA Smart card you can transfer electronic cash to your card from your bank account, and you can then use your card at various retailers and on the internet.

Online payment options:

There are more online payment options than ever before and as an online entrepreneur, you want to offer as many as you can on your site.

A study by CyberSource Corp. found that websites providing four or more payment methods other than credit cards had a sales conversion rate 12 percent higher than those offering just one online payment option in addition to credit cards.

In other words, the more online payment options you offer, the more online payment processing you'll do on your site and the more money you'll make.

Here are the online payment options you could offer on your site:

1) Credit card processing

If you were only going to offer one online payment option to prospective buyers, this would be the one to choose. Credit cards are still the most popular way to pay for goods and services online.

To set up credit card processing on your website, (MasterCard, Visa, American Express, Discover), you need to get an Internet merchant account.

You can get an Internet merchant account through your local banks. Notice I say banks; to get credit card processing of all the major credit cards on your website you may need to get Internet merchant accounts with two separate banks as many banks only deal with some of the credit cards involved.

You can also get an Internet merchant account through a third party merchant account provider, such as Beanstream, Moneris, PSiGate or InternetSecure.

The advantages of getting an Internet merchant account through a third party merchant account provider are that most don't require any security deposits (unlike banks), are quickly set up, and often can be bundled with ecommerce service packages that include the Internet gateway you need for online credit card processing (Web point-of-sale) and a shopping cart.

The disadvantage is higher fees. Discount fees in particular tend to be higher than if you had set up your Internet merchant accounts through the banks.

Wherever you get your Internet merchant account, you will have to also purchase an Internet

gateway service. The gateway verifies information, transfers requests and authorizes credit cards in real time. All four of the companies I've mentioned above offer these credit card processing services as well, but there are many others that do too – including PayPal.

2) PayPal

PayPal is now also an all-in-one online payment solution. Their Website Payments Standard program lets you accept Visa, MasterCard, Discover, and American Express credit card payments as well as bank transfers and offer PayPal as well – with no monthly fees, setup or cancellation fees. PayPal charges you a fee of 1.9 to 2.9 percent of transaction plus 30 cents per order, depending on your company's sales volume.

PayPal also offers an upgraded version of Website Payments Standard called Website Payments Pro, where customers check out right on your site rather than on PayPal's (currently available only in the U.S.).

They also offer a PayFlow Gateway and PayPal Express Checkout for businesses that already have Internet merchant accounts.

E-Money

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.

Electronic Fund Transfer

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

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

Electronic Funds Transfer (EFT) is a system of transferring money from one bank account directly to another without any paper money changing hands. One of the most widely-used EFT programs is direct deposit, through which payroll is deposited straight into an employee's bank account. However, EFT refers to any transfer of funds initiated through an electronic terminal, including credit card, ATM, Fedwire and point-of-sale (POS) transactions. It is used for both credit transfers, such as payroll payments, and for debit transfers, such as mortgage payments.

How EFT works

Transactions are processed by the bank through the Automated Clearing House (ACH) network, the secure transfer system that connects all U.S. financial institutions. For payments, funds are transferred electronically from one bank account to the billing company's bank, usually less than a day after the scheduled payment date.

The ACH Network operates as a batch processing system. Financial institutions accumulate ACH transactions throughout the day, which are handled via batch processing later on. According to NACHA, which creates payment and financial messaging rules and standards, the ACH Network handles 24 billion EFTs each year, accounting for more than $41 trillion transferred. The ACH Network is one of the largest and most reliable payment systems in the world, according to the association.

To complete an EFT, the receiving party must provide the following information:

- The name of the bank receiving funds
- The type of account receiving funds (e.g., checking or savings)
- The bank's ABA routing number
- The recipient's account number

The growing popularity of EFT for online bill payment is paving the way for paperless transactions where checks, stamps, envelopes and paper bills are obsolete. The benefits of EFT include reduced administrative costs, increased efficiency, simplified bookkeeping, and greater security. However, the number of companies who send and receive bills through the Internet is still relatively small.

Types of EFTs

The most common types of EFTs include:

- **Direct deposit**: Enables businesses to pay employees. During the employee onboarding process, new employees typically specify the financial institution to receive the direct deposit payments.
- **Wire transfers**: Used for non-regular payments, such as the down payment on a house.
- **Automated Teller Machines (ATMs)**: Allows cash withdrawals and deposits, fund transfers and checking of account balances at multiple locations, such as branch locations, retail stores, shopping malls and airports.
- **Debit cards:** Allows users to pay for transactions and have those funds deducted from the account linked to the card.
- **Pay-by-phone systems**: Allows users to pay bills or transfer money over the phone.
- **Online banking**: Available via personal computer, tablet or smartphone. Using online banking, users can access accounts to make payments, transfer funds and check balances.

Regulations

The U.S. Government monitors EFT compliance through Regulation E of the Federal Reserve Board, which implements the Electronic Funds Transfer Act (EFTA). The EFTA was passed by the U.S. Congress in 1978 to protect consumers engaging in EFTs. Regulation E governs financial transactions with electronic payment services, specifically with regard to disclosure of information, consumer liability, error resolution, record retention and receipts at electronic terminals.

Consumers can sue for damages in court if financial institutions break laws established by the EFTA. For example, if ATM card is reported as stolen and the financial institution failed to prevent a transfer, the card's owner is entitled to the money lost.

Users can't be forced to use EFTs to make or to receive a payment, except for overdraft checking fees. When a checking account is overdrawn, the financial institution can use EFTs to deduct overdraft fees from the consumer's account. With a few exceptions, employers can require that employees are paid by EFT. Employees can choose the financial institution to receive the funds.

If an ATM or debit card is lost or stolen and reported to the financial institution before any transactions take place, the card's owner is not held responsible for any subsequent transactions. Depending on when the card is reported stolen or lost, the card's owner could be liable for between $50 and an unlimited amount of charges.

EFTs usually settle on the next business day, but can take longer during bank holidays. International transactions (IATs) and high-value transactions above $25,000 are not eligible for same-day processing.

RISK IN ELECTRONIC PAYMENT SYSTEM

The Risk of Fraud

Electronic payment systems are not immune to the risk of fraud. The system uses a particularly vulnerable protocol to establish the identity of the person authorizing a payment. Passwords and security questions aren't foolproof in determining the identity of a person. So long as the password and the answers to the security questions are correct, the system doesn't care who's on the other side. If someone gains access to your password or the answers to your security question, they will have gained access to your money and can steal it from you.

The Risk of Tax Evasion

The law requires that businesses declare their financial transactions and provide paper records of them so that tax compliance can be verified. The problem with electronic systems is that they don't fit very cleanly into this paradigm and so they can make the process of tax collection very frustrating for the Internal Revenue Service. It is at the business's discretion to disclose payments received or made via electronic payment systems in a fiscal period, and the IRS has no way of knowing if it's telling the truth or not. That makes it pretty easy to evade taxation.

The Risk of Payment Conflicts

One of the idiosyncrasies of electronic payment systems is that the payments aren't handled by humans but by an automated electronic system. The system is prone to errors, particularly when it has to handle large amounts of payments on a frequent basis with many recipients involved. It's important to constantly check your pay slip after every pay period ends in order to ensure everything makes sense. Failure to do this may result in payment conflicts caused by technical glitches and anomalies.

The Risk of Impulse Buying

Impulse buying is already a risk that you face when you use non-electronic payment systems. It is magnified, however, when you're able to buy things online at the click of a mouse. Impulse buying can become habitual and makes sticking to a budget almost impossible.

Electronic payment System

E-commerce sites use electronic payment, where electronic payment refers to paperless monetary transactions. Electronic payment has revolutionized the business processing by reducing the paperwork, transaction costs, and labor cost. Being user friendly and less time-consuming than manual processing, it helps business organization to expand its market reach/expansion. Listed below are some of the modes of electronic payments −

- Credit Card
- Debit Card
- Smart Card
- E-Money
- Electronic Fund Transfer (EFT)

Credit Card

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

- **The card holder** − Customer
- **The merchant** − seller of product who can accept credit card payments.
- **The card issuer bank** − card holder's bank
- **The acquirer bank** − the merchant's bank
- **The card brand** − for example , visa or Mastercard.

Credit Card Payment Proces

Step	Description
Step 1	Bank issues and activates a credit card to the customer on his/her request.
Step 2	The customer presents the credit card information to the merchant site or to the merchant from whom he/she wants to purchase a product/service.
Step 3	Merchant validates the customer's identity by asking for approval from the card brand company.
Step 4	Card brand company authenticates the credit card and pays the transaction by credit. Merchant keeps the sales slip.
Step 5	Merchant submits the sales slip to acquirer banks and gets the service charges paid to him/her.
Step 6	Acquirer bank requests the card brand company to clear the credit amount and gets the payment.
Step 6	Now the card brand company asks to clear the amount from the issuer bank and the amount gets transferred to the card brand company.

Debit Card

Debit card, like credit card, is a small plastic card with a unique number mapped with the bank account number. It is required to have a bank account before getting a debit card from the bank. The major difference between a debit card and a credit card is that in case of payment through debit card, the amount gets deducted from the card's bank account immediately and

there should be sufficient balance in the bank account for the transaction to get completed; whereas in case of a credit card transaction, there is no such compulsion.

Debit cards free the customer to carry cash and cheques. Even merchants accept a debit card readily. Having a restriction on the amount that can be withdrawn in a day using a debit card helps the customer to keep a check on his/her spending.

Smart Card

Smart card is again similar to a credit card or a debit card in appearance, but it has a small microprocessor chip embedded in it. It has the capacity to store a customer's work-related and/or personal information. Smart cards are also used to store money and the amount gets deducted after every transaction.

Smart cards can only be accessed using a PIN that every customer is assigned with. Smart cards are secure, as they store information in encrypted format and are less expensive/provides faster processing. Mondex and Visa Cash cards are examples of smart cards.

Smart cards.

A smart card, chip card, or integrated circuit card (ICC) is any pocket-sized card with embedded integrated circuits. Smart cards are made of plastic, generally polyvinyl chloride, but sometimes polyethylene terephthalate based polyesters, acrylonitrile butadiene styrene or polycarbonate.

Smart cards can provide identification, authentication, data storage and application processing. Smart cards may provide strong security authentication for single sign-on (SSO) within large organizations

Types of smart cards:

Contact smart cards

Contact smart cards have a contact area of approximately 1 square centimeter (0.16 sq in), comprising several gold-plated contact pads. These pads provide electrical connectivity when inserted into a reader,[8] which is used as a communications medium between the smart card and a host (e.g., a computer, a point of sale terminal) or a mobile telephone. Cards do not contain batteries; power is supplied by the card reader

Contactless smart cards

A second card type is the contactless smart card, in which the card communicates with and is powered by the reader through RF induction technology. These cards require only proximity to

an antenna to communicate. Like smart cards with contacts, contactless cards do not have an internal power source. Instead, they use an inductor 'to capture some of the incident radio-frequency interrogation signal, rectify it, and use it to power the card's electronics

Example of widely used contactless smart cards are London's Oyster card, Hong Kong's Octopus card, Tokyo's Suica and Pasmo cards used for public transportation

Smart Cards and Electronic Commerce:

Smart cards are turning out to be a fundamental piece of the transformation of retailing into electronic commerce. The impressive growth of the Internet is making electronic shopping at least a real possibility, if not a habit, among computer users. However, the business model used in current electronic commerce applications still cannot enjoy the full potential of the electronic medium. Moreover, concerns about the reliability of an invisible counterpart and about the safety of the Internet for credit card information increase the wariness and thereby limit the use of the electronic shopping on the part of customers.

Of the estimated 360 billion payments that took place in the United States in 1995, approximately 300 billion could not have taken place using the existing electronic media. Such transactions involved micro-payments p; i.e. payments for less than $10 p; which are virtually outside of the electronic arena for lack of a payment method compatible with such low amounts. Credit cards or checks are simply too expensive to use for micro-payments, and the e-cash currently being experimented on the World Wide Web does not seem to have the characteristics to appeal to shoppers. For this reason, smart cards could be a fundamental building block of widespread use of electronic commerce, since they are an instrument to pay at a low cost for transactions involving small amounts of money.

Another big advantage of smart cards for electronic commerce is their use for the customization of services. It is already possible to purchase tailored services on the World Wide Web p; MyYahoo and FireFly are well known examples. However, in order for the service supplier to deliver the customized service, the user has to provide each supplier with her profile p; a boring and time consuming activity. A smart card can contain a non-encrypted profile of the bearer, so that the user can get customized services even without previous contacts with the supplier.

Finally, smart cards are a key technology enabler for financial institutions. The processing power, the portability and the interactive properties of smart cards will constitute the basis for a revolution in the relationship between consumers and banks. PC-based home banking and phone banking will give way to card banking: a phone equipped with a smart card reader will be all that is needed for any kind of transaction.

Credit Cards and Smart Cards have become the most common forms of payment for e-commerce transactions. In North America almost 90% of online B2C transactions were made with this payment type. Now a days, to decrease the risk of fraud, more security steps are being taken by the government and banks to increase the use of plastic money, such as the use of the card verification number (CVN) which detects fraud by comparing the verification number printed on the signature strip on the back of the card with the information on file with the cardholder's issuing bank.

A Smart card is similar to a credit card a popular smart card initiative is the VISA Smart card. Using the VISA Smart card you can transfer electronic cash to your card from your bank account, and you can then use your card at various retailers and on the internet.

Online payment options:

There are more online payment options than ever before and as an online entrepreneur, you want to offer as many as you can on your site.

A study by CyberSource Corp. found that websites providing four or more payment methods other than credit cards had a sales conversion rate 12 percent higher than those offering just one online payment option in addition to credit cards.

In other words, the more online payment options you offer, the more online payment processing you'll do on your site and the more money you'll make.

Here are the online payment options you could offer on your site:

1) Credit card processing

If you were only going to offer one online payment option to prospective buyers, this would be the one to choose. Credit cards are still the most popular way to pay for goods and services online.

To set up credit card processing on your website, (MasterCard, Visa, American Express, Discover), you need to get an Internet merchant account.

You can get an Internet merchant account through your local banks. Notice I say banks; to get credit card processing of all the major credit cards on your website you may need to get Internet merchant accounts with two separate banks as many banks only deal with some of the credit cards involved.

You can also get an Internet merchant account through a third party merchant account provider, such as Beanstream, Moneris, PSiGate or InternetSecure.

The advantages of getting an Internet merchant account through a third party merchant account provider are that most don't require any security deposits (unlike banks), are quickly set up, and

often can be bundled with ecommerce service packages that include the Internet gateway you need for online credit card processing (Web point-of-sale) and a shopping cart.

The disadvantage is higher fees. Discount fees in particular tend to be higher than if you had set up your Internet merchant accounts through the banks.

Wherever you get your Internet merchant account, you will have to also purchase an Internet gateway service. The gateway verifies information, transfers requests and authorizes credit cards in real time. All four of the companies I've mentioned above offer these credit card processing services as well, but there are many others that do too – including PayPal.

2) PayPal

PayPal is now also an all-in-one online payment solution. Their Website Payments Standard program lets you accept Visa, MasterCard, Discover, and American Express credit card payments as well as bank transfers and offer PayPal as well – with no monthly fees, setup or cancellation fees. PayPal charges you a fee of 1.9 to 2.9 percent of transaction plus 30 cents per order, depending on your company's sales volume.

PayPal also offers an upgraded version of Website Payments Standard called Website Payments Pro, where customers check out right on your site rather than on PayPal's (currently available only in the U.S.).

They also offer a PayFlow Gateway and PayPal Express Checkout for businesses that already have Internet merchant accounts.

E-Money

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.

Electronic Fund Transfer

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

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

Electronic Funds Transfer (EFT) is a system of transferring money from one bank account directly to another without any paper money changing hands. One of the most widely-used EFT programs is direct deposit, through which payroll is deposited straight into an employee's bank account. However, EFT refers to any transfer of funds initiated through an electronic terminal, including credit card, ATM, Fedwire and point-of-sale (POS) transactions. It is used for both credit transfers, such as payroll payments, and for debit transfers, such as mortgage payments.

How EFT works

Transactions are processed by the bank through the Automated Clearing House (ACH) network, the secure transfer system that connects all U.S. financial institutions. For payments, funds are transferred electronically from one bank account to the billing company's bank, usually less than a day after the scheduled payment date.

The ACH Network operates as a batch processing system. Financial institutions accumulate ACH transactions throughout the day, which are handled via batch processing later on.

According to NACHA, which creates payment and financial messaging rules and standards, the ACH Network handles 24 billion EFTs each year, accounting for more than $41 trillion transferred. The ACH Network is one of the largest and most reliable payment systems in the world, according to the association.

To complete an EFT, the receiving party must provide the following information:

- The name of the bank receiving funds
- The type of account receiving funds (e.g., checking or savings)
- The bank's ABA routing number
- The recipient's account number

The growing popularity of EFT for online bill payment is paving the way for paperless transactions where checks, stamps, envelopes and paper bills are obsolete. The benefits of EFT include reduced administrative costs, increased efficiency, simplified bookkeeping, and greater security. However, the number of companies who send and receive bills through the Internet is still relatively small.

Types of EFTs

The most common types of EFTs include:

- **Direct deposit**: Enables businesses to pay employees. During the employee onboarding process, new employees typically specify the financial institution to receive the direct deposit payments.
- **Wire transfers**: Used for non-regular payments, such as the down payment on a house.
- **Automated Teller Machines (ATMs)**: Allows cash withdrawals and deposits, fund transfers and checking of account balances at multiple locations, such as branch locations, retail stores, shopping malls and airports.

- **Debit cards:** Allows users to pay for transactions and have those funds deducted from the account linked to the card.
- **Pay-by-phone systems**: Allows users to pay bills or transfer money over the phone.
- **Online banking**: Available via personal computer, tablet or smartphone. Using online banking, users can access accounts to make payments, transfer funds and check balances.

Regulations

The U.S. Government monitors EFT compliance through Regulation E of the Federal Reserve Board, which implements the Electronic Funds Transfer Act (EFTA). The EFTA was passed by the U.S. Congress in 1978 to protect consumers engaging in EFTs. Regulation E governs financial transactions with electronic payment services, specifically with regard to disclosure of information, consumer liability, error resolution, record retention and receipts at electronic terminals.

Consumers can sue for damages in court if financial institutions break laws established by the EFTA. For example, if ATM card is reported as stolen and the financial institution failed to prevent a transfer, the card's owner is entitled to the money lost.

Users can't be forced to use EFTs to make or to receive a payment, except for overdraft checking fees. When a checking account is overdrawn, the financial institution can use EFTs to deduct overdraft fees from the consumer's account. With a few exceptions, employers can require that employees are paid by EFT. Employees can choose the financial institution to receive the funds.

If an ATM or debit card is lost or stolen and reported to the financial institution before any transactions take place, the card's owner is not held responsible for any subsequent transactions. Depending on when the card is reported stolen or lost, the card's owner could be liable for between $50 and an unlimited amount of charges.

EFTs usually settle on the next business day, but can take longer during bank holidays. International transactions (IATs) and high-value transactions above $25,000 are not eligible for same-day processing.

RISK IN ELECTRONIC PAYMENT SYSTEM

The Risk of Fraud

Electronic payment systems are not immune to the risk of fraud. The system uses a particularly vulnerable protocol to establish the identity of the person authorizing a payment. Passwords and security questions aren't foolproof in determining the identity of a person. So long as the password and the answers to the security questions are correct, the system doesn't care who's on the other side. If someone gains access to your password or the answers to your security question, they will have gained access to your money and can steal it from you.

The Risk of Tax Evasion

The law requires that businesses declare their financial transactions and provide paper records of them so that tax compliance can be verified. The problem with electronic systems is that they don't fit very cleanly into this paradigm and so they can make the process of tax collection very frustrating for the Internal Revenue Service. It is at the business's discretion to disclose payments received or made via electronic payment systems in a fiscal period, and the IRS has no way of knowing if it's telling the truth or not. That makes it pretty easy to evade taxation.

The Risk of Payment Conflicts

One of the idiosyncrasies of electronic payment systems is that the payments aren't handled by humans but by an automated electronic system. The system is prone to errors, particularly when it has to handle large amounts of payments on a frequent basis with many recipients involved. It's important to constantly check your pay slip after every pay period ends in order to ensure everything makes sense. Failure to do this may result in payment conflicts caused by technical glitches and anomalies.

The Risk of Impulse Buying

Impulse buying is already a risk that you face when you use non-electronic payment systems. It is magnified, however, when you're able to buy things online at the click of a mouse. Impulse buying can become habitual and makes sticking to a budget almost impossible

Anatomy of E-Commerce applications

•Multimedia Content for E-Commerce Applications

•Multimedia Storage Servers & E-Commerce Applications

i. Client-Server Architecture in Electronic Commerce

ii. Internal Processes of Multimedia Servers

iii. Video Servers & E-Commerce

•Information Delivery/Transport & E-Commerce Applications

•Consumer Access Devices

Multimedia Content for E-Commerce Applications

•Multimedia content can be considered both fuel and traffic for electronic commerce applications.

•The technical definition of multimedia is the use of digital data in more than one format, such as the combination of text, audio, video, images, graphics, numerical data, holograms, and animations in a computer file/document. See in Fig.

•Multimedia is associated with Hardware components in different networks.

•The Accessing of multimedia content depends on the hardware capabilities of the customer.

Multimedia Storage Servers & E-Commerce Applications

•E-Commerce requires robust servers to store and distribute large amounts of digital content to consumers.

•These Multimedia storage servers are large information warehouses capable of handling various content, ranging from books, newspapers, advertisement catalogs, movies, games, & X-ray images.

•These servers, deriving their name because they serve information upon request, must handle large-scale distribution, guarantee security, & complete reliability

i. Client-Server Architecture in Electronic Commerce

•All e-commerce applications follow the client-server model

•Clients are devices plus software that request information from servers or interact known as message passing

•Mainframe computing , which meant for "dump"

•The client server model, allows client to interact with server through request-reply sequence governed by a paradigm known as message passing.

•The server manages application tasks, storage & security & provides scalability-ability to add more clients and client devices(like Personal digital assistants to Pc's. See in fig.

ii. Internal Processes of Multimedia Servers

•The internal processes involved in the storage, retrieval & management of multimedia data objects are integral to e-commerce applications.

•A multimedia server is a hardware & software combination that converts raw data into usable information & then dishes out.

•It captures, processes, manages, & delivers text, images, audio & video.

•It must do to handle thousands of simultaneous users.

•Include high-end symmetric multiprocessors, clustered architecture, and massive parallel systems.

iii. Video Servers & E-Commerce

The electronic commerce applications related to digital video will include

1. Telecommunicating and video conferencing
2. Geographical information systems that require storage & navigation over maps

3. Corporate multimedia servers
4. Postproduction studios
5. shopping kiosks.

•Consumer applications will include video-on-demand.

•The figure which is of video–on demand consist video servers, is an link between the content providers (media) & transport providers (cable operators)

Information Delivery/Transport & E-Commerce Applications

•Transport providers are principally telecommunications, cable, & wireless industries.

Information Transport Providers	Information Delivery Methods
•Telecommunication companies	long-distance telephone lines; local telephone lines
•Cable television companies	Cable TV coaxial, fiber optic & satellite lines
•Computer-based on-line servers	Internet; commercial on-line service providers
•Wireless communications	Cellular & radio networks; paging systems

Consumer Access Devices

Information Consumers	Access Devices
•Computers with audio & video capabilities	Personal/desktop computing Mobile computing
•Telephonic devices	Videophone

•Consumer electronics	Television + set-top box Game systems
•Personal digital assistants (PDAs)	Pen-based computing, voice-driven computing

Firewall and its Types

A firewall is a type of cybersecurity tool used to filter traffic on a network. Firewalls can separate network nodes from external traffic sources, internal traffic sources, or even specific applications. Firewalls can be software, hardware, or cloud-based, with each type of firewall having unique pros and cons.

Firewall Types:

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

Firewall Delivery Methods:

- Software firewalls
- Hardware firewalls
- Cloud firewall

Type 1: Packet-Filtering Firewalls

As the most “basic” and oldest type of firewall architecture, packet-filtering firewalls create a checkpoint at a traffic router or switch. The firewall performs a simple check of the data packets coming through the router—inspecting information such as the destination and origination IP

address, packet type, port number, and other surface-level details without opening the packet to examine its contents. It then drops the packet if the information packet doesn't pass the inspection.

The good thing about these firewalls is that they aren't very resource-intensive. Using fewer resources means they are relatively simple and don't significantly impact system performance. However, they're also relatively easy to bypass compared to firewalls with more robust inspection capabilities.

Type 2: Circuit-Level Gateways

Circuit-level gateways are another simplistic firewall type meant to quickly and easily approve or deny traffic without consuming significant computing resources. Circuit-level gateways work by verifying the transmission control protocol (TCP) handshake. This TCP handshake check is designed to ensure that the session the packet is from is legitimate.

While extremely resource-efficient, these firewalls do not check the packet itself. So, if a packet held malware but had the proper TCP handshake, it would easily pass through. Vulnerabilities like this are why circuit-level gateways are not enough to protect your business by themselves.

Type 3: Stateful Inspection Firewalls

This firewall type combines packet inspection technology and TCP handshake verification to create a more significant level of protection than either of the two architectures could provide alone.

However, these firewalls also put more of a strain on computing resources. This may slow down the transfer of legitimate packets compared to the other solutions.

Type 4: Proxy Firewalls (Application-Level Gateways/Cloud Firewalls)

Proxy firewalls operate at the application layer to filter incoming traffic between your network and the traffic source—hence, the name "application-level gateway." These firewalls are delivered via a cloud-based solution or another proxy device. Rather than letting traffic connect directly, the proxy firewall first establishes a connection to the source of the traffic and inspects the incoming data packet.

This check is similar to the stateful inspection firewall in looking at both the packet and the TCP handshake protocol. However, proxy firewalls may also perform deep-layer packet inspections, checking the actual contents of the information packet to verify that it contains no malware.

Once the check is complete and the packet is approved to connect to the destination, the proxy sends it off. This creates an extra layer of separation between the "client" (the system where the packet originated) and the individual devices on your network—obscuring them to create additional anonymity and protection for your network.

The one drawback to proxy firewalls is that they can create a significant slowdown because of the extra steps in the data packet transfer process.

Type 5: Next-Generation Firewalls

Many of the most recently-released firewall products are touted as "next-generation" architectures. However, there is no consensus on what makes a firewall genuinely next-gen.

Some typical features of next-generation firewall architectures include deep-packet inspection (checking the actual contents of the data packet), TCP handshake checks, and surface-level packet inspection. Next-generation firewalls may consist of other technologies, such as intrusion prevention systems (IPSs), that automatically stop attacks against your network.

The issue is that there is no one definition of a next-generation firewall, so verifying what specific capabilities such firewalls have before investing in one is essential.

Firewall Deployment Architecture 1: Software Firewalls

Software firewalls include any type of firewall that is installed on a local device rather than a separate piece of hardware (or a cloud server). The big benefit of a software firewall is that it's highly useful for creating defense in depth by isolating individual network endpoints from one another.

However, maintaining individual software firewalls on different devices can be difficult and time-consuming. Furthermore, not every device on a network may be compatible with a single software firewall, which may mean having to use several different software firewalls to cover every asset.

Firewall Deployment Architecture 2: Hardware Firewalls

Hardware firewalls use a physical appliance that acts like a traffic router to intercept data packets and traffic requests before they're connected to the network's servers. Physical appliance-based firewalls like this excel at perimeter security by ensuring malicious traffic from outside the network are intercepted before the company's network endpoints are exposed to risk.

However, the major weakness of a hardware-based firewall is that it is often easy for insider attacks to bypass them. Also, the actual capabilities of a hardware firewall may vary depending on the manufacturer—some may have a more limited capacity to handle simultaneous connections than others, for example.

Firewall Deployment Architecture 3: Cloud Firewalls

Whenever you use a cloud solution to deliver a firewall, it can be called a cloud firewall or firewall-as-a-service (FaaS). Many consider cloud firewalls synonymous with proxy firewalls since a cloud server is often used in a firewall setup (though the proxy doesn't necessarily *have* to be on the cloud, it frequently is).

The primary benefit of having cloud-based firewalls is that they are straightforward to scale with your organization. As your needs grow, you can add additional capacity to the cloud server to filter larger traffic loads. Cloud firewalls, like hardware firewalls, excel at perimeter security.

Cyber Crime

Definition of Cybercrime

Any offenses committed against individuals or groups of individuals to harm the reputation or cause physical or mental trauma through electronic means can be defined as Cybercrime. Electronic means can include but are not limited to, the use of modern telecommunication networks such as the Internet (networks including chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS).

There are many privacy concerns surrounding cybercrime when sensitive information is intercepted and leaked to the public, legally or otherwise. Some of that information may include data about military deployments, internal government communications, and even private data about high-value individuals. Cybercrime is not confined to individuals alone. Internationally, both governmental and non-state actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes. Cybercrimes crossing international borders and involving the actions of at least one nation-state is sometimes referred to as cyberwarfare.

In 2018, a study by Center for Strategic and International Studies (CSIS), in partnership with McAfee, a leading cybersecurity firm concludes that close to $600 billion, nearly one percent of global GDP, is lost to cybercrime each year.

Candidates can check out the relevant links given below to prepare for the upcoming exams even better-

Cyber Security	National Cyber Security Policy	Upgrading India's cybersecurity architecture
National Crime	Code of Criminal	Indian Penal Code (IPC) – History,

Records Bureau (NCRB)	Procedure (CrPC)	Structure & Recent Developments

Laws against Cybercrime in India

Ever since the introduction of cyber laws in India, the Information Technology Act (IT Act) 2000 covers different types of crimes under cyber law in India. The following types of cybercrimes are covered under the IT Act 2000.

- **Identity theft** – Identity theft is defined as theft of personnel information of an individual to avail financial services or steal the financial assets themselves.
- **Cyberterrorism** – Cyberterrorism is committed with the purpose of causing grievous harm or extortion of any kind subjected towards a person, groups of individuals, or governments.
- **Cyberbullying** – Cyberbullying is the act of intimidating, harassment, defaming, or any other form of mental degradation through the use of electronic means or modes such as social media.
- **Hacking** – Access of information through fraudulent or unethical means is known as hacking. This is the most common form of cybercrime know to the general public.
- **Defamation** – While every individual has his or her right to speech on internet platforms as well, but if their statements cross a line and harm the reputation of any individual or organization, then they can be charged with the Defamation Law.
- **Trade Secrets** – Internet organization spends a lot of their time and money in developing software, applications, and tools and rely on Cyber Laws to protect their data and trade secrets against theft; doing which is a punishable offense.
- **Freedom of Speech** – When it comes to the internet, there is a very thin line between freedom of speech and being a cyber-offender. As freedom of speech enables individuals to speak their mind, cyber law refrains obscenity and crassness over the web.

- **Harassment and Stalking** – Harassment and stalking are prohibited over internet platforms as well. Cyber laws protect the victims and prosecute the offender against this offense.

Information Technology Act 2000

The Information Technology Act, 2000 also Known as an **IT Act** is an act proposed by the Indian Parliament reported on 17th October 2000. This Information Technology Act is based on the United Nations Model law on Electronic Commerce 1996 (UNCITRAL Model) which was suggested by the General Assembly of United Nations by a resolution dated on 30th January, 1997. It is the most important law in India dealing with Cybercrime and E-Commerce.
The main objective of this act is to carry lawful and trustworthy electronic, digital and online transactions and alleviate or reduce cybercrimes. The IT Act has 13 chapters and 90 sections. The last four sections that starts from 'section 91 – section 94', deals with the revisions to the Indian Penal Code 1860.

The IT Act, 2000 has two schedules:

- **First Schedule –**
  Deals with documents to which the Act shall not apply.
- **Second Schedule –**
  Deals with electronic signature or electronic authentication method.

The offences and the punishments in IT Act 2000 :

The offences and the punishments that falls under the IT Act, 2000 are as follows :-

1. Tampering with the computer source documents.
2. Directions of Controller to a subscriber to extend facilities to decrypt information.
3. Publishing of information which is obscene in electronic form.
4. Penalty for breach of confidentiality and privacy.
5. Hacking for malicious purposes.
6. Penalty for publishing Digital Signature Certificate false in certain particulars.
7. Penalty for misrepresentation.
8. Confiscation.
9. Power to investigate offences.
10. Protected System.

11. Penalties for confiscation not to interfere with other punishments.
12. Act to apply for offence or contravention committed outside India.
13. Publication for fraud purposes.
14. Power of Controller to give directions.

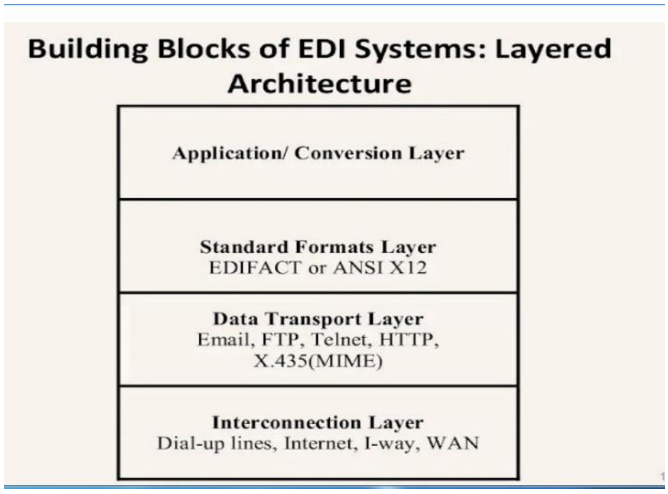
Sections and Punishments under Information Technology Act, 2000 are as follows :

SECTION	PUNISHMENT
Section 43	This section of IT Act, 2000 states that any act of destroying, altering or stealing computer system/network or deleting data with malicious intentions without authorization from owner of the computer is liable for the payment to be made to owner as compensation for damages.
Section 43A	This section of IT Act, 2000 states that any corporate body dealing with sensitive information that fails to implement reasonable security practices causing loss of other person will also liable as convict for compensation to the affected party.
Section 66	Hacking of a Computer System with malicious intentions like fraud will be punished with 3 years imprisonment or the fine of Rs.5,00,000 or both.
Section 66 B, C, D	Fraud or dishonesty using or transmitting information or identity theft is punishable with 3 years imprisonment or Rs. 1,00,000 fine or both.
Section 66 E	This Section is for Violation of privacy by transmitting image of private area is punishable with 3 years imprisonment or 2,00,000 fine or both.
Section 66 F	This Section is on Cyber Terrorism affecting unity, integrity, security, sovereignty of India through digital medium is liable for life imprisonment.
Section 67	This section states publishing obscene information or pornography or transmission of obscene content in public is liable for imprisonment up to 5 years or fine of Rs.

	10,00,000 or both.

EDI Layered Architecture

rif



Application Layer

It consists of the actual business applications that are going to be connected through the EDI systems forthe exchange of electronic information. These applications may use their own electronic record formats and document formats for storing, retrieving, and processing the information within the company systems. For EDI to operate, they need to convert the internal company document format to a format that can be understood by the system used by the trading partner. When the trading partners are small in number, then the converters for various partner formats can be built.

But, as the number of partners with different internal formats increase, the task of building converters for each proprietary format to other format becomes overwhelmingElectronic Data Interchange (EDI) is a computer-to-computer exchange of business documents in a standard electronic format between two or more trading partners. It enables companies to exchange information electronically in a structured format, eliminating the need for manual data entry and reducing the cost and time associated with paper-based transactions.

EDI was first introduced in the 1960s as a way for companies to exchange business documents electronically. Over time, the standardization of EDI formats and protocols has enabled

businesses to integrate their internal systems with those of their trading partners, improving efficiency and reducing errors.

EDI transactions can include purchase orders, invoices, shipping notices, and other business documents. The EDI standard defines the format and content of these documents, ensuring that they are easily interpreted by both the sender and the receiver

Electronic Data Interchange (EDI)

Electronic Data Interchange (EDI) is a computer-to-computer exchange of business documents in a standard electronic format between two or more trading partners. It enables companies to exchange information electronically in a structured format, eliminating the need for manual data entry and reducing the cost and time associated with paper-based transactions.

EDI was first introduced in the 1960s as a way for companies to exchange business documents electronically. Over time, the standardization of EDI formats and protocols has enabled businesses to integrate their internal systems with those of their trading partners, improving efficiency and reducing errors.

EDI transactions can include purchase orders, invoices, shipping notices, and other business documents. The EDI standard defines the format and content of these documents, ensuring that they are easily interpreted by both the sender and the receiver.

EDI has become an important part of many businesses, particularly those in the supply chain and logistics industries. It allows for faster and more accurate processing of transactions, leading to improved customer satisfaction and increased profits.

Imagine writing a letter to your friend while communicating every time, Can not imagine right? Since today humans live in an era where they can very easily communicate through the internet. Now, imagine the same case with businesses, where communication and exchange of very important documents are constantly required, doing this the old way, it will take forever for the messages to reach the other party, but also the documents will pile up as there is a lot of information that is needed to be stored and kept. It is a tedious and cumbersome process indeed, this is where EDI plays its role.

Electronic Data Exchange is the direct exchange of data and important business documents through the Internet and in a very professional manner. Two different companies sitting at the extreme corners of the world can very easily interchange information or documents (like sales orders, shipping notices, invoices, etc) with the help of EDI.

EDI Documents:

The most common documents exchanged via EDI are:

- Invoices
- Purchase Orders
- Financial Information letters
- Transaction Bills
- Shipping requests and notifications
- Acknowledgment and feedback
- Transcripts
- Claims
- Business Correspondence letters

EDI Users:

- Central and state government agencies
- Industry
- Banking
- Retailing
- Manufacturing
- Insurance
- Healthcare
- Automotive
- Electronics
- Grocery
- Transportation

History of EDI

Edward Guilbert is known to be the father of electronic data exchange, introduced EDI back in the 1960s in the supply chains. The US Transportation industry implemented EDI for better communication among different companies. In 1985, the UN created EDIFACT EDI for better reach of Global technology. Approximately 12000 companies started using EDI in the US. The US grocery and automobile industry very swiftly accepted EDI due to the easy process and standard form of data exchange. In today's time, with following EDI's compliance, the big and major companies are using EDI for their communication among businesses.

Examples of EDI include Purchase orders, invoices, shipping statuses, payment information, and so on.

How EDI works?

The data or the information that one company sends the other first gets prepared to be sent, then the information/document is translated into EDI format. The document is then connected and transmitted to the other business, the connection is direct and point to point.

Uses of EDI :

EDI is widely used in various industries for exchanging business documents electronically. Some of the common uses of EDI are:

- **Order Processing:** EDI allows companies to exchange purchase orders and sales orders electronically, eliminating the need for manual data entry and reducing errors.
- **Invoicing:** EDI can be used to exchange invoices electronically, reducing the time and cost associated with paper-based invoicing.
- **Shipping and Receiving:** EDI can be used to exchange shipping notices and receiving documents, enabling companies to track the movement of goods in real-time.
- **Inventory Management:** EDI can be used to exchange inventory information, enabling companies to manage their inventory levels more effectively.
- **Supply Chain Management:** EDI is used extensively in the supply chain management process, enabling companies to exchange information with their suppliers, distributors, and customers.

- **Healthcare:** EDI is used in the healthcare industry to exchange patient data, claims, and other healthcare-related information between healthcare providers, insurance companies, and government agencies.
- **Financial Transactions:** EDI can be used to exchange financial transactions such as payment advice and remittance advice, reducing the time and cost associated with manual payment processing.

Advantages of EDI:

There are several advantages to Electronic Data Interchange:

- **The paper usage reduced:** The expense of storing, printing, recycling, reduces up to the maximum amount due to the EDI.
- **Improved quality of Data:** The data entry errors are reduced due to EDI.
- **Speed Increases:** The best advantage is the increase in the speed of the data interchange. With everything going online, the speed of the information transfer increases exponentially.
- **Security:** By following the Protocols and the standard rules, the security of all the important documents is always secure and safe.
- **Information accuracy:** Since the information exchanged is based on standards agreed by the sender and receiver both, the correct information is always transferred regardless of where they belong to.
- **Less Cost:** With very less errors, fast response time, every thing becoming automated, and no use of paper, the cost automatically reduces.

Disadvantages of EDI:

- The initial setup of the EDI is very Time-consuming.
- EDI standards keep on changing after some amount of time.
- A very systematic and proper back up is required as the entire data relies on EDI.
- The setup and maintenance of the EDI is very Expensive.

Classification of E-Commerce

Different types of E-commerce The major different types of e-commerce are:

business-to-business (B2B)

business to-consumer (B2C)

business-to-government (B2G)

consumer-to-consumer (C2C)

mobile commerce (m-commerce).

What is B2B e-commerce?

B2B e-commerce is simply defined as e-commerce between companies. This is the type of e-commerce that deals with relationships between and among businesses. About 80% of e-commerce is of this type, and most experts predict that B2B ecommerce will continue to grow faster than the B2C segment. The B2B market has two primary components: e-frastructure and e-markets. Efrastructure is the architecture of B2B, primarily consisting of the following: ¬ logistics - transportation, warehousing and distribution (e.g., Procter and Gamble). ¬Application service providers - deployment, hosting and management of packaged software from a central facility (e.g., Oracle and Linkshare).¬ Outsourcing of functions in the process of e-commerce, such as Webhosting,security and customer care solutions (e.g., outsourcing providers such as eShare, NetSales, Enterprises and Universal Access). ¬Auction solutions software for the operation and maintenance of real-time auctions in the Internet (e.g., Moai Technologies and OpenSite Technologies).¬content management software for the facilitation of Web site content management and delivery (e.g., Interwoven and ProcureNet). ¬Web-based commerce enablers (e.g., Commerce One, a browser-based, XMLenabled purchasing automation software). What is B2C e-commerce? 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 i.e. 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. Its origins can be traced to online retailing. B2C e-commerce reduces transactions costs by increasing consumer access to information and allowing consumers to find the most competitive price for a product or service. B2C e-commerce also reduces market entry barriers since the cost of putting up and maintaining a Web site is much cheaper than installing a “brick-and-mortar” structure for a firm. In the case of information goods, 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. What is B2G e-commerce? 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 assumed that the public sector has the greatest need for making its procurement system more effective.15Web-based purchasing policies increase the transparency of the procurement process(and reduces the risk of irregularities). To date, however, the size of the B2G ecommerce market as a component of total e-commerce is insignificant, as government-procurement systems remain undeveloped. What is C2C e-commerce? 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. • Classified ads at portal sites such as Excite Classifieds and eWanted (an interactive,online marketplace. What is m-commerce? M-commerce (mobile commerce) is the buying and selling of goods and services through wireless technology-i.e., handheld devices such as cellular telephones and personal digital assistants (PDAs). Japan is seen as a global leader in m-commerce. As content delivery over wireless devices becomes faster, more secure, and scalable, some believe that m-commerce will surpass wireline e-commerce as the method of choice for digital commerce transactions. Industries affected by m-commerce include: ● Financial services, including mobile banking (when customers use their handheld devices to access their accounts and pay their bills), as well as brokerage services (in which stock quotes can be displayed and trading conducted from the same handheld device). ● Telecommunications, in which service changes, bill payment and account reviews can all be conducted from the same handheld device. ● Service/retail, as consumers are given the ability to place and pay for orders onthe-fly and ● Information services, which include the delivery of entertainment, financial news, sports figures and traffic updates to a single mobile device. What forces are fueling e-commerce? There are at least three major forces fuelling e-commerce: 丨 Economic forces, 丨 Marketing 丨 Customer interaction forces, and 丨 Technology, particularly multimedia convergence. Economic forces. One of the most evident benefits of e-commerce is economic

efficiency resulting from the reduction in communications costs, low-cost technological infrastructure, speedier and more economic electronic transactions with suppliers, lower global information sharing and advertising costs, and cheaper customer service alternatives. Market forces. Corporations are encouraged to use e-commerce in marketing and promotion to capture international markets, both big and small. The Internet is likewise used as a medium for enhanced customer service and support. It is a lot easier for companies to provide their target consumers with more detailed product and service information using the Internet. Technology forces.The growth of ecommerce. For instance, technological advances in digitizing content, compression and the promotion of open systems technology have paved the way for the convergence of communication services into one single platform. This in turn has made communication more efficient, faster, easier, and more economical as the need to set up separate networks for telephone services, television broadcast, cable television, and Internet access is eliminated. From the standpoint of firms/businesses and consumers, having only one information provider means lower communications costs. Components of Successful e-commerce transaction loop: E-commerce does not refer merely to a firm putting up a Web site for the purpose of selling goods to buyers over the Internet. For e-commerce to be a competitive alternative to traditional commercial transactions and for a firm to maximize the benefits of e-commerce, a number of technical as well as enabling issues have to be considered. A typical e-commerce transaction loop involves the following major players and corresponding requisites: The Seller should have the following components: ● A corporate Web site with e-commerce capabilities (e.g., a secure transaction server); ● A corporate intranet so that orders are processed in an efficient manner; and ● IT-literate employees to manage the information flows and maintain the ecommerce system. Transaction partners include: ● Banking institutions that offer transaction clearing services (e.g., processing credit card payments and electronic fund transfers). ● National and international freight companies to enable the movement of physical goods within, around and out of the country. For business-to-consumer transactions, the system must offer a means for cost-efficient transport of small packages (such that purchasing books over the Internet, for example, is not prohibitively more expensive than buying from a local store). ● Authentication authority that serves as a trusted third party to ensure the integrity and security of transactions. Consumers (in a business-to-consumer transaction) who: ● Form a critical mass of the population with access to the Internet and disposable income enabling widespread use of credit cards; and ●

Possess a mindset for purchasing goods over the Internet rather than by physically inspecting items. Firms/Businesses (in a business-to-business transaction) that together form a critical mass of companies (especially within supply chains) with Internet access and the capability to place and take orders over the Internet. Government, to establish: ● A legal framework governing e-commerce transactions (including electronic documents, signatures, and the like). ● Legal institutions that would enforce the legal framework (i.e., laws and regulations) and protect consumers and businesses from fraud, among others.

Applications of E-Commerce.

- ***Retail and Wholesale***

  Ecommerce has numerous applications in this sector. E-retailing is basically a B2C, and in some cases, a B2B sale of goods and services through online stores designed using virtual shopping carts and electronic catalogs. A subset of retail ecommerce is m-commerce, or mobile commerce, wherein a consumer purchases goods and services using their mobile device through the mobile optimized site of the retailer. These retailers use the E-payment method: they accept payment through credit or debit cards, online wallets or internet banking, without printing paper invoices or receipts.

- ***Online Marketing***

  This refers to the gathering of data about consumer behaviors, preferences, needs, buying patterns and so on. It helps marketing activities like fixing price, negotiating, enhancing product features, and building strong customer relationships as this data can be leveraged to provide customers a tailored and enhanced purchase experience.

- ***Finance***

  Banks and other financial institutions are using e-commerce to a significant extent. Customers can check account balances, transfer money to other accounts held by them or others, pay bills through internet banking, pay insurance premiums, and so on. Individuals can also carry out trading in stocks online, and get information about stocks to trade in from websites that display news, charts, performance reports and analyst ratings of companies.

- ***Manufacturing***

  Supply chain operations also use ecommerce; usually, a few companies form a group and create an electronic exchange and facilitate purchase and sale of

goods, exchange of market information, back office information like inventory control, and so on. This enables the smooth flow of raw materials and finished products among the member companies and also with other businesses.

- ***Online Booking***

  This is something almost every one of us has done at some time – book hotels, holidays, airline tickets, travel insurance, etc. These bookings and reservations are made possible through an internet booking engine or IBE. It is used the maximum by aviation, tour operations and hotel industry.

- ***Online Publishing***

  This refers to the digital publication of books, magazines, catalogues, and developing digital libraries.

- ***Digital Advertising***

  Online advertising uses the internet to deliver promotional material to consumers;it involves a publisher, and an advertiser. The advertiser provides the ads, and the publisher integrates ads into online content. Often there are creative agencies which create the ad and even help in the placement. Different types of ads include banner ads, social media ads, search engine marketing, retargeting, pop-up ads, and so on.

- ***Auctions***

  Online auctions bring together numerous people from various geographical locations and enable trading of items at negotiated prices, implemented with e-commerce technologies. It enables more people to participate in auctions. Another example of auction is bidding for seats on an airline website – window seats, and those at the front with more leg room generally get sold at a premium, depending on how much a flyer is willing to pay.

  E-Commerce is all around us today, and as an entrepreneur, you should also get into this realm if you want to expand your markets, get more customers and increase your profitability.

Questions Bank

1. Define E-Commerce and list out their Advantages and disadvantages
2. Briefly discuss about Anatomy of E-Commerce
3. Explain in detail about classification of E-Commerce
4. Define EdI and Explain Layered Architecture of EDI.
5. Discuss briefly about Information Technology Act 2000.
6. Define Firewall and explain its types in detail.