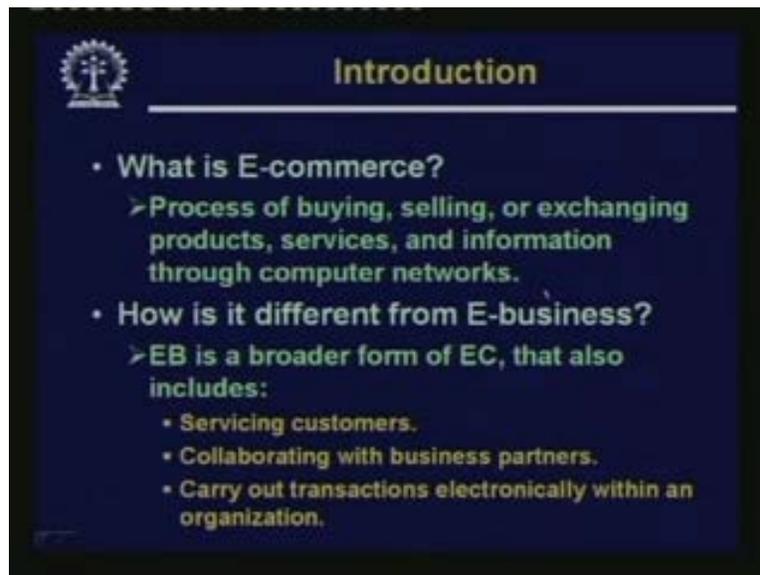


Internet Technology
Prof. Indranil Sengupta
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur
Lecture No #35
Electronic commerce

In the last few lectures we were talking about the various cryptographic techniques and primitives some applications. Now today in this lecture we shall be talking about one most important application of security. In general which has pervaded the internet and also all lives in a sense. You are right; we are going to talk about electronic commerce. Now electronic commerce is a subject which has significant components from various interdisciplinary areas. Well, computer science and IT is one area. Of course there are a number of managements and social aspects as well. So today our topic of discussion is electronic commerce.

(Refer Slide Time: 01:45)

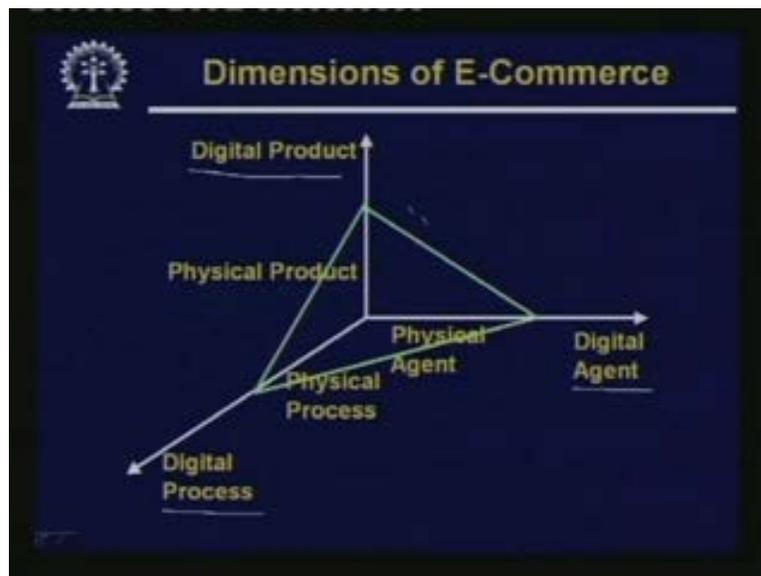


First let us try to see what we really mean by electronic commerce or e-commerce in short. Now electronic commerce you can define as follows. It can be defined as the process of buying selling or exchanging products services and information through computer networks. Now in this definition there are a few important terms like we have mentioned that all this transactions are being carried out over a computer network. This is important and second we are not only transacting products but also services and information. So we are broadening the scope of trading over the computer network under the preview of e-commerce. Now there is another related term sometimes used E-business electronic business. Now though people use two terms interchangeably.

But there is a distinct difference electronic business of EB in short is in a sense a broader form of electronic commerce. So it is essentially electronic commerce which also includes the following. They can also have a mechanism to service the customers which normally E-commerce does not

provide collaborating with other business partners and carry out transactions electronically within an organization. Normally when you talk about e-commerce we mean transactions between an organization and some customer or a person who is sitting outside. But here we can also have transaction inside an organization. That is what business is all about. Now let us look this diagram.

(Refer Slide Time: 03:50)



This diagram shows you some of the dimensions of electronic commerce. You see here we have shown a three dimensional coordinate axis system where on one end we are showing the digital products, on the other side we are showing digital process, on the other side, digital agent. Now as we move towards the agent. You see we have the corresponding physical vertex physical product, physical process, physical agent. Now this triangle which is shown here, the size and the position of the vertices of this triangle actually decides that whether we are towards the physical domain or towards the digital domain. Now the difference between this physical domain and the digital domain should be clear.

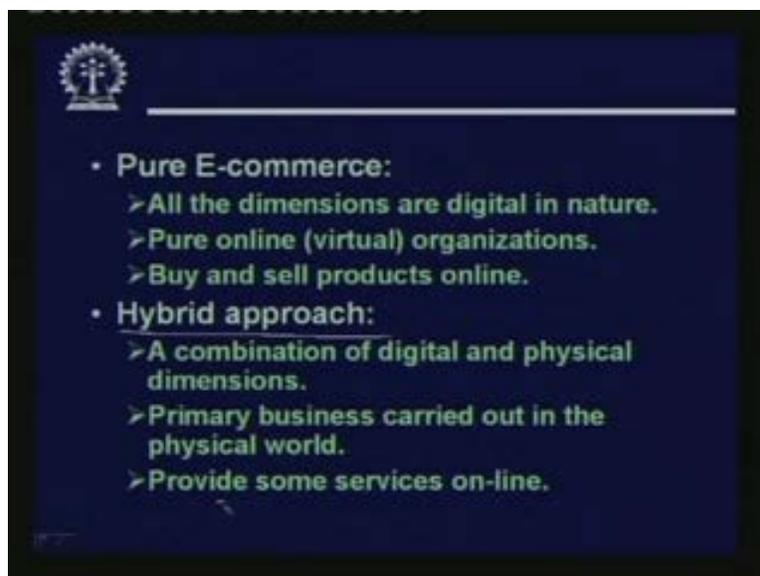
See when we do a conventional shopping, we go to a shop physically we select the items to purchase; then we pay our money and get the item we want to purchase. So that is an example of a physical transaction where the parties in question have to physically interact among themselves by being physically present at a particular place. When you are transacting over the network through the internet then you need not be present physically. You are digitally sending request over the network and you are getting back a confirmation or request again digitally over the network. So this is the difference between physical and the digital transactions. Now as this diagram shows again there is an axis for products agents are the middle men and the process steps involved.

(Refer Slide Time: 05:41)



If we talk about traditional commerce which we are more familiar with, at least till today here all the dimensions are physical in nature, the agents, the process and also the products. Here all the business transactions are carried out offline. Buying and selling products are carried out through physical middlemen or agents and their representatives. So in traditional commerce there is the concept of physical one-to-one interaction and physical transactions carried out. So the essential idea is that a person has to be physically present at a particular designated place in order to carry out certain step of the transactions.

(Refer Slide Time: 06:37)

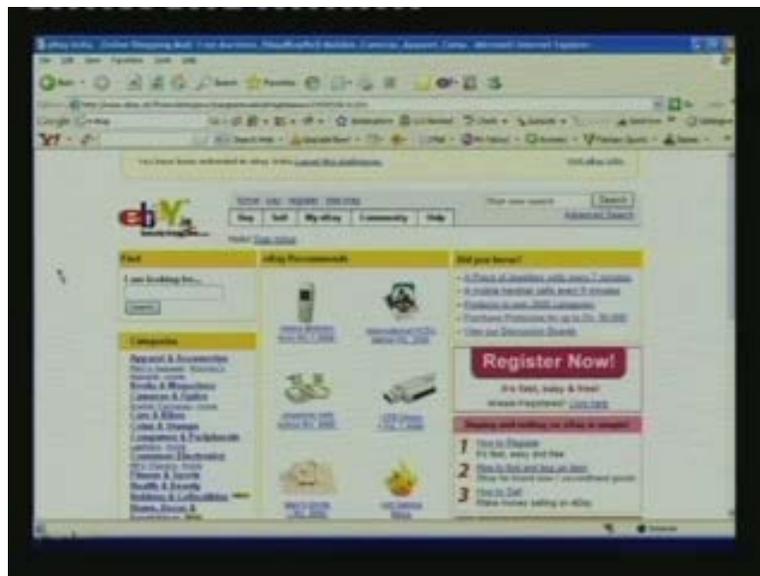


Let us now talk about pure E-commerce. Now in a pure electronic commerce all the three

dimensions are digital in nature. Pure online or virtual organization and also buying and selling of the products are done online. Now pure E-commerce is a good concept but in practice most of the kind of products that we used to buy or most of the transactions we want to make it cannot be handled in a pure electronic form. For example I order a book over the net. I specify my credit card to make the payment everything is fine up to here. But when the book is to be delivered to me, someone has to give it for posting or through courier and the book has to be physically delivered to me. This is one part which cannot be done electronically.

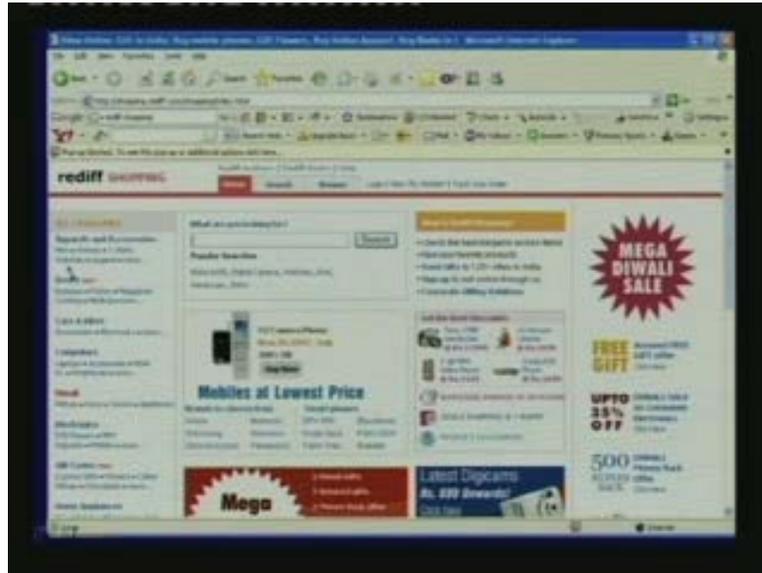
But however if I purchase a software product, a software tool for which I make a payment and after making the payment the company or the seller allows me to download that program from the network. So here everything is done electronically. There is no physical involvement of anybody involved here. So what I mean to say is that in practice we mostly see some kind of a hybrid approach. Some combination of digital and physical dimensions. This is most common nowadays. The primary business which consist of the actual delivery of the equipment's. The goods, the products, they are carried out in the physical world. But the other services and other parts of the transactions they can be carried out electronically over the network.

(Refer Slide Time: 08:35)



Now some examples this is the website of the well-known ebay portal. The ebay you must have heard of this portal. This ebay is a website which allows any one to advertise their products and to buy and sell them. Suppose I have a product to sell I can post it on bay and any prospective buyer can login to ebay and look at my product and if he or she likes it can buy. It also provides means of auctions. The best bid whoever puts in gets the product. So ebay is one such very popular website through which these kinds of transactions can be carried out. Let us look at another website rediff shop.

(Refer Slide Time: 09:24)



Now rediff shopping, I am sure many of you have heard the experience of transacting using rediff shopping. Through rediff shopping you can have a wide variety of products which you can buy, which you can send to your friend as a gift and so on. So here again there is an interface which you can select the products. You can view the prices you can view the different variations, different manufacturers and you can select.

(Refer Slide Time: 10:00)



Then we have another portal amazon.com. Now today amazon.com looks very much like yet another shopping site. But when amazon.com was initially, you can say initiated or started. It was basically a portal which was meant for buying and selling of books. But today books are

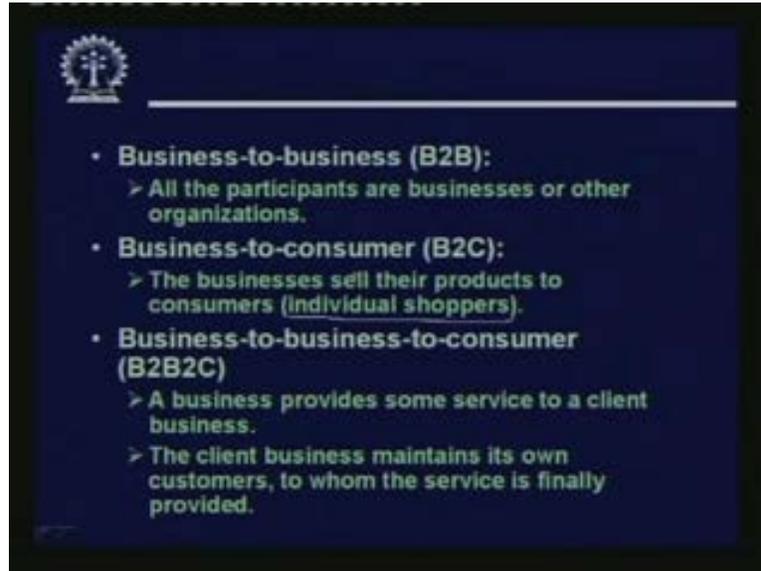
available, of course but you can buy other things as well. Well if you look into this page you will see that there is an advertisement for a Samsung high definition TV. There is an advertisement of a camera, dress, materials, etcetera. So all these kind of things are also available through that same single portal amazon.com. So I have shown just some examples which have become so popular. Through these websites through these portals we often carry out several transactions electronically and that constitutes electronic commerce. But now the question arises that in order to do these kinds of transactions what are the requirements? What are the different kinds of transactions one is expected to make? And of course what are the security requirements which we become very important in this changing scenario where I am making payments over the network by typing in my credit card number and other sensitive information over the network? If anyone get hold of these then there is of course ample scope out. So this is one issue which has to be addressed in a very clear and definitive way.

(Refer Slide Time: 11:48)



So now let us try to look at some classification of E-commerce by the nature of transaction. Now transactions can be carried out by various parties in a number of different ways. So here we try to look at the different kinds of variation in that respect.

(Refer Slide Time: 12:10)



Business to business or B2B, this is the kind of transaction where the participants are businesses or other organizations. Which means the end user or the customer is not a part of this transaction. Say one business house is transacting with another business house carrying out some kind of transaction which is meant for the own product for their own development, that kind of thing. But it is not the way you are selling a finished a product to a customer. But in this business to consumer you do that business to consumer or B2C. Here the businesses sell their products to consumers. So here we are talking about the individual shopper websites like rediff or amazon. They are basically B2C kind of systems. Now there an individual sitting in his own room can use the internet facility to select a product and place an order for the same. So these kinds of things are possible.

Now in more complex kind of transaction you may involve business to business to consumer kind of things where one business house is sending some information to another business house which in turn is servicing the customers or consumers. So a business provides some service to a client business. So here we are defining some kind of hierarchy of businesses. So now representative agents they may represent a larger company. This is one example you can have a larger company. That company carries out transaction with smaller the zonal representatives. And the zonal representatives in turn they service the consumers of the individual customers. So business provides some service to client business and the client business will maintain its own customers to whom finally the service would be provided. This is the concept of B2B2C.

(Refer Slide Time: 14:29)



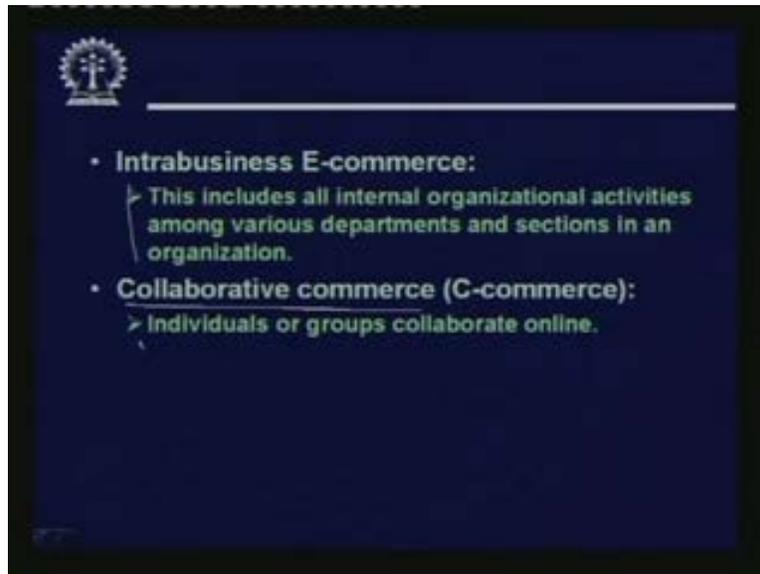
Consumer to business like that ebay portal I have mentioned where you can both buy and sell things. Here an individual can also sell products or provide services through the internet to organizations. These products can be meant to businesses like in C2B or it can be consumer to consumer like C2C? Say myself as a consumer I am posting details of a product on the website and you as an individual can come to that website and buy that product. So it is a customer to customer interaction to a common platform. This is the so called C2C. So here an individual sells products or services directly to another individual. But there are two new kinds of transactions which have started to become popular nowadays. One is called mobile commerce, other is called location commerce.

Mobile commerce is essentially E-commerce in a wireless mobile environment. Nowadays almost all of us are in position of a mobile phone and the day is not far where all these kinds of transactions we can carry out through our mobile phone. And when you do it through our mobile phone it should have some additional functionality available on the mobile through which we can carry out meaningful transactions. And when I say these additional facilities this includes the security aspects of it. And this location commerce is a special form of mobile commerce of M-commerce. Location commerce I am giving an example. Suppose I am traveling in a new city, I have arrived in a new city. I am walking along the road.

Now automatically some SMSs will arrive on my mobile telling me or informing me about the shops in my immediate neighborhood. So there will be system which will globally track my location where I am and will continuously keep me updated with context dependent information. Either it can come through an SMS or it can come out of some user request. I can ask. I can send a request that, what are the good places to eat in the nearby vicinity of where I am standing now. So this falls under the preview of L commerce; location commerce. So these are basically M commerce transactions targeted to individuals in specific locations at specific times. So I have given you just one example so you can easily expand this scope of this to cover more complex

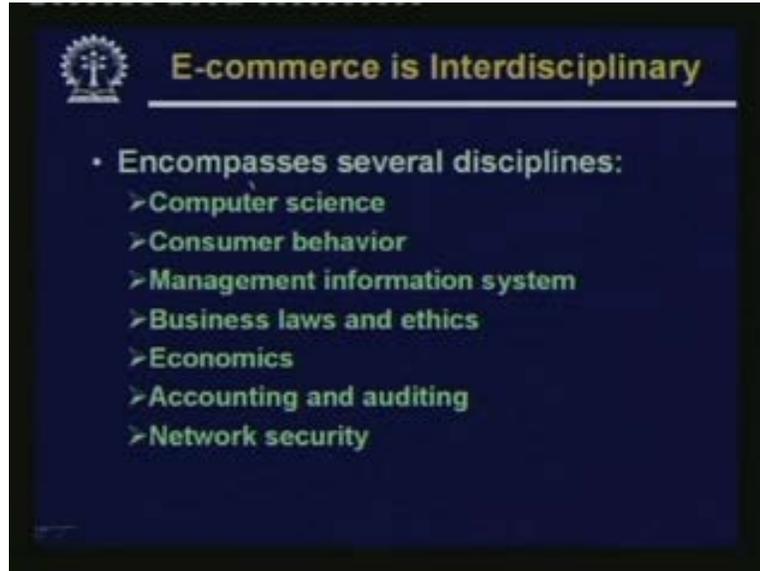
kind of situations.

(Refer Slide Time: 17:24)



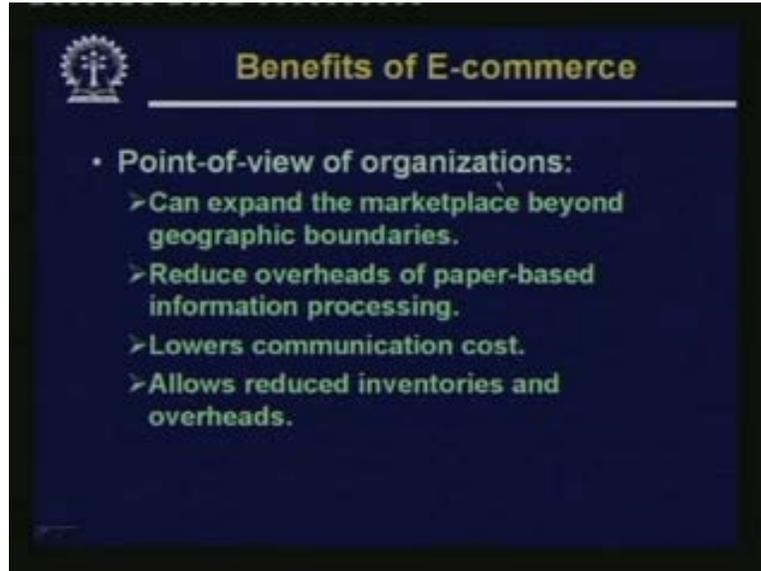
There can be intrabusiness E-commerce. This means, inside an organization all internal activities amongst the various departments sections and units they can carry out transactions in a similar way and there is a concept called collaborative commerce where individuals or groups they collaborate. This is not exactly buying and selling items. They do some kind of collaboration in order to carry out some meaningful task. So we have seen the different variations the different kinds of transactions that can be carried out in an electronic scenario when we are in the digital world.

(Refer Slide Time: 18:12)



Now I mentioned earlier that E-commerce is an interdisciplinary activity. Now this slide actually highlights what I really meant by that. Say any E-commerce solutions if you want to arrive at a good and meaningful E-commerce solution it must encompass several disciplines. Computer science and information technology is of course one analysis of consumer behavior management information system. Business laws and ethics, economics, accounting, auditing and of course last but not the least network security. So many things all come into the picture when we are talking about E-commerce. Because here we are talking about a new and emerging way or mechanism of carrying out business which is bound to change our daily lives. So there is a very strong social impact as well. So all this interdisciplinary issues come into the picture starting from laws and ethics down to consumer behavior and so on. So this is one issue.

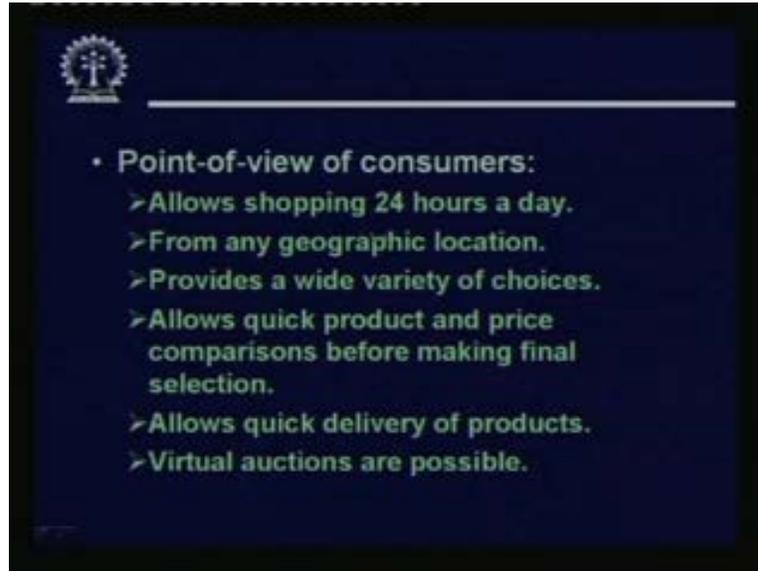
(Refer Slide Time: 19:25)



Looking at the benefits where some of the benefits you can immediately understand from the point of view of organizations we are trying to sell their products. E-commerce will help us in expanding the marketplace beyond the geographic boundaries. Earlier when you opened a shop you would have expected that the customers of the shop would only be the persons who are coming from the neighborhood. But now if you have set up a portal or a website through which you are allowing people to carry out business or shopping online you do not know exactly where your customers are physically located. May be in the same neighborhood, may be in another neighborhoods other cities other countries you really do not know. So this helps in breaking the geographic boundaries or guidelines. Obviously it will reduce lots of overheads of paper based information processing. It virtually eliminates the user of paper lowers communication cost.

Because everything is done digitally over the internet which is a very low cost network infrastructure and it allows reduced inventories and overheads. Now in your shop, you would be stocking items in excess amount with expectation that people might come and they should find the item in stock. But now you have a scenario when after getting an order you give them a promise that your item would be delivered in 24 hours or 48 hours. Then you need not keep everything in stock. After getting the order you can process the order so that the items get delivered by the specified deadline. It is not necessarily true that the item has to be delivered from your shop physically. There can be several centers located worldwide the nearest center may entrust the responsibility of sending the requested item to the customer by post.

(Refer Slide Time: 21:39)



Now from the point of view of the consumers let us see the advantages. Now from the point of view, of consumers of course the biggest advantage is that this allows shopping 24 hours a day. Today you can buy a train ticket or you can buy an air ticket sitting at your home anytime of the day. The day has passed where you have to stand in a long queue in a reservation counter and you will have to wait till your turn comes when you arrive at the counter and find out what are the tickets available, what are the different alternatives. You often do not get sufficient information before you can take a decision because your time is short at the counter. But now when you have this portals you can relax you can see the different alternatives say for instance if you are talking of a train ticket you can see what are the different trains, what are their times, what are the seat availability in the different classes, dates and you can select the train in which you want to decide to travel and you can make the booking accordingly. So this is a very big advantage you get in the modern day scenario.

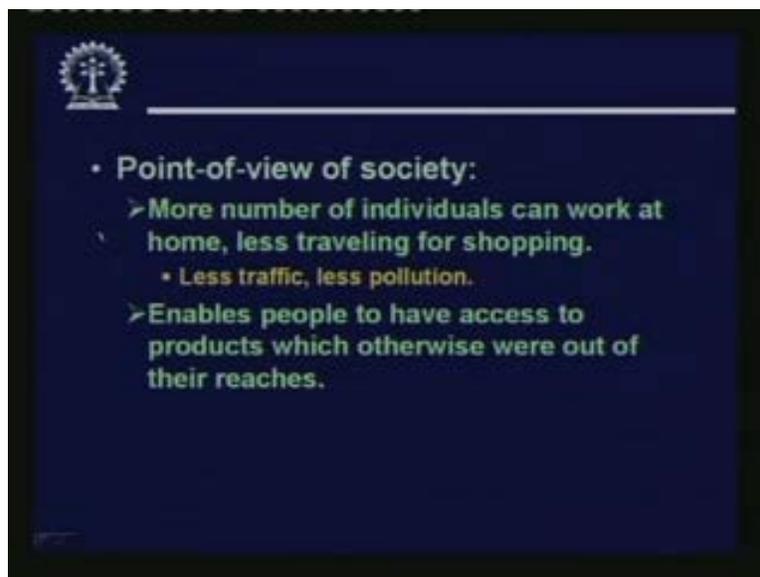
And second thing is that it is not necessary from your home you can do so from any geographic location. This is a very big advantage. Even if I am on the move, even if I am sitting on the airport, if I have an internet access I can buy a train ticket sitting there itself. I need not have to contact any agent. I need not have to go to anybody. I can make that booking myself. So there are many such electronic transactions which eliminate the need or the presence of the middlemen. You know that there are many cases where these middlemen can prove to be a good nuisance. This is one example I have sited where the convenience to the end user can be expanded or increased many forth and I mentioned it provides a wide variety of choices. Now the user can look at the different varieties compare their qualities their prices and then can decide on the exact product or the auction to select.

It allows quick product and price comparison as I said before making the final selection. These are relative terms allows quick delivery of products depending on where are you, depending on where your nearest delivery center is. Products are delivered really fast. Of course if you keep in mind, products will not be delivered as fast as when you go to a shop and buy a packet of biscuit

it can never be that fast. It will have to be sent by post or by courier it has to reach that way to your home. And I have said that websites like ebay they also allow you to participate in auctions. Virtual auctions are possible. Well, why I say virtual auction? Because, if you look at the real auction houses, there you will have to visit the auction house, in person you will have to look at the items physically which are up for auction of course looking at physically with your own eyes.

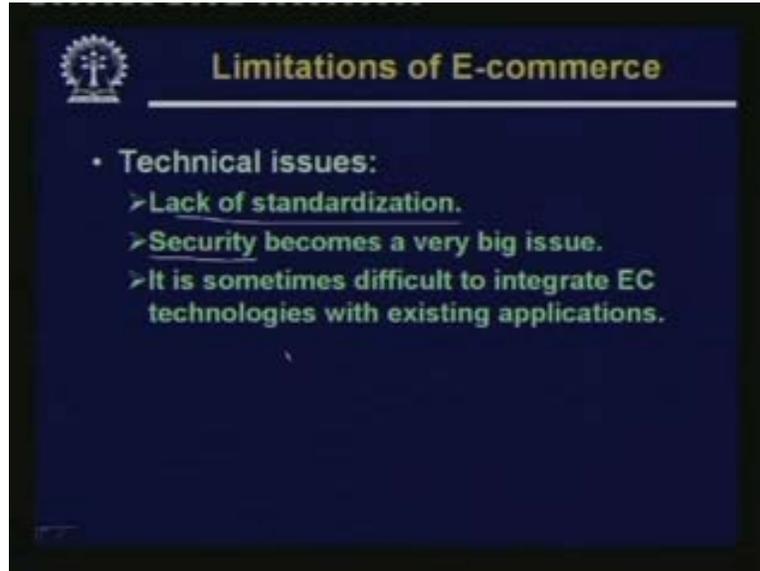
There is no substitute for that and after that you can participate in the auction. You can present your bids and there is a very finite during our presence at that place whoever gives the highest bid gets that product. But now you have a different scenario where all the details specification of the products that can include the photographs shot video clips and like they are available in the website. You can have a look at them and after you are satisfied about the product you want to bid for you, can post to bid. And for all products there is typically a last bid time 48 hours. So within that 48 hours, whoever is the highest bidder you an also have a look at the current or the present highest bid. So you can carry out auction this way. That is why it is called virtual auction because you are not present physically at the auction site.

(Refer Slide Time: 26:21)



Now some advantages from the point of view of the society. Well in our country we still do not see this as much as we see it in other countries. But I am sure a day will come when we will see this pretty widely more number of individuals can work at home and less traveling for shopping. Which means, indirectly less traffic less pollution because the vehicles are the biggest source of pollution if you have to travel less your pollution will also get down? Second important thing is that with this feature people can have access to products which otherwise were out of their reaches. Say sitting here sitting at your home you can order for a product which otherwise is not available in your country. The product is manufactured in some other country. If you place an order for it will be sent to you buy post. This is another big advantage you get. So the advantages are there from the point of view of the business house. The shop, the customer and also from the point of view of the society in general.

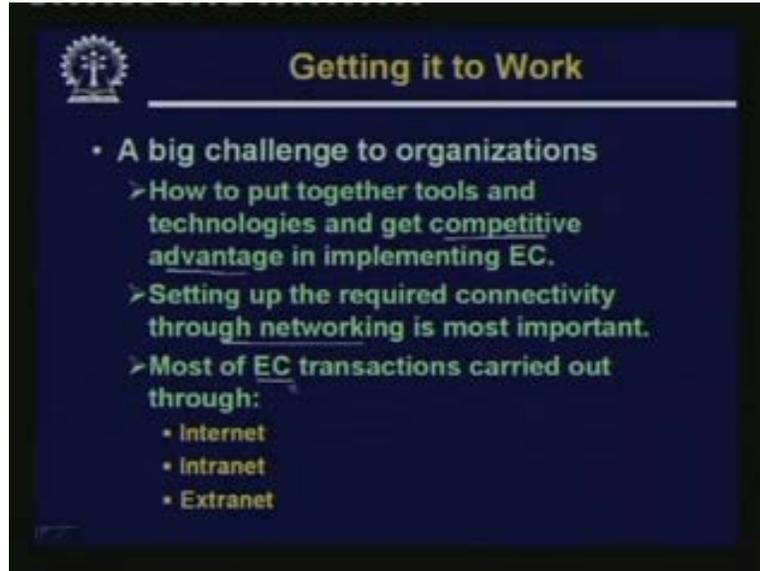
(Refer Slide Time: 27:49)



There are some limitations too. The main limitation is lack of standardization. So as I have said this amazon.com was one of the first websites which came up with this concept of online shopping. They started with books. In the same way there are numerous other websites and other you say, these kinds of E-commerce portals which have come up. But the problem is that most of them have come up with their proprietary interfaces and protocols. There is absolute lack of standardization of course some standards have been proposed and used. But the number of such standards are also too many. So this is one big problem that faces a prospective user or a provider of E-commerce.

Suppose you have a company you want to provide for E-commerce you will have to decide how you want to go about doing it. What are the standards you need to follow? There are a number of such issues. Of course security is most important. Because unless you can have almost virtual security; virtually fool proof security, you cannot convince your customers to come and carry out business with you. Due to this lack of standardization primarily it becomes difficult sometimes to integrate electronic commerce technology with existing applications. Because they were developed at different times with different goals in mind. When you want to integrate the two, there are a lot of issues in the interfaces. Lot of incompatibilities miss matches. So you need to put in a lot of effort in order to develop an E-commerce application.

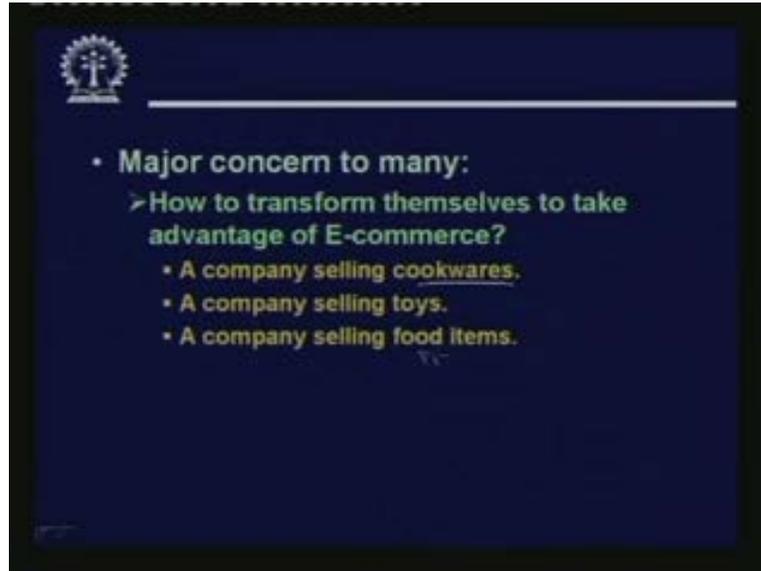
(Refer Slide Time: 29:52)



Now in order to get the whole thing to work, there are some challenges to the organizations which you need to address. First thing is that as I said there are many tools and technologies which are available, there are too many standards. So the organization has to decide how to put together all these tools and technologies to have a good and feasible system which can enable you to get competitive advantage over your rivals. Secondly, setting up the required connectivity through networking. This is of course important. You need to have good connectivity. Well the customers will not be satisfied if they have to wait too long when they are trying to carry out some transaction.

So you must ensure you have to carry out a survey. What is the kind of customer demand you expect and what is the kind of bandwidth you need to provide to meet the requirements. So your internet bandwidth and other network infrastructure should very much depend on that kind of a customer survey. And thirdly is that organizations must keep in mind that most of the electronic commerce transactions are carried out through internet intranet and extranet. So suitable technologies, suitable security policies, security mechanisms, should be placed in order to, you can carry out such transactions securely in the environment under question. It can be internet, it can be intranet or extranet.

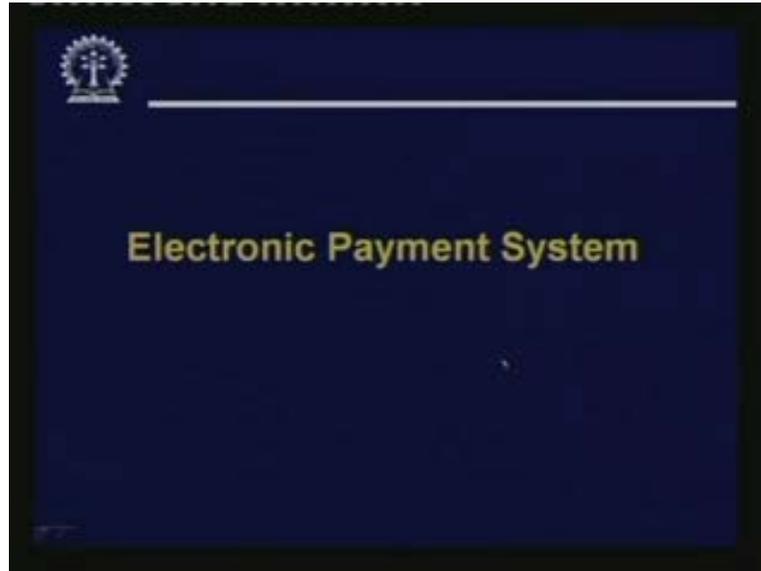
(Refer Slide Time: 31:44)



There is some concern like suppose you have a company, you have a shop; you sell some product. The question is how do you transform yourself to take advantage of E-commerce? Now here there are a number of issues. See you look at the kind of company suppose I am a company who wants to sale goods. If I am a company who sell books, it is not an issue, I accept orders. There are some courier services with whom I have a tie up. They come I give the books with the address and they send the books by courier to the customers. Suppose I am a toy shop. For a toy shop the main problem arises that a book user can select on line in a much better way. But for toys it gives a different kind of an impact when someone sees the toys, touches it with the hand sees it from different angles its capabilities. So these are the kind of things which has to be kept in mind. So if you are a prospective toy seller you should set up your portal in such a way that something closest to this can be provided.

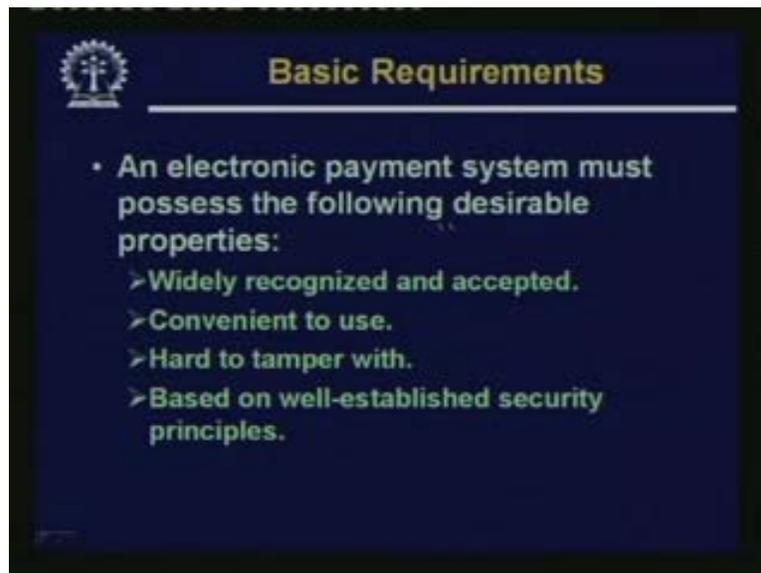
For example you can provide some short video clips animations of the toys. You can show pictures of the toys from different directions angles. You can give the detail specifications and stuff. So these are the things. But you think of some companies which is selling cookware, food items, their requirements and the way they will be advertising their products will be very much different. So if you are a company which is selling food then the way you will be advertising for the food will be entirely different from the way you will be advertising from say advertising for toys. So this is the kind of analysis you have to make and you will have to design your portal in an appropriate way. So these are the biggest challenges, you can come up with a portal. But a prospective customer will come to a portal not find enough information not to be convinced and go to some other place. This is certainly not what you want.

(Refer Slide Time: 34:18)



Now let us come to the most important issue here; the electronic payment system. Now here we are talking about transactions carried over the network. So ultimately somehow payments are the most important thing behind transaction. Payments have to done electronically because if this is one part which has to be physical. Someone has to go physically and carry it out. Then it is no good you have to have some mechanism.

(Refer Slide Time: 34:56)



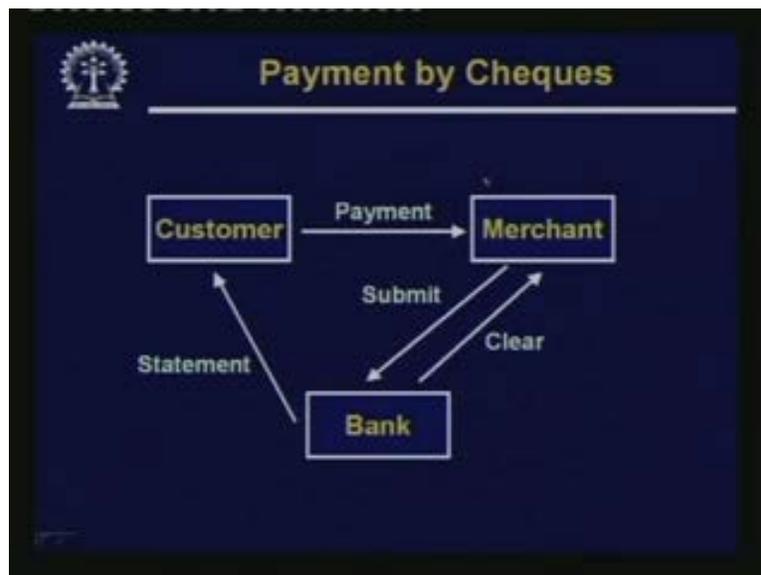
Now the basic requirements of an electronic payment system are follows. Any electronic payment systems satisfy the following requirements. It must be widely recognized and accepted. It must be convenient to use. It should be hard to tamper with; it should be based on well-

established security principles. Now actually we would be talking about several such electronic payment systems. But before going into that I would like to show you some technology which we use pretty frequently. Like many of you would have a smart card, here I have a smart card in my hand. This looks very much the size of a credit card. But if you look into this card, one corner there is a small built in processor and circuit which is there inside the card.

So unlike credit card which just stores some static information in it, I put it or swipe it on a card. This static information gets extracted and gets authenticated from some other place in this card. In addition to some storage I also have a small processor. It is typically an 8 bit microprocessor. It can also be a 16 bit processor. The idea is that this card not only has some information data about myself stored. It also has some processing capability with which I can carry out or I can run some cryptographic algorithms locally on my card and you may be have a device like this. This is called a card reader. This kind of a card can go inside and you can have connectivity to a pc. There is a cable you can connect.

This device to a pc, you can develop an application and this application may demand you to insert this card into this device. Now what might happen here is that some algorithm or some tools software may be run running locally on the card which can give you unparalleled security. Which otherwise you cannot achieve by either a credit card or something. So if you have a smart card is the technology of tomorrow. If you have a smart card you can do much more than just providing your identification and authentication. You can carry out some very sensitive computation even locally inside the card. The card is a memory and also a small processor. It is a very small computer inside.

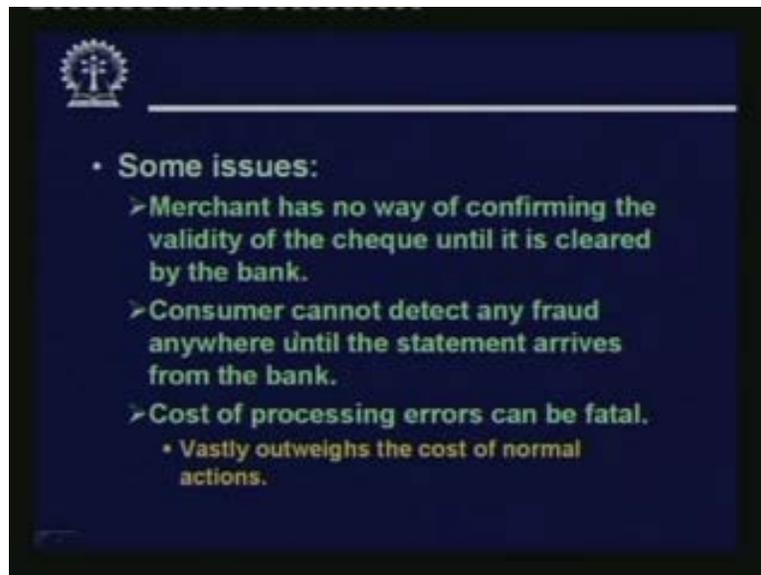
(Refer Slide Time: 37:59)



So now let us look at the different types of payment systems. First we look at the way we which we are most familiar with payment by cheques. Well payment by cash if of course there. But I am not considering that. We are considering those kinds of transactions where some flow of process is there before the money actually exchanges hands. If it just payment by cash it is direct

payment between the customer and the shop. But in the payment by cheque diagrammatically is shown here. The customer makes a payment to the merchant by cheque. The merchant after receiving the cheque submits it to the bank and the bank after verification clears the cheque; sends intimation to the merchant that the money has been transferred to the account of the merchant. And finally periodically the customers will be provided with a bank statement which will show that the amount which was paid to the merchant by cash has actually being deducted from the customer's account. But this system has some drawbacks.

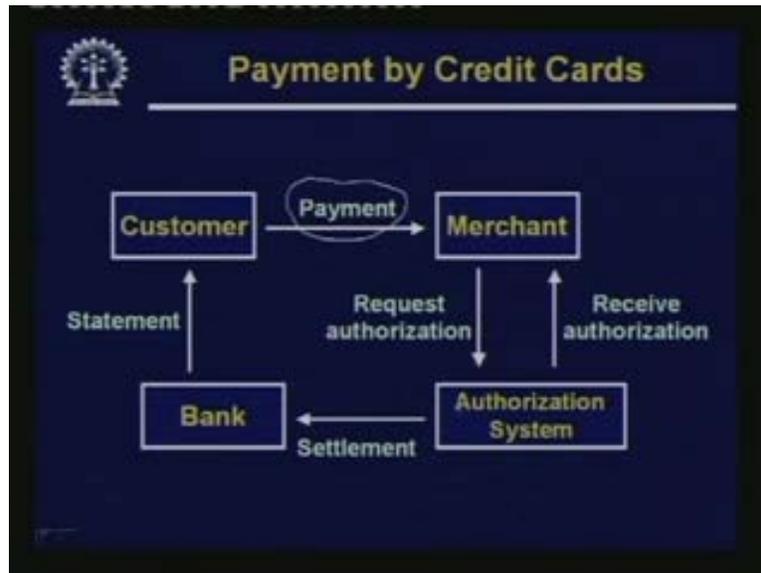
(Refer Slide Time: 39:30)



The first is that the merchant has no way of confirming the validity of the cheque until it is cleared by the bank. This is why sometimes cheques bounce. This can be delivered; this can be due to some mistake on the part of the customer. Suppose I do not remember how much money I have in the bank. Suppose I have 5000 rupees I write a cheque for 6000 rupees. The cheque will get bounce from bank. So unless the cheque is submitted and the cheque bounces back the merchant does not come to know this the customer has paid a cheque and has taken away a product. But the money is not realized. This is one drawback here. So the consumer also will not be able to detect anything until the statement arrives from the bank. So here also there is a chance of a fraud.

Suppose I have written a cheque, someone adds some additional digits to the value also write somehow in the space provided in the amount. So that the amount in the cheque gets increased, it is some kind of fraud and the person who has issued the cheque will also not know about the fraudulent until or unless the cheques the bank pass book later after updation. So after looking at the bank statement I will come to know actually how much money was paid by me. The cost of processing errors due to some error, if there is some error in the figures. Say earlier all transactions were done by the banks manually. The moneys or the amounts they were written in some ledger books by clerks. If there are some errors in the recording, so this error could have been fatal. The cost of processing errors in this case can vastly outweigh the cost of normal actions. This is one drawback.

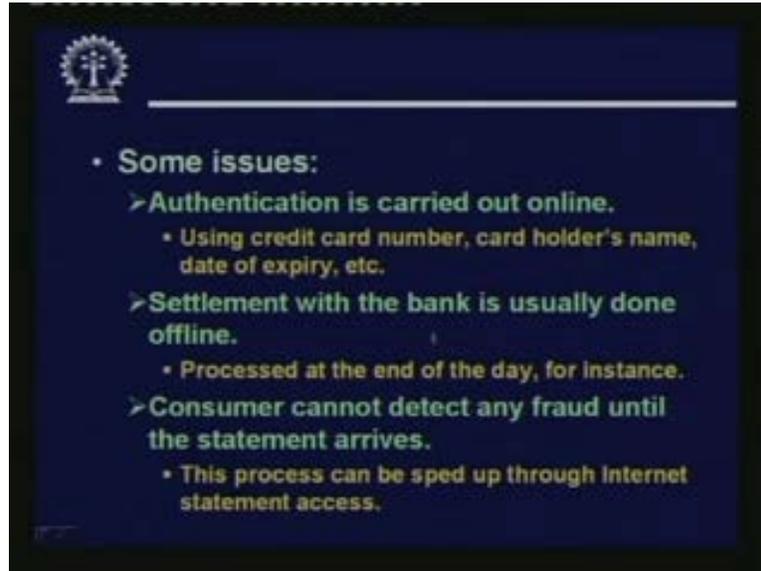
(Refer Slide Time: 41:36)



So now most of us carry out transactions using credit cards. Now let us see this. Now if you are using credit cards, there are slight different modes of flow which you follow. Customer makes payment to the merchant. Now this payment which I have shown here, this is not the payment of a cheque or the money. Rather I go the shop, I show the credit card, I swipe the credit card on the credit card machine of the merchant and the merchant of course gets some kind of a confirmation from the local or the nearest credit card get access point of the agency. So after you give the payment swipe the card, merchant contacts the authorization system, requests for the authorization, receives the authorization.

And after this authorization is received the small slips which are there in the machine gets printed. And the customer is asked to sign one of those slips and return it back to the merchant. Merchant later on will submit that physically to the bank. So until or unless merchant submits that slip physically to the bank money will not be realized. Money will not be transferred. So there is a settlement which is done offline to the bank. So after the settlement process is complete, only then the money is deducted and finally the customer will come to know that the money has been deducted when the customer receives the statement from the bank finally. But here also there are a number of issues. The issues are as follows.

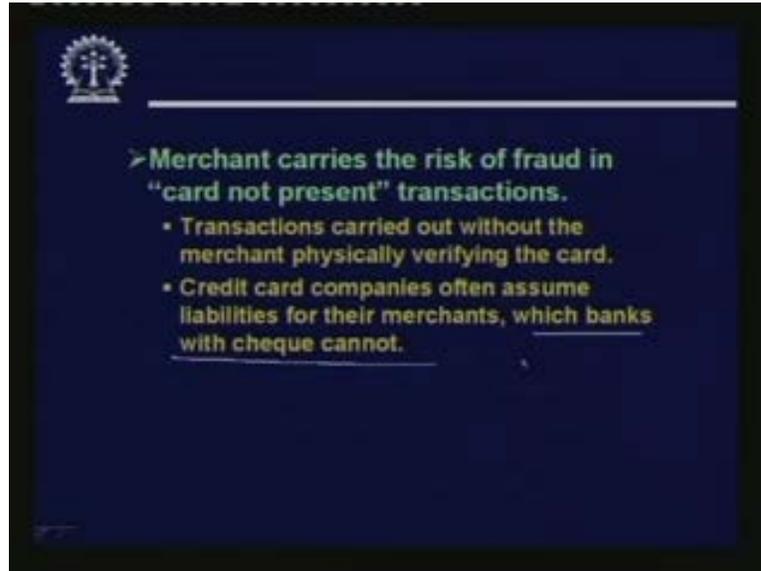
(Refer Slide Time: 43:45)



First is that authentication or the customer identification is carried out online. How? Nowadays in almost all credit cards the photograph of the customer is there. So when I go shop with my credit card my photograph is verified. There is my signature on the card. I also signature I also put my signature on that slip. Signature is verified, my credit card number is getting authorized from the authorization agency. It also looks at the credit card number the data of expire my name all these things together. So this authentication is carried out online. This uses the credit card number, the name of the card holder, date of expiry. These kinds of information however as I said settlement with the bank is not done online, this is done offline. This processing is carried out for example at end of the day. During the day there can be many customers which will be visiting your shop. They will be making payments by credit card.

You collect all the slips and finally at the end of the day you make the adjustment or settlement with bank with those slips. Now consumer cannot detect any fraud until the statement arrives. Because sometimes we see that due to some mistake on the part of the operator the same amount may be detected twice. This kind of things happens, but the amount is typed wrongly. Sometimes this kind of error occurs. So consumer will not be able to detect this until or unless the statement arrives. This process however can be spread up, if the consumer has access to internet statement access. So the statements can be accessed online and the user can immediately login and find out that how much money was actually deducted or the request for deduction? How much money was put in? So in that way the verification can be done faster. If you have this kind of online access available.

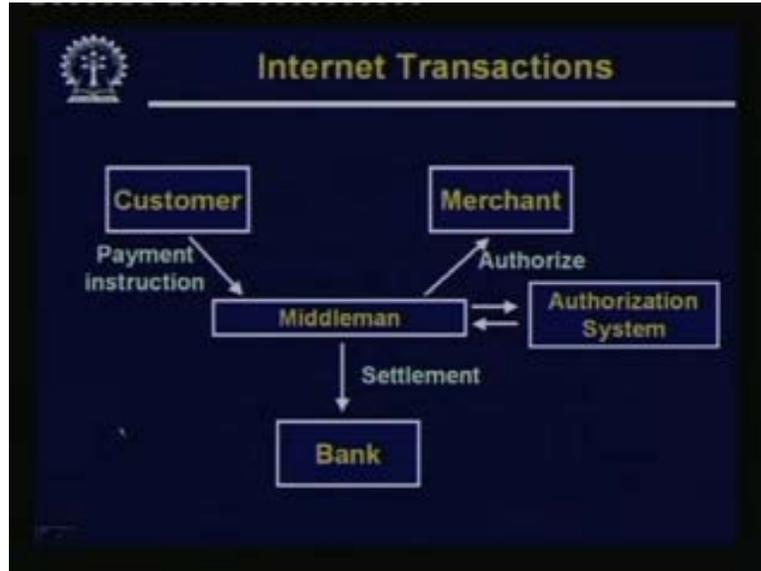
(Refer Slide Time: 46:17)



There is another thing merchant carries the risk of fraud in card not present transactions. See, here so far I have talked about the situation where the customer comes to the shop, shows the credit card, physically swipes it on the machine and gets authenticated and signs on a piece of paper and makes the payment. But nowadays you know many payments can also be made over the internet. There in addition to the credit card number your name date of the birth you are also asked to specify that secret three digit code which is there on the back of the card and some other questions some times are asked. So if you type in all this information then your purchase request will be registered and is assumed that you have made the payment. These are called so called card not present transactions. Because, the merchant has not seen the card physically. Only the card numbers you have typed, but there is no guarantee that it is your own card or you have stolen the card from somebody or you have found the card from somewhere else.

So how will the merchant check for that, it is very difficult for the merchant to check for that? Say I am giving an example. Once I went abroad I placed order online for a small electronic item, just about an hour later there was a phone call to the place from where I placed the order. Because they also ask me to type the phone number where I am right now. They called and tried to verify my identity. They asked me that was the last transaction I carried out using the card so that they can verify that whether I am the person or not. And a few other information about myself; about where I live, what I do. These kinds of information are also present in the database. So this is one way the merchant can provide or can have some kind of confidence in the identity of the person before actually approving the transaction to proceed. So as I said, these card not present transactions are those which are carried out without the merchant physically verifying the card. Usually the credit card companies assume liabilities for their merchants, which banks with cheque cannot. Banks cannot take the liabilities for the cheque. But, credit card companies usually take liability for these cases.

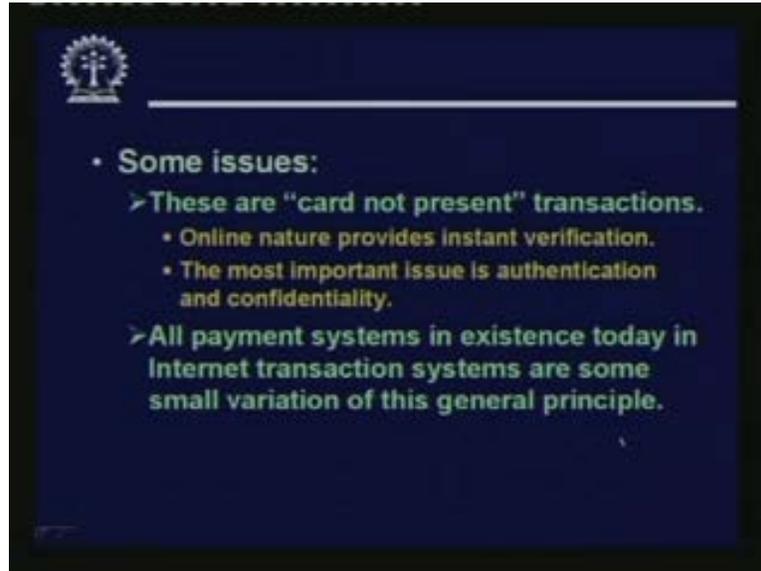
(Refer Slide Time: 49:07)



This is what we normally do over the internet. This is the typical picture of the so called internet transaction. So here you see the customer and the merchant are not interacting directly during the payment. I do not know how many of you have noticed this thing. Suppose I am going, I have visited some site through which I want to carry out some shopping. I have selected the items to purchase. Then I have clicked on payment. So now I am taken to a site which is not part of the site; it is a third party. I am taken to another site which verifies my transaction. So it is not the merchant site which I visited earlier. So the picture is somewhat like this. When I am going to make the payment, see during selection customer and merchant can interact directly. But during payment the instructions are sent to a third party or a middleman. This is a trusted site where the merchant had authorized.

So from the merchant site you will automatically be taken to this particular website. Typically this website starts with https which is actually http running on top of SSL. So all transactions whatever you type will be transmitted in an encrypted way. So you are safe in whatever you have typed in. No one else will be able to know that. So the customer will be sending all transactions to the middleman. The middleman in turn will be contacting the credit card authorization system and get it authorized. And finally inform the merchant that well I have verified I have authorized. And also the middleman will send request for settlement to the bank. Finally again as I said the bank will send a statement back to the customer later on. So the customer will know that actually how much money was deducted. So this is a typical system which we follow in the internet.

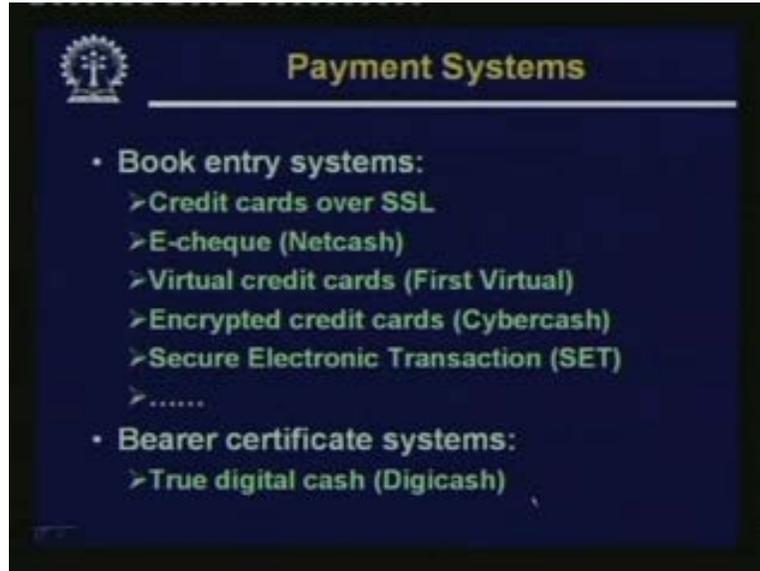
(Refer Slide Time: 51:33)



Here some issues are there again. These are all card not present transactions because as I said this is purely an internet transaction. Here whatever is done online verification by third party everything is done online settlement request to bank. This means instant verification, since everything is done online which unlike in this physical credit card transactions, sometimes verification is deferred till the end of the day. So the issues like authentication and confidentiality are much better managed here. Because you are interacting with a trusted third party through a secure interface through https and you are more confident of this transaction.

This is how this takes place. So all the payment systems that we see around us today which work in the internet namely which are internet transaction systems are some small minor variations of this general principle. You look at any shopping site they will work in a similar principle. When you want to purchase either they will take you to a third party or they will take you to a separate special secure page of their own. This is another alternative. So instead of a third party they have a similar interface built by themselves. They can use that. So the idea is similar.

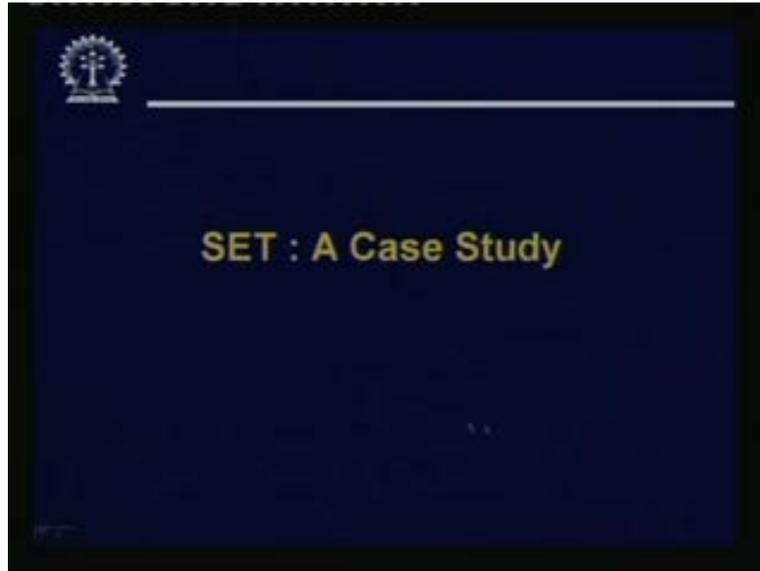
(Refer Slide Time: 53:14)



So I have said that there is a lack of standard. There are many payment systems which are present in use, many of which are in fact used over the internet also. So this slide just gives you some names credit card over secure socket layer. Electronic cheque, netcash this system which uses this. Virtual credit cards, first virtual is a system which uses this encrypted credit cards cybercash. See here the idea is that in cybercash the user whoever he or she types will never type the original credit card number. But only the encrypted version will be sent. So this is another level of production you can say and secure electronic transaction. This consists of SET protocols actually for ensuring security. We will just briefly look at SET a few of the features and there are some systems. See here these are all book entry systems like whatever you are carrying out they will go into the transaction book of some agency. There is another mechanism where the bearer or the consumer they get some kind of certification. Some kind of digital cash.

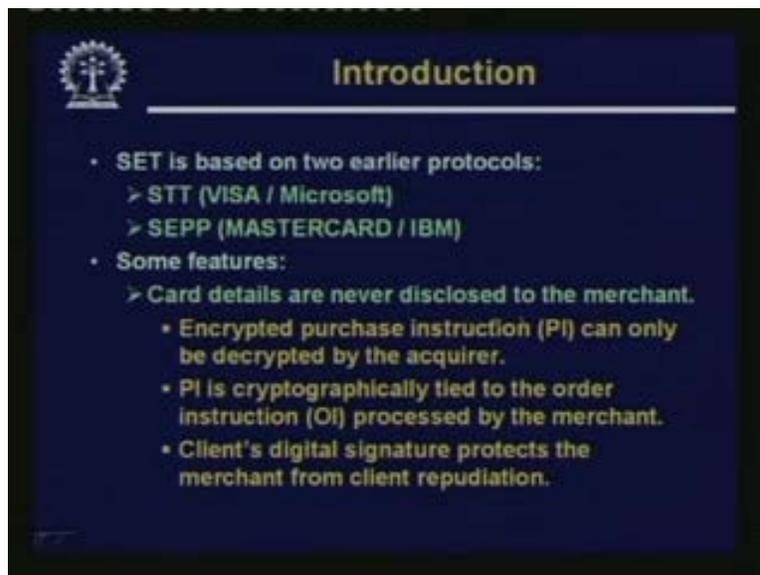
Well I am giving an example of digital cash. Digital cash is something like I carry out some money. In my purse I can make payments; in the same way I will carry my money electronically in some cards. Those cards I can present in some recognized shopping outlets and from there they can debit amount from my card and give it back. So that card is as good as a debit card it is as good as money in that card. Debit card the concept is very similar. It is something like digital cash. So here some kind of certification system identifies the bearer digicash is one such system.

(Refer Slide Time: 55:31)



Now very quickly we will look some of the features of the secure electronic transaction SET.

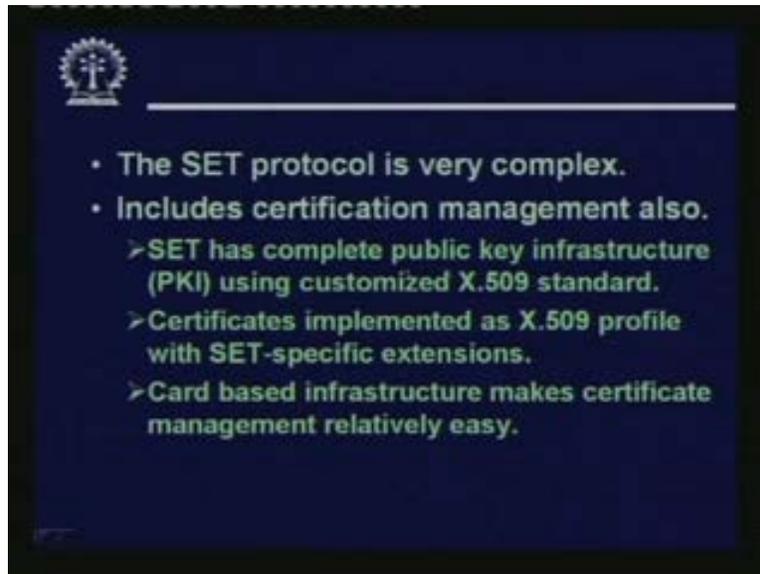
(Refer Slide Time: 55:39)



Actually is a set of protocols as I have said based on two earlier protocols. One STT which was used by VISA, Microsoft and SEPP which was used by MASTERCARD IBM. Some features are as follows. The card details are never disclosed to the merchant. Encrypted purchase instruction PI can only be decrypted by the acquirer. The purchase instruction is cryptographically tied to the order instruction. Client's digital signature protects the merchant from client repudiation. So there is protection in all aspects protecting the client protecting the server protecting the credit card number protecting the integrity of a transaction. There are a lot

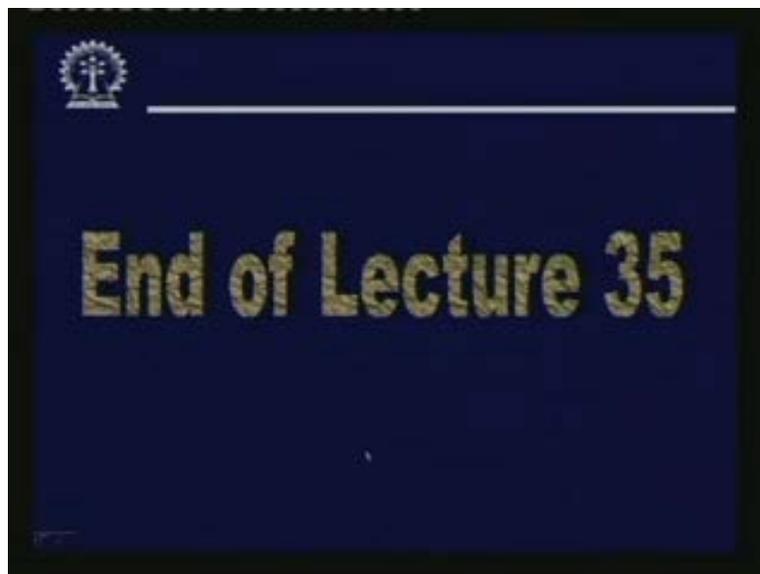
of things involved inside.

(Refer Slide Time: 56:29)



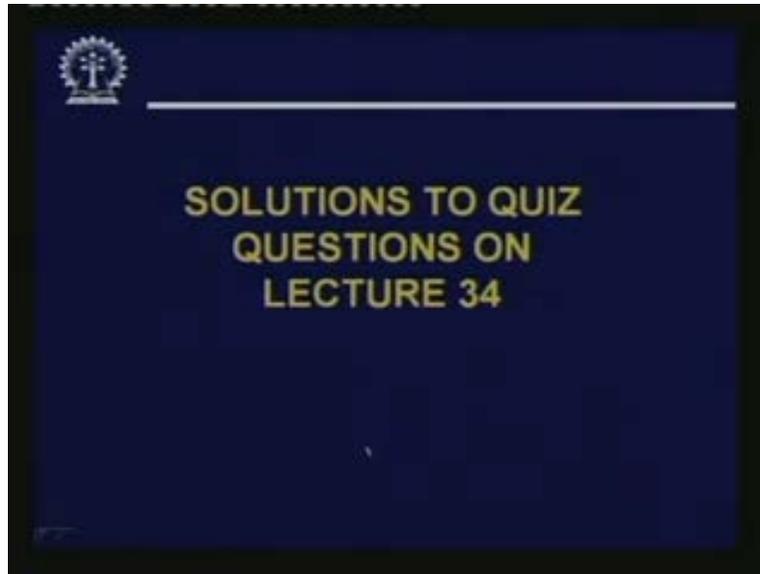
In fact the SET protocol is very complex. This includes certification management also. We will talk about certificate management later. Certificate management is a mechanism with which you can get the public key of an agency through a certified authority. There is some standard X.509. So in SET this implementation exists and card based infrastructure. This also makes management of the certificates relatively easy.

(Refer Slide Time: 57:05)

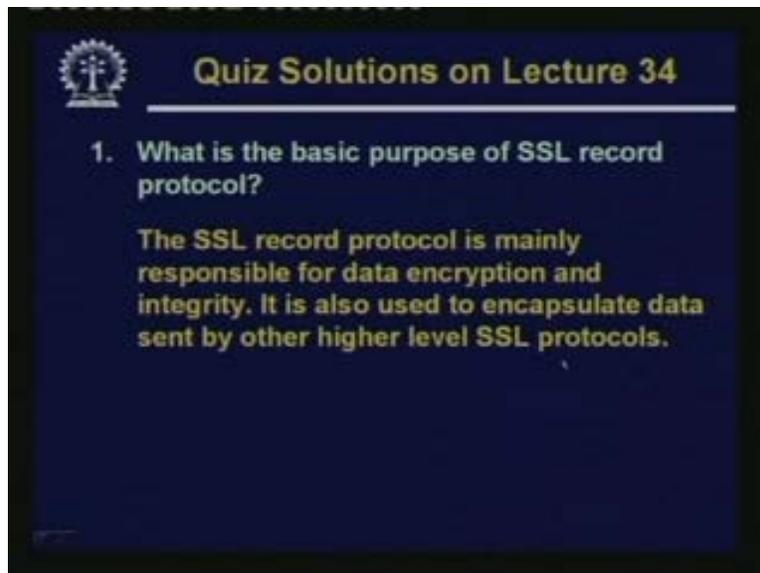


So with this we come to the end of this particular lecture. We quickly look at some of the answers to the quiz questions we had post in our last class.

(Refer Slide Time: 57:12)



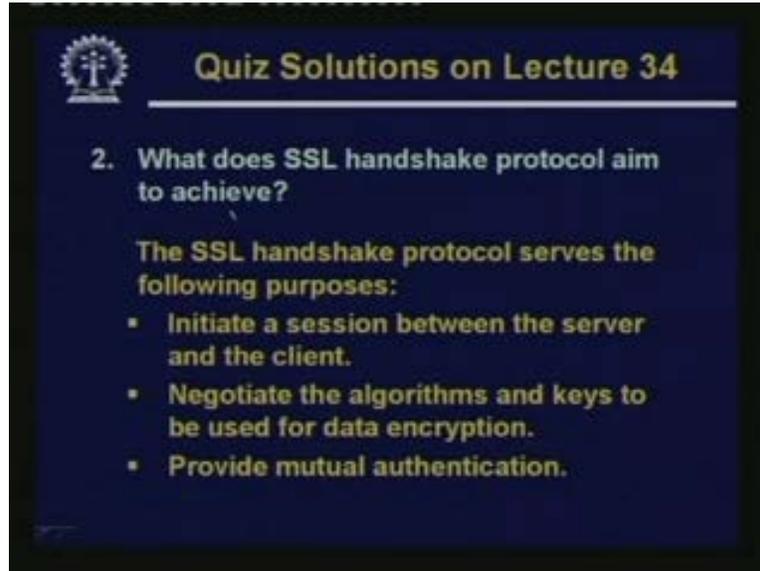
(Refer Slide Time: 57:14)



What is the basic purpose of SSL record protocol?

The SSL record protocol is mainly responsible for data encryption and integrity. It is also used to encapsulate data sent by other higher level SSL protocols. That is the basic purpose of SSL record protocol.

(Refer Slide Time: 57:35)



The slide features a dark blue background with a white logo in the top left corner. The title "Quiz Solutions on Lecture 34" is written in yellow at the top. Below the title, a question is posed in white text. The answer is provided in yellow text, including a list of three bullet points.

Quiz Solutions on Lecture 34

2. What does SSL handshake protocol aim to achieve?

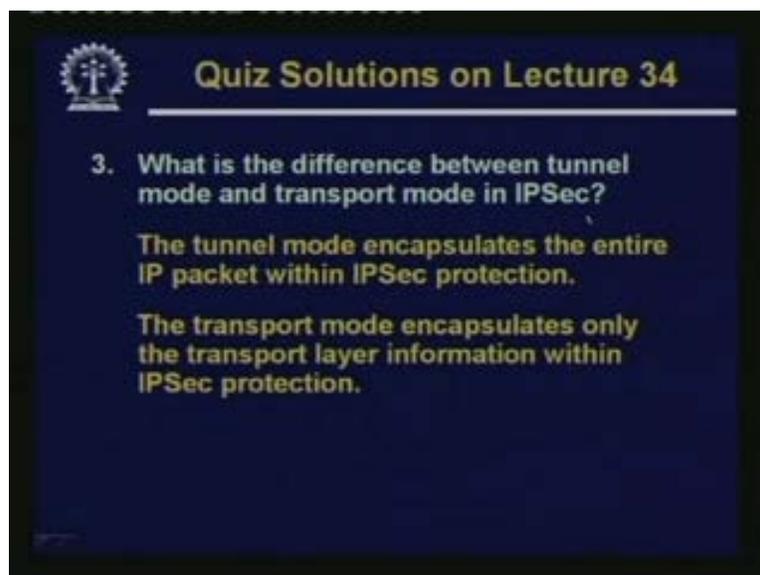
The SSL handshake protocol serves the following purposes:

- Initiate a session between the server and the client.
- Negotiate the algorithms and keys to be used for data encryption.
- Provide mutual authentication.

What does SSL handshake protocol aim to achieve?

It aims to achieve these three things. Initiate a session between the server and the client, negotiates the algorithms and keys to be used for data encryption and thirdly prove mutual authentication.

(Refer Slide Time: 57:56)



The slide features a dark blue background with a white logo in the top left corner. The title "Quiz Solutions on Lecture 34" is written in yellow at the top. Below the title, a question is posed in white text. The answer is provided in yellow text, including two paragraphs.

Quiz Solutions on Lecture 34

3. What is the difference between tunnel mode and transport mode in IPSec?

The tunnel mode encapsulates the entire IP packet within IPSec protection.

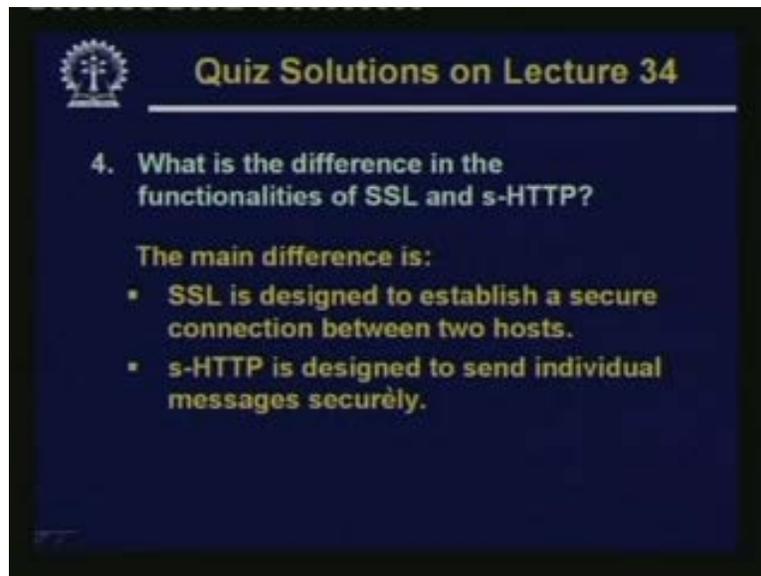
The transport mode encapsulates only the transport layer information within IPSec protection.

What is the difference between tunnel mode and transport mode in IPSec?

Well in the tunnel mode encapsulation of the entire IP packet is carried out within IPSec protection. Whereas in transport mode encapsulation of only the transport layer information is

done. The headers of IP are not encrypted.

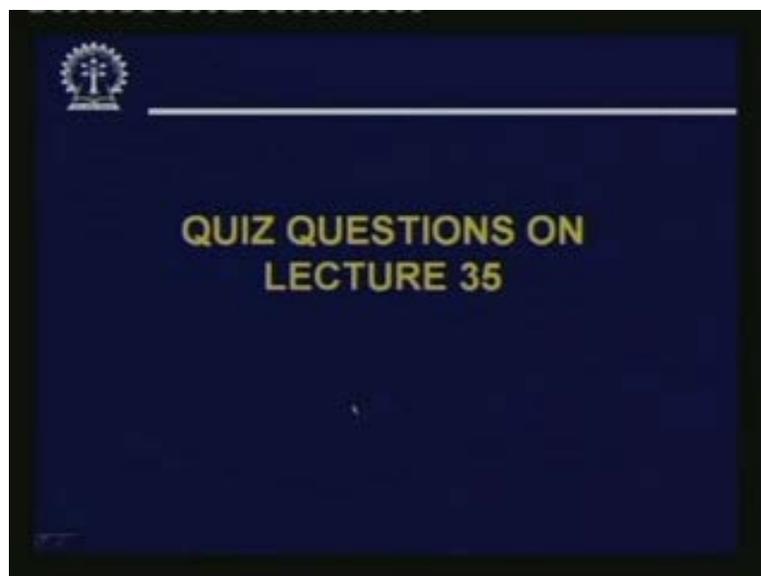
(Refer Slide Time: 58:22)



What is the difference in the functionalities of SSL and s-HTTP?

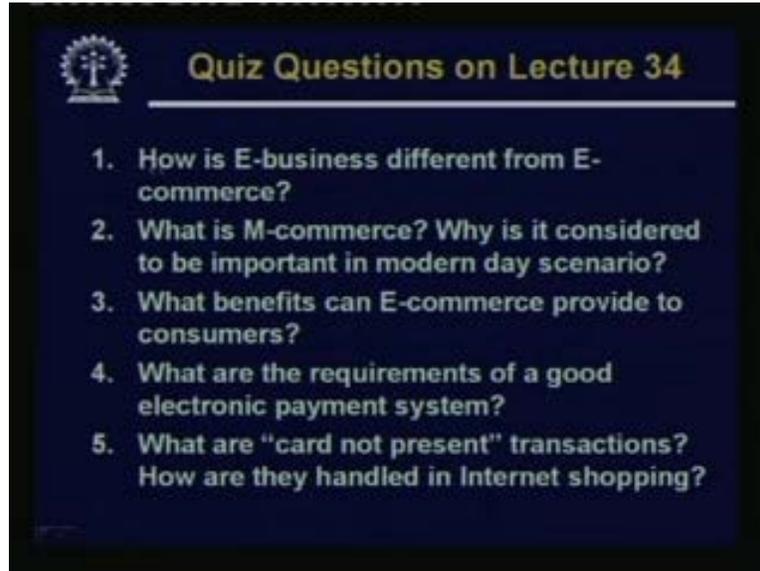
The main difference is SSL is designed to establish a secure connection between two hosts. All packet transmissions subsequently will be secure. But in s-HTTP it is used to design or to send individual messages securely. So it only helps in securing individual packets or messages not the whole session. All messages flowing during the session.

(Refer Slide Time: 58:56)



So, some questions from today's class.

(Refer Slide Time: 58:56)



How is E-business different from E-commerce?

What is M-commerce?

Why is it considered to be important in modern day scenario?

What benefits can E-commerce provide to consumers?

What are the requirements of a good electronic payment system?

What are card not present transactions how are they handled in internet shopping?

So with this we come to the end of this lecture. Thank you.