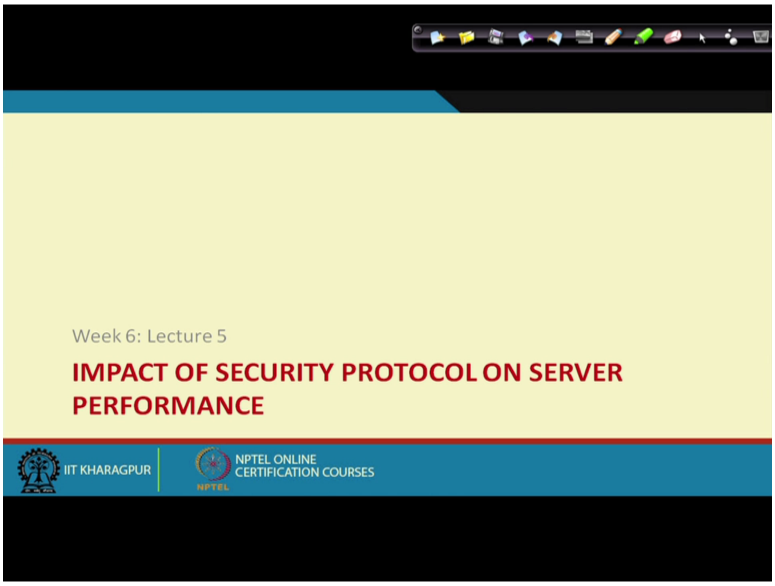
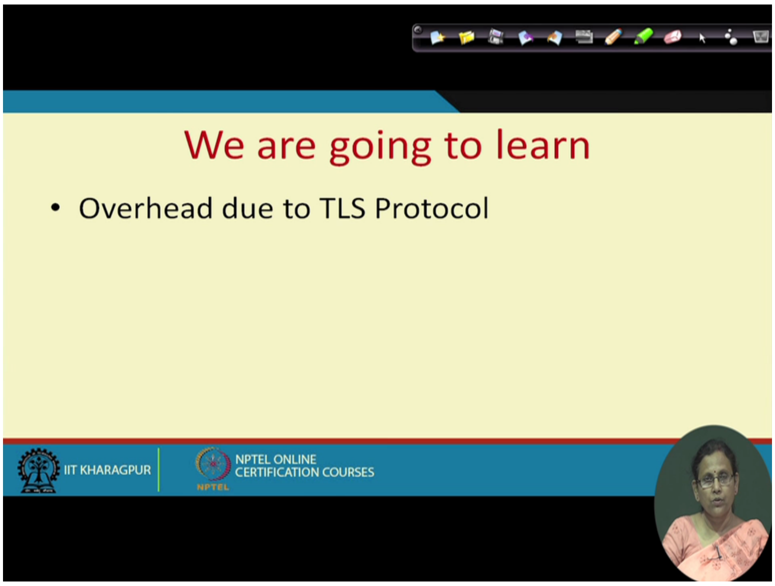
Course on E-Business
By Prof. Mamata Jenamani
Department of Industrial and Systems Engineering
Indian Institute of Technology Kharagpur
Lecture 32 Impact of Security Protocol On Server Performance

So we continue our discussion on the impact of the security protocol the security protocol just now we studied is TLS Protocol in the last lecture we studied is TLS protocol what is its impact on server performance so I would like to let you know that if you are going through this lecture it is essential that you have covered the previous lecture so otherwise it will be difficult to follow this one because here simply we are considering one numeric example.

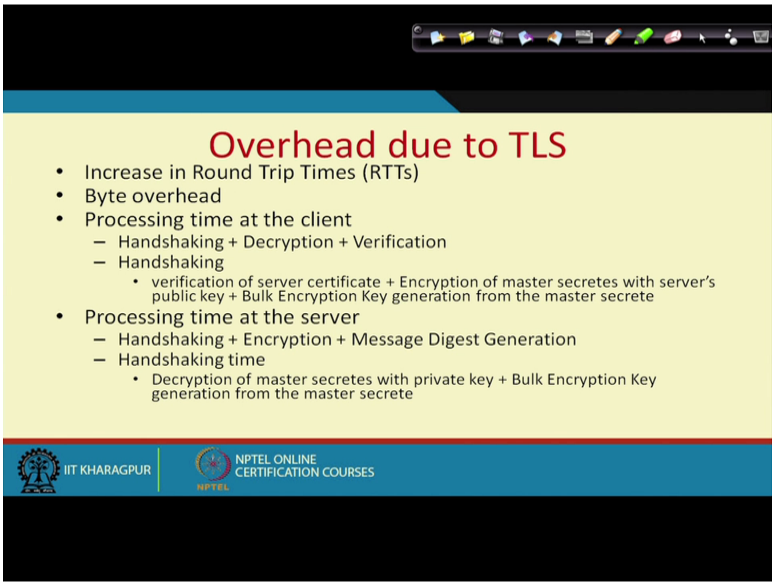
(Refer Slide Time: 0:54)





So let us look what is the overhead due to TLS protocol through one example will be understanding various situations situations and to see that whether we should be actually encrypting the entire site or encrypting a part of the site or will be using some kind of hardware for this encryption process and what is the impact of taking doing all this through all the trying all these combination of finding out the most beneficial way of implementing the security Protocol in your E business site.

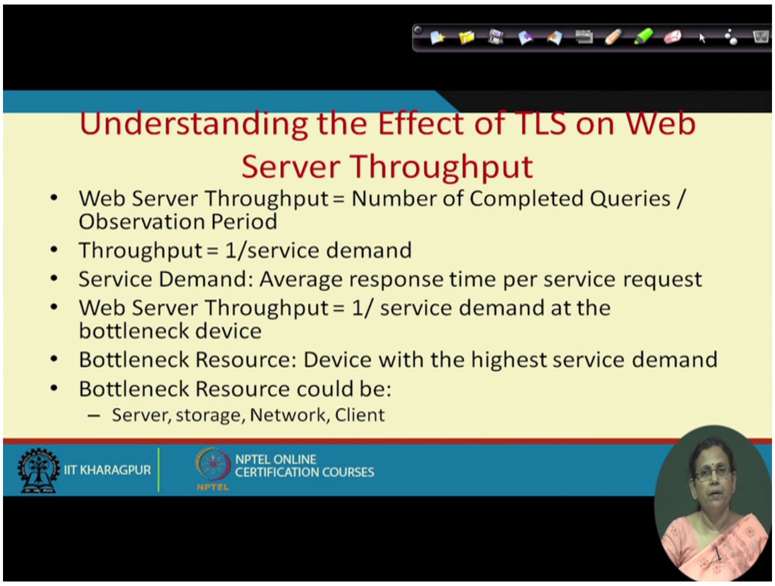
(Refer Slide Time: 1:45)



So let us try to go through this example as we have told you this TLS protocol actually increases the overhead so this increasing round tip trip time is it happen due to the transfer the multiple time handshake the handshake that the data before the actual data actually sent many other data elements are sent and some kind of cryptographic algorithms are carried out so last class we discussed what are the processing time involved at client.

And server end this includes handshaking time plus bulk data transfer time during handshake both and client and server do different kinds of operation during record protocol which is for bulk data transfer server encrypts it and the client decrypts it to read that.

(Refer Slide Time: 2:51)



So let us now see one example what is the effect of this TLS protocol on web server throughput? So while talking about this web server (())(3:01) performance wwe have understood that E in a E commerce setting if your server does not perform well if the response time is too slow then people will not be staying in your server they will be immediately moving to some other place.

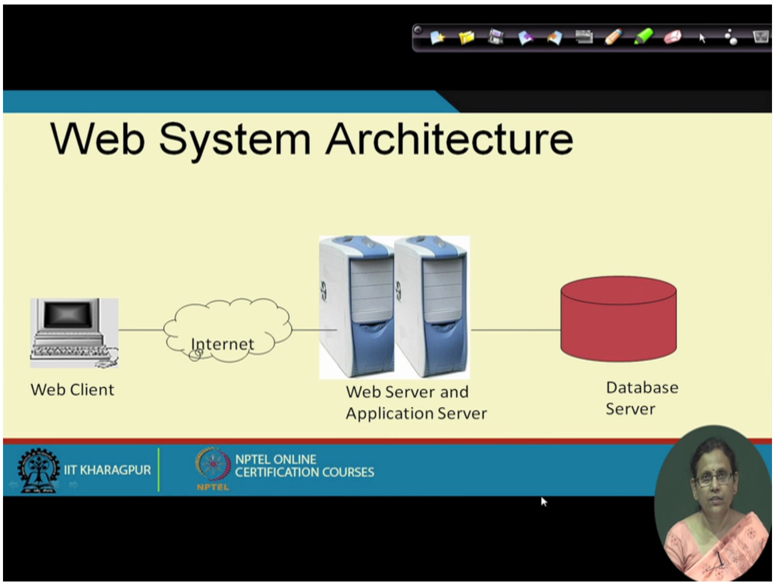
So therefore I would like to see what is the impact of such security protocol on server throughput so now look at the the definition of a how let us have a numeric value to compute the server throughput. The server throughput is equal to the number of completed queries per observation period number of completed queries you mean the number of pages the number of page request sent to the server.

And response sent back by the server so this is about the number of responses send back by the server so this your server throughput so this throughput is equal to one upon the surface demand by the clients where the service demand is the average response time for service request so web server throughput is equal to one upon service demand at the bottleneck device.

So here I would like to remind you about your web system architecture so to understand the concept of bottleneck device.

Bottleneck resource let us try to understand what is the web system architecture? In fact we have already studied about this web system architecture in in the previous one of the previous lectures.

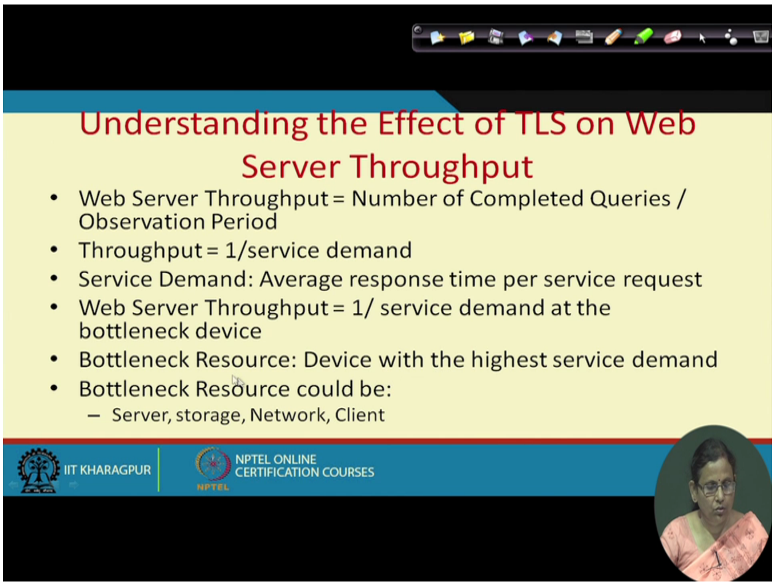
(Refer Slide Time: 5:10)



Just to remind you once again I show you about the web server architecture. When the client connects to the server 3 things are now involved one is web server which interns connects to the application server and application server connects to the data base server so it is data base server application server and web server and sometimes this web server and application server will be content with in the web server.

And data base server might be different or sometimes in fact the umm all the time this will be a logically different entity and probably physically different as well here also they are logically separate entities and sometimes they can be physically separate as well.

(Refer Slide Time: 6:04)

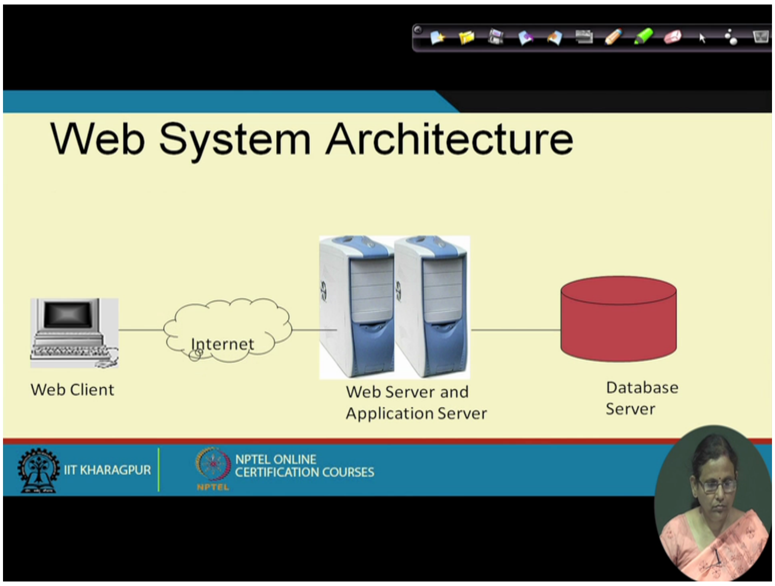


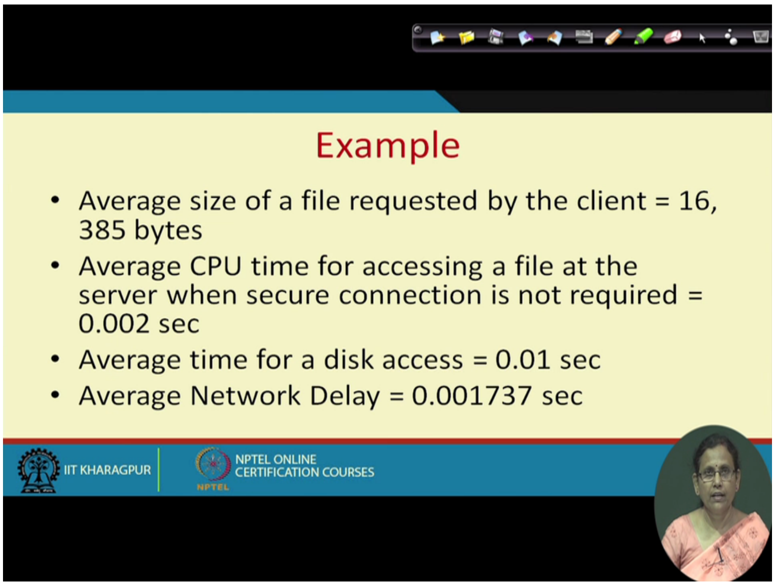
So out of those resources we will be like to find out where is the bottleneck and in earlier literature also I have told you when there is a slow response time experienced by the client it may be due to the fact that the client machine itself is the slow the network the service provider through which the client connect it may be slow then the network over which the packets are going the network might be congested.

And might be taking time then ISP the Internet service provider at the end of the server may be not be performing well and finally the server so server intern connects to database so all this entities who are involved in this wave transaction are responsible for slow response time during web transaction so therefore if we adopt the security measure we have to find out who is now the bottleneck device.

Now which is the which is the bottleneck device the bottleneck device is the one with highest service demand what is highest service demand maximum time is taken at the bottleneck device even if the other devices perform well because of the bottleneck device the system will be slow .

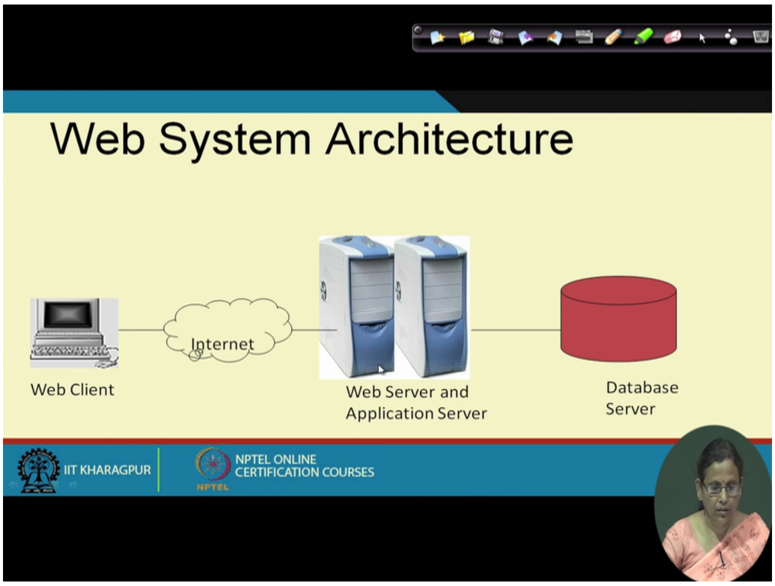
(Refer Slide Time: 7:45)





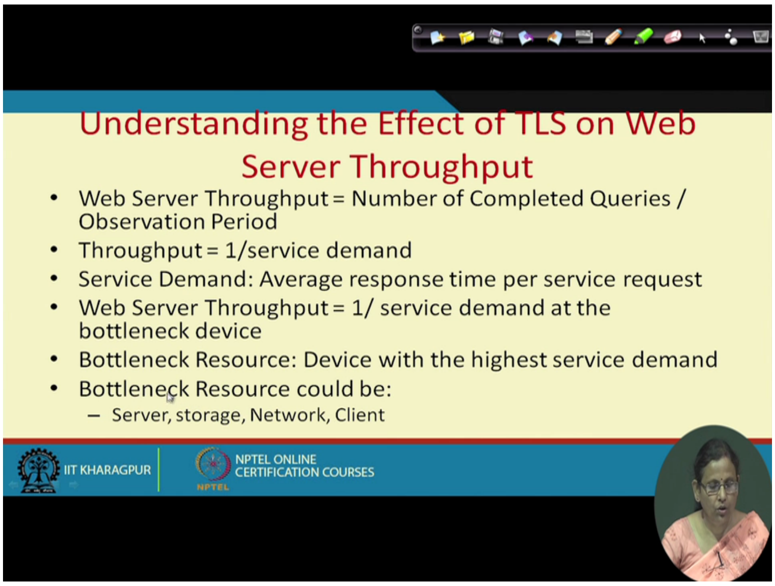
So let us look at this example suppose you are trying to send the files and the average file size requested by the client is some bytes then average CPU time for accessing the file at the server when the secure connection is not there it is this much then average time to for for a disk access is point 01 second then average network delay is given here point 001737 second. Now this is because when the packet get transferred over the network this is the for the disk access disk access time means.

(Refer Slide Time: 8:32)



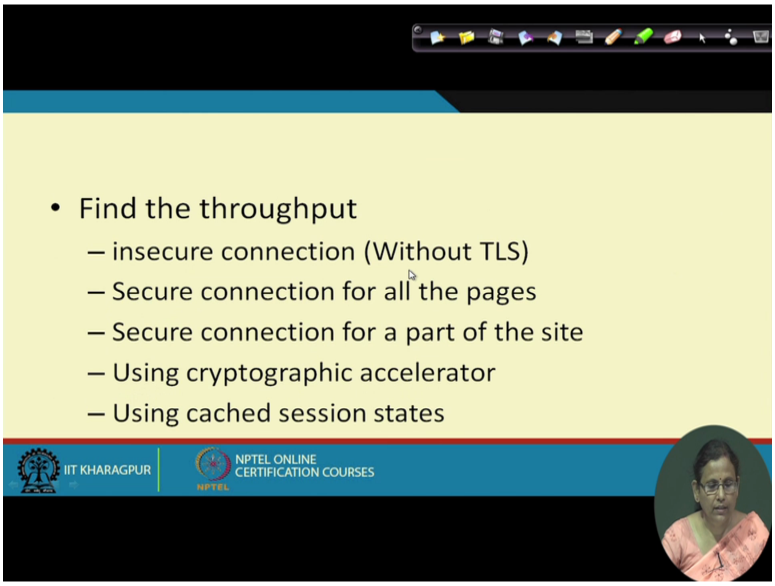
From web server when you access the database server that is a disk access time.

(Refer Slide Time: 8:43)



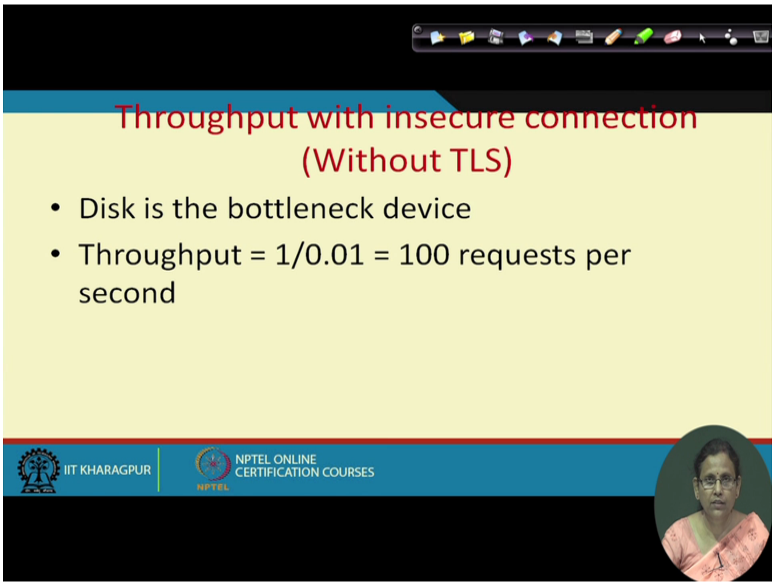
So your bottleneck device can be storage network client and this thing and here the network delay disk access delay and then CPU time for accessing a file at the server when it is not going through the storage it is this much and this is the file size.

(Refer Slide Time: 9:07)



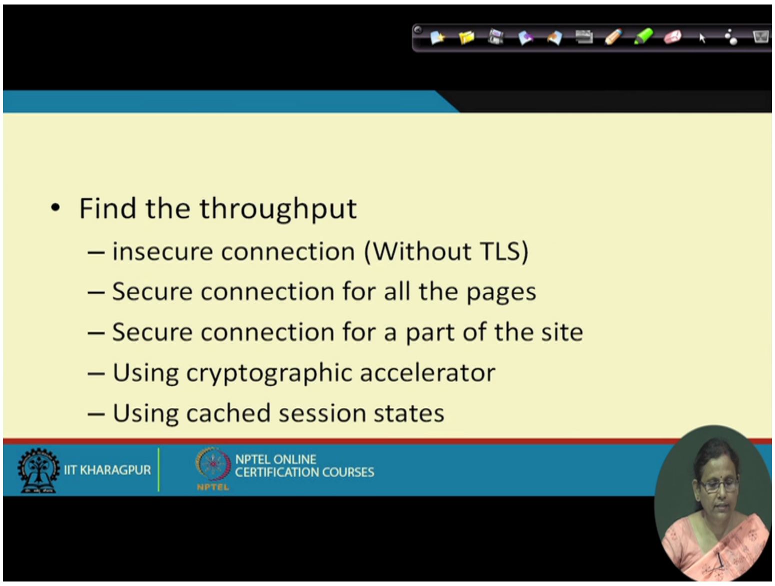
Now look at our aim is to find out what is the servers performance when there is performance in terms of throughput when there is insecure connection there is no TLS when all the pages are secured then the secure connection for a part of the site and using some cryptographic accelerator which is a some kind of hardware device and using the cached session states so how it is going to affect the servers performance that we are going to see.

(Refer Slide Time: 9:37)



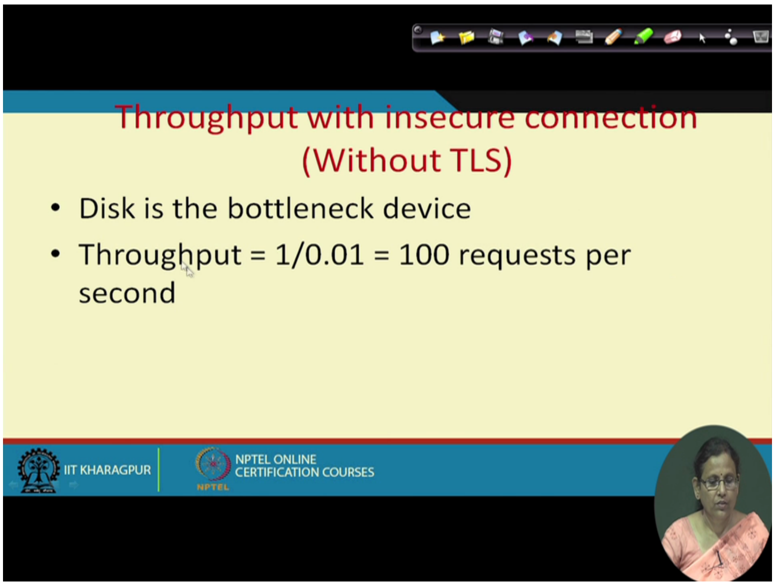
Then throughput with insecure connection.

(Refer Slide Time: 9:43)



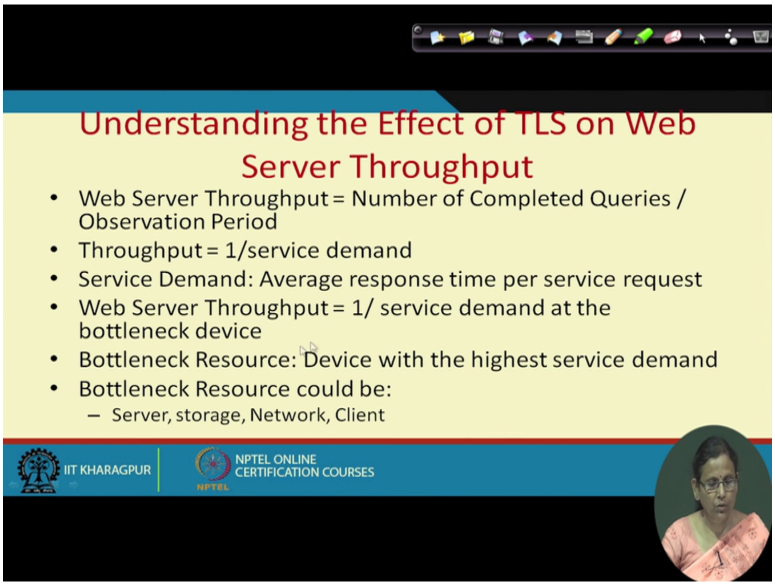
If you look at this data this data which device takes more time it is the disk so disk is the bottleneck device in when the system is insecure then the TLS protocol is not implemented.

(Refer Slide Time: 10:02)



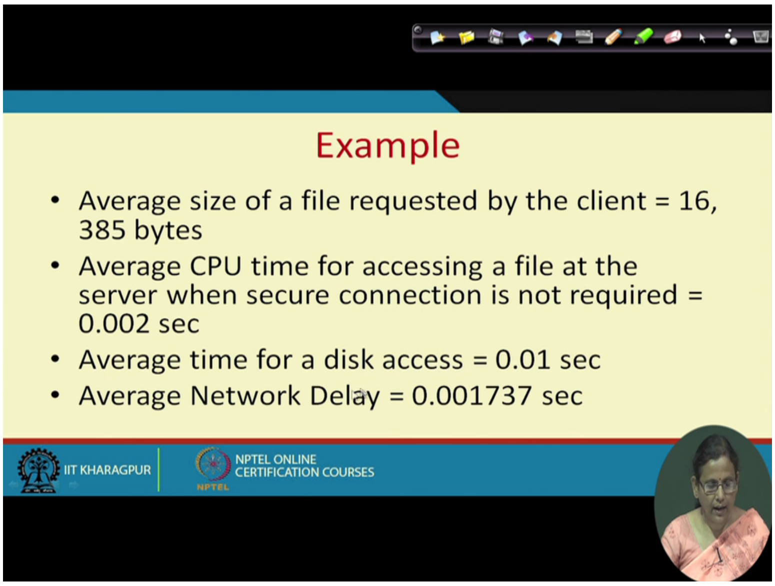
So what is our throughput? Throughput formula was one upon the bottleneck.

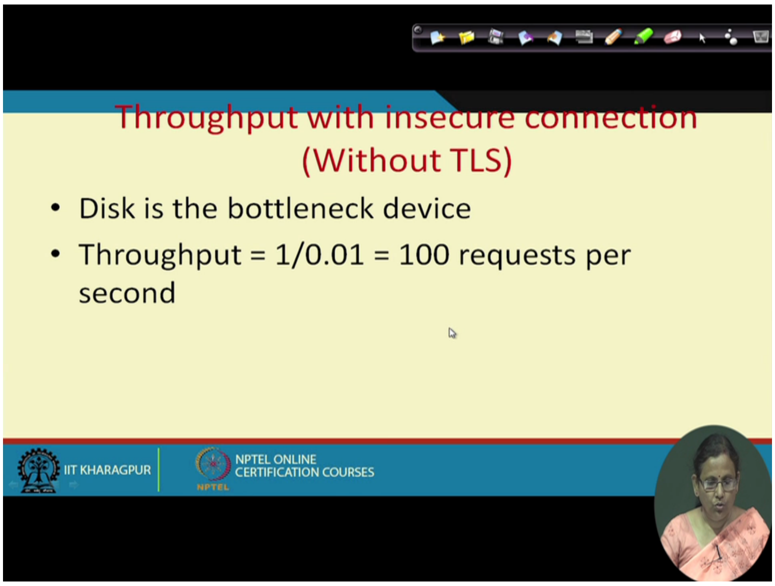
(Refer Slide Time: 10:10)



Let us look at the throughput Formula this web server throughput was 1upon service demand at the bottleneck ser bottleneck device and what is service demand? Average response time per service request so average response time per service request for this particular example.

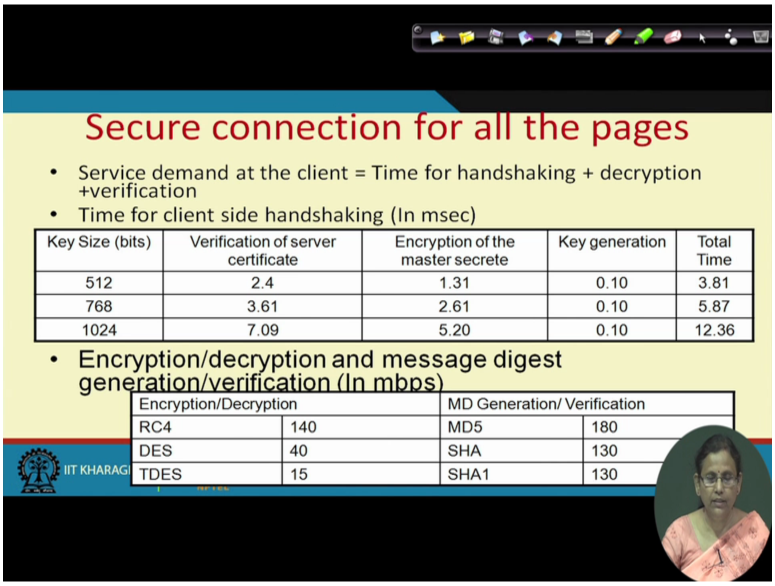
(Refer Slide Time: 10:29)





Was the highest in case of this disk? So therefore the throughput is 100 request per second it cannot go beyond this now let us see if TLS is implemented in the whole site what is the situation?

(Refer Slide Time: 10:46)



If the TLS is implemented besides bulk encryption some handshaking also takes place so the it is the time for handshaking and for decryption and verification that of course there is one step called verification to verify whether the content has been modified in between or not now lets say.

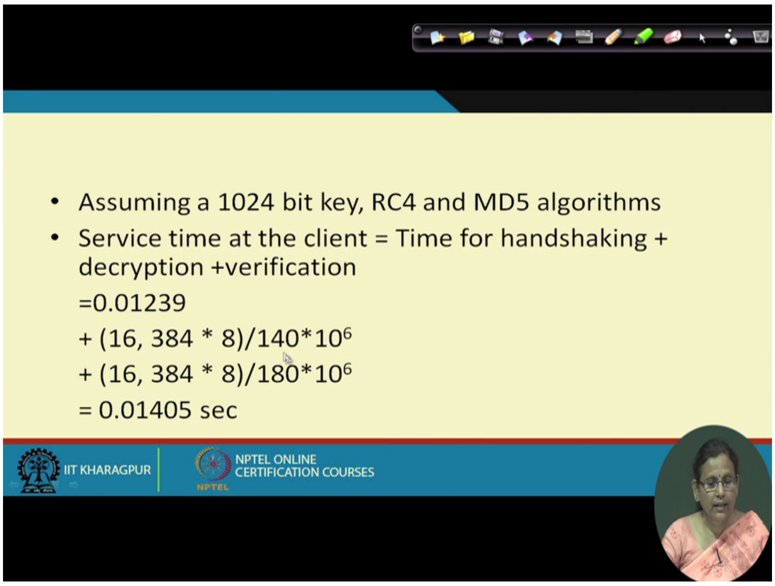
And as I have told you already in the one of the previous classes the time actually increases with that of the key size now suppose for the time for handshaking is when the key size is

512, 768, 1024 the verification time for server certificate are this much then the encryption of the master secret try to remember what we studied during during this handshaking procedure TLS handshaking procedure.

There was exchange of server certificate there was exchange there was generation of this master key at both I mean there there was encryption and decryption of the master secret and there was time for key generation so including all this times the total time for the client side handshake has been this as you can see how the time increases with the key size then once this is done then the encryption.

And decryption of the message digest at both the ends has to be done because the data has to be sent with along with that message digest so for encryption and decryption it is this is the time and I mean this is in terms of megabits per second so this much of this much of bits get generated at both the ends during this encryption decryption and message digest generation process.

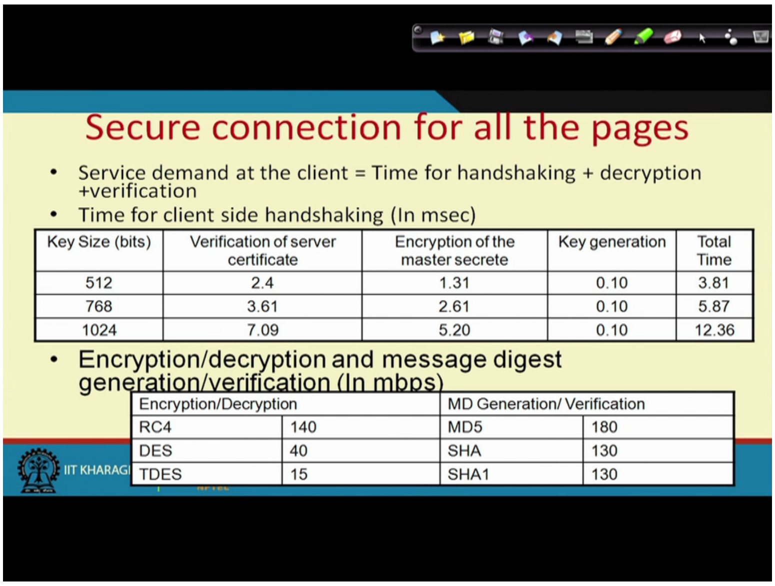
(Refer Slide Time: 13:22)



Then this is the values for various key sizes assuming that you have a 1024 bit key RC4 and MD5 algorithm here we are using for encryption decryption three options available RC4 DES and TDS these are what these are the these are what? These are actually the bulk encryption see during handshaking (())(13:51) takes place aft your key gets generated by sharing some secrets.

Since after the key gets generated using that key the bulk data transfer has to takes place so for that bulk data transfer.

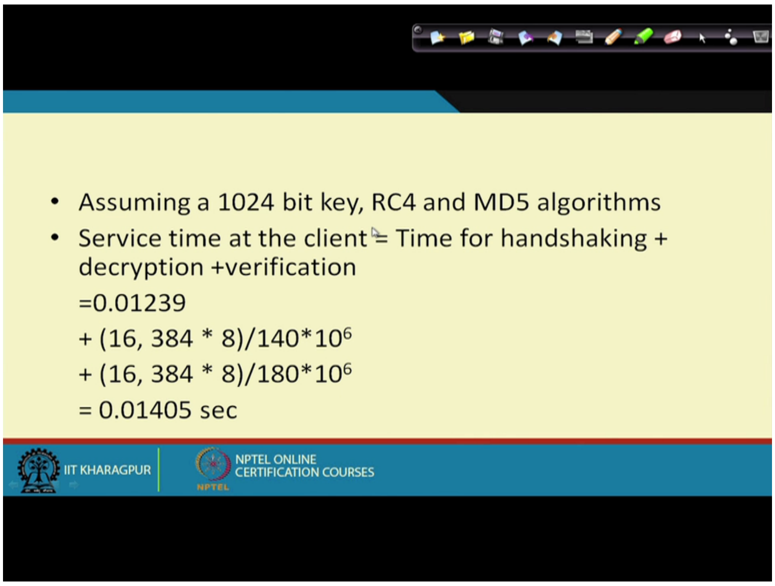
(Refer Slide Time: 14:11)



Some encryption decryption algorithm has to be used so 3 options are given here look during handshaking procedure which algorithm will be chosen is decided. Similarly for message digest generation and verification why it is done this (())(14:26) this MD5 SHA , SHA 1 they are all hatching algorithm what for their use they are used for not what is the mean what is the use of this hatch function?

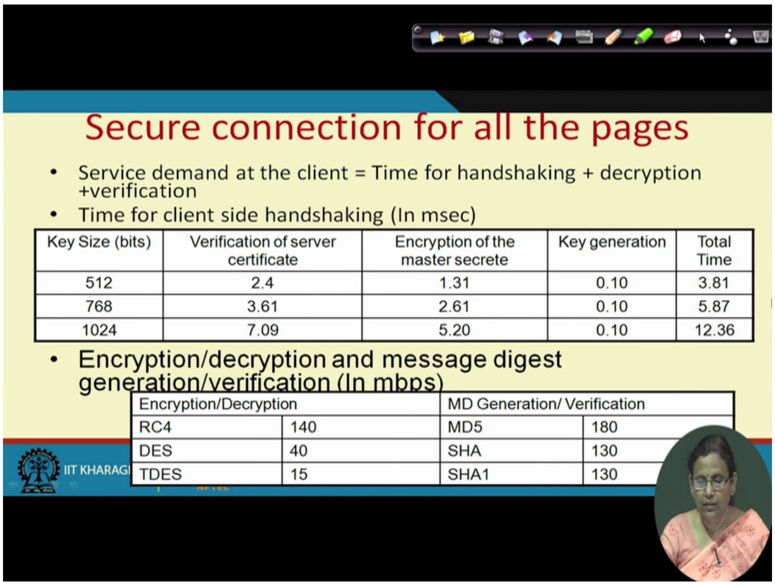
Hatch function helps in umm authentication non repudation and the data integrating so it whether the right data has during this procedure the encrypted data which has come whether the right data has come or the encrypted data on its way has got modified that has to be checked so again some hatching is used so there are three options were available so with this three options based on the negotiated algorithm for encryption decryption.

(Refer Slide Time: 15:20)



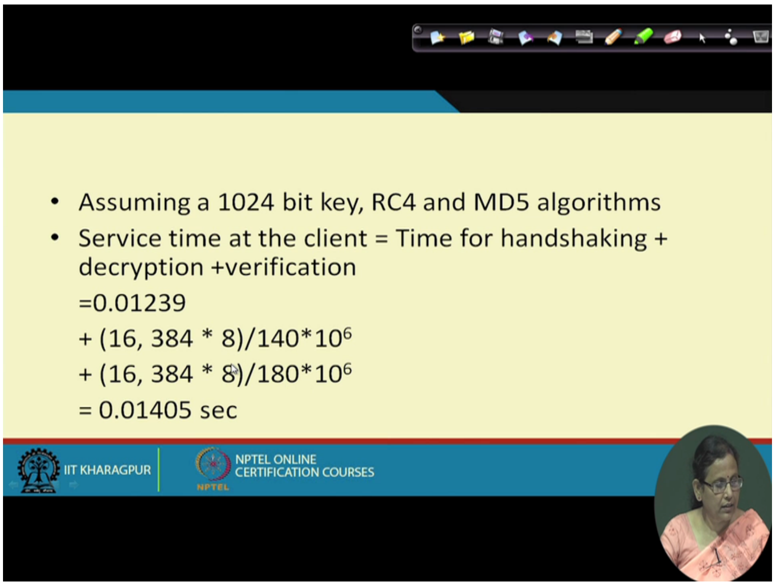
And hatching assuming that RC4 for encryption and MD5 for hatching is used the total service time at the client is equal to time for hand shaking plus time for a decryption. Decryption of the data which is sent by the server after the server is authenticated during handshaking procedure. So this total time is actually the time for handshaking.

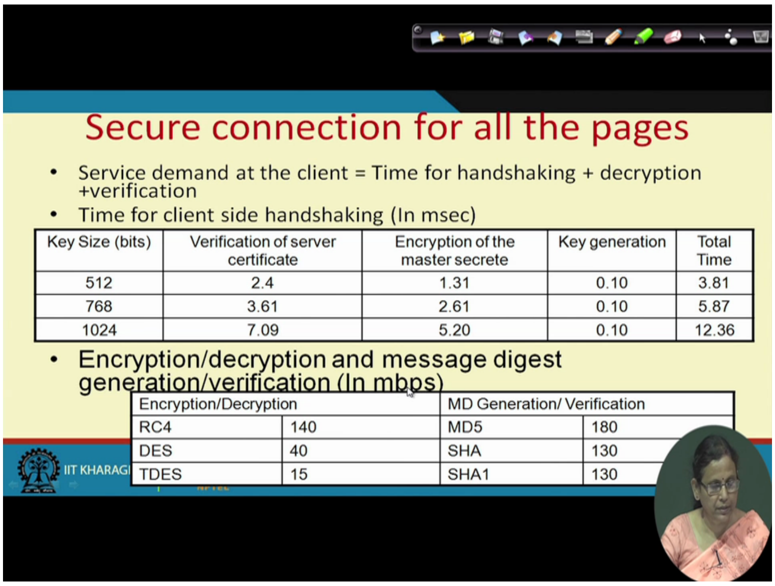
(Refer Slide Time: 15:51)



This time time was in in milli second.

(Refer Slide Time: 15:57)





Throughput with insecure connection (Without TLS)

- Disk is the bottleneck device
- Throughput = 1/0.01 = 100 requests per second

Understanding the Effect of TLS on Web Server Throughput

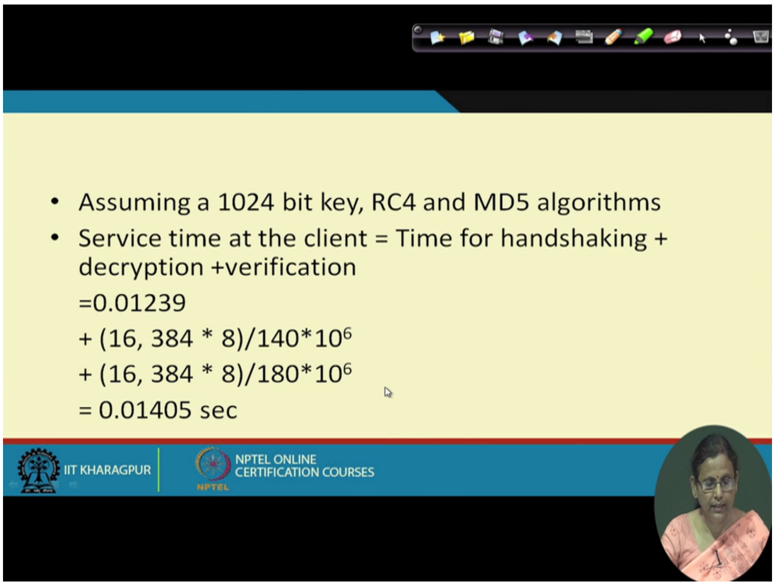
- Web Server Throughput = Number of Completed Queries / Observation Period
- Throughput = 1/service demand
- Service Demand: Average response time per service request
- Web Server Throughput = 1/ service demand at the bottleneck device
- Bottleneck Resource: Device with the highest service demand
- Bottleneck Resource could be:
  - Server, storage, Network, Client

Example

- Average size of a file requested by the client = 16, 385 bytes
- Average CPU time for accessing a file at the server when secure connection is not required = 0.002 sec
- Average time for a disk access = 0.01 sec
- Average Network Delay = 0.001737 sec

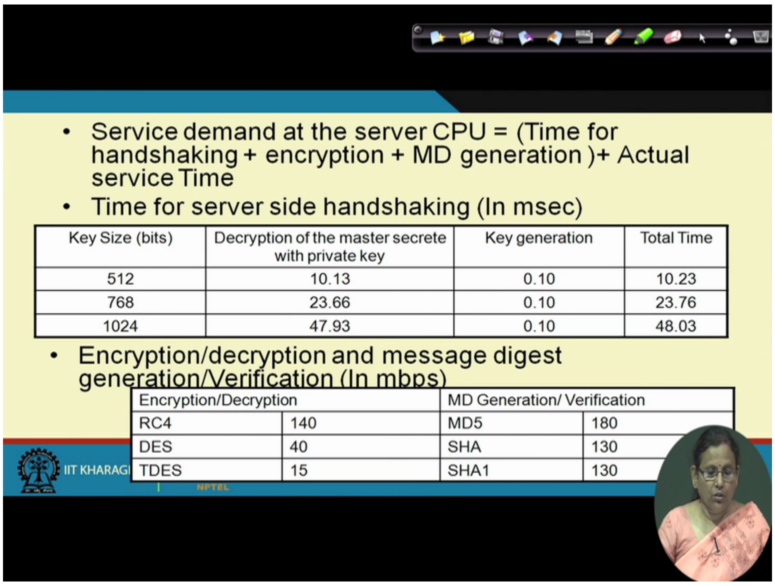
Then the other one the this one was the conversion rate in terms of mbps and total file size average file size that we discussed here was average file size is was this much of bit 16,385 bytes so that byte now need to be converted to during the message digest generation so this is this was in bytes so number of bits it was converted.

(Refer Slide Time: 16:28)



And it was megabytes per second so that is how the total time turns out to be this much this are simple calculation you can do it yourself and this much time gets this thing.

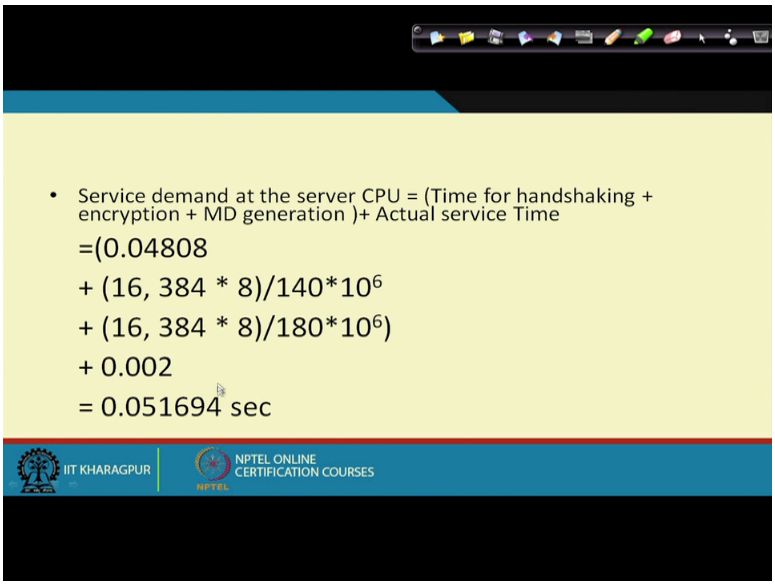
(Refer Slide Time: 16:38)



Now at the server side again similar operations happen and during this handshaking I am not going to the details but here again you the there is a decryption of the master secret which with its own private key and we have one of the earlier lecturers I have told you this private key operations are bit costly so more time is taken by this key generation same time and this is the total time so assuming again that this 3 algorithm.

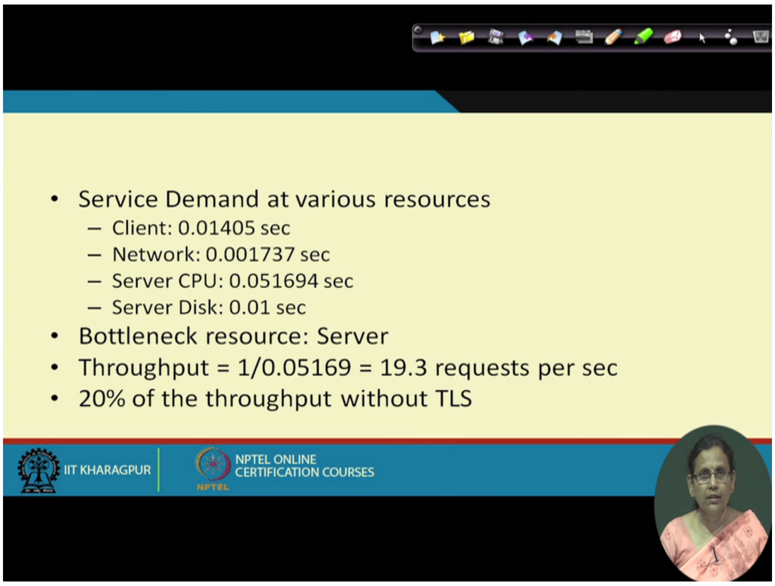
This 3 encryption algorithms and option for this three decryption algorithm sorry hatching functions are available and assuming that RC4 and MD5 are used and this is the time taken for hand shaking and 10 because that key that was used earlier the same size key will be using those assuming that is 1024 size key is used for hand shaking.

(Refer Slide Time: 17:39)



This is the calculation is again same now this is the total time so if this is the total time.

(Refer Slide Time: 17:49)

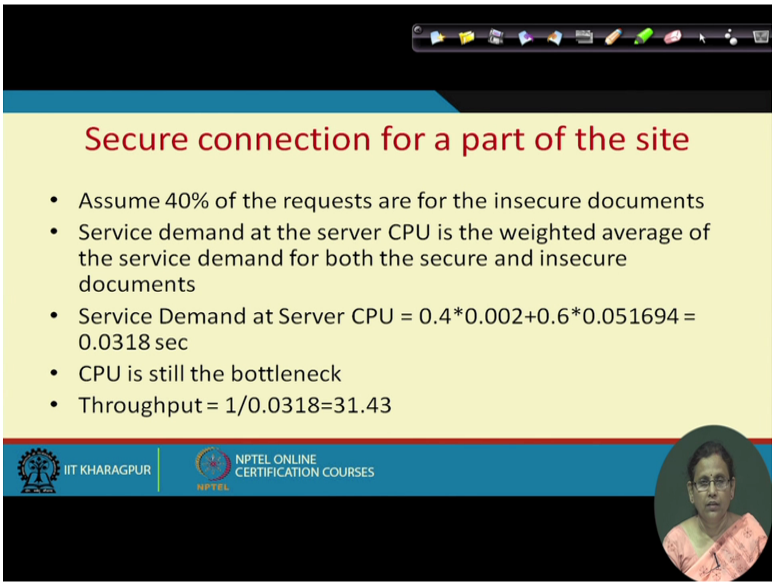


What becomes the bottleneck now servers disk time remain same clients time has increased network remains same this is now server time. So earlier when the server use to be the bottleneck device now client has here earlier when the disk for data access was used to be your bottleneck device now you are server has become bottleneck device and what is the decrease in throughput earlier it was hundred request per second.

Now it is 19.3 request per second so it is 20% of the throughput without TLS so so much slower it is now becoming so therefore it is advisable that the whole site need not be actually encrypted whole by whole side we means all the pages a particular website contains thousands of pages so instead of encrypting thousands of pages all of them because it is so costly and it will make your server response time go down so much your throughput will decrease so much.

So what you will be doing you may be may like to partially encrypt a part of the site so partially encrypt the site only the important pages will be now encrypted.

(Refer Slide Time: 19:36)

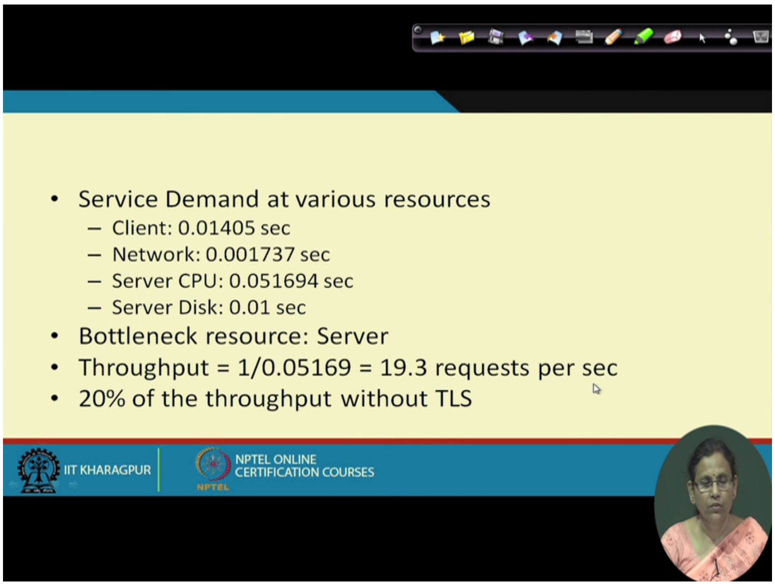


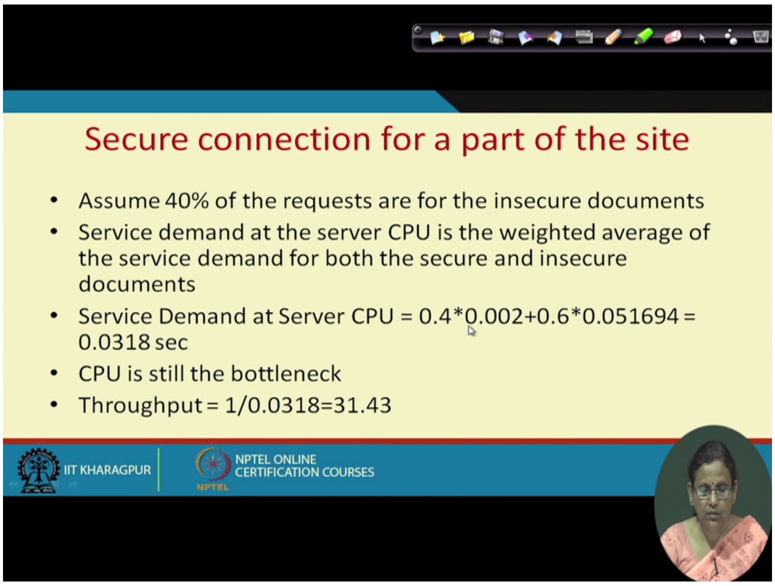
Okay, now a you come to a different scenario. Scenario is you assume that there is 40% of the request are for the insecure documents and the service demand at the CPU is the weighted average of the service demand for both secure and insecure documents so your 40% is for insecure document and 60 % is for secure document for insecure documents your disk was the bottleneck and for secure document your server was the bottleneck.

Now if you take a weighted average this average of this you still get the CPU I mean the you see your getting the weighted average at the server end this was already the servers throughput for the time taken at the server when the for the insecure document and this is for the secure document you are taking the weighted average of this now it is you find still this time is higher.

Than the disk access time which was point 01 so CPU or the server is still the bottleneck so therefore your throughput is one upon the bottlenecks his thing so it it turns out to be 31.43 pages per second. So from 100 pages 100 pages per second when you secure everything in your site you was able to send around some 19 what was exact number the 19.3 request per second you were able to serve.

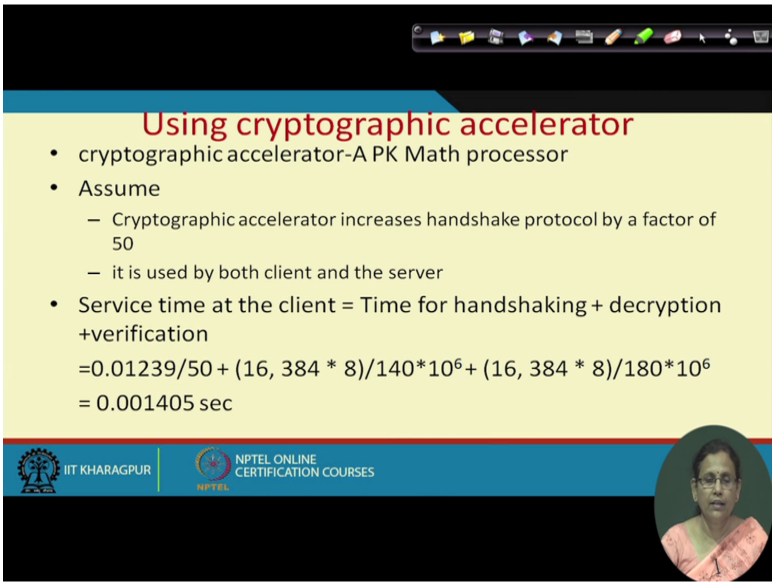
(Refer Slide Time: 21:36)





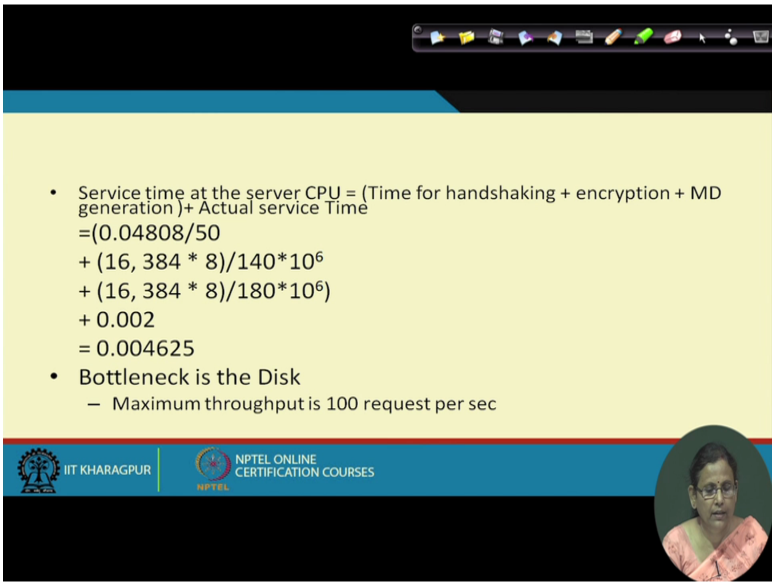
Now it has because you you did not make all your document secure only 60% of your documents are now secured it has now increased so much. So therefore while working in a while securing your website you should be very very careful that you should unnecessarily secure unnecessarily make arrangements for making all the files in your site secure because there will be some files which are public enough. And can be seen by everybody so it they=n need not go through the secure connection ok.

(Refer Slide Time: 22:18)



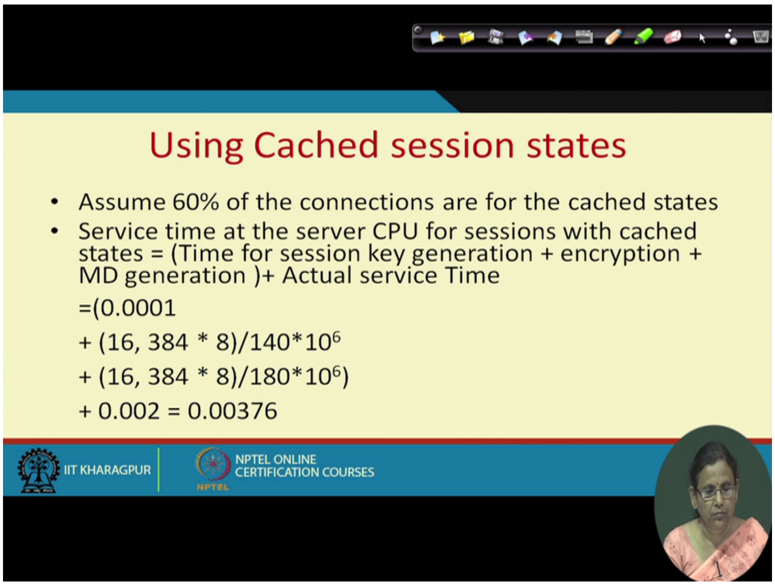
Now if you look at the use of a cryptographic accelerator which is a kind of math processor and assuming that it will increase the handset protocol by a factor of 50% and it is used by both client and server the service time at the client is this calculations are like earlier has now this much it has become now very fast.

(Refer Slide Time: 22:49)



Service time at the server CPU has also umm decreased then in the bottleneck now becomes the disk so by using hardware device for for calculating this doing the security operation you will your maximum throughput remains as it is. So therefore we can conclude that using hardware devices is a good option.

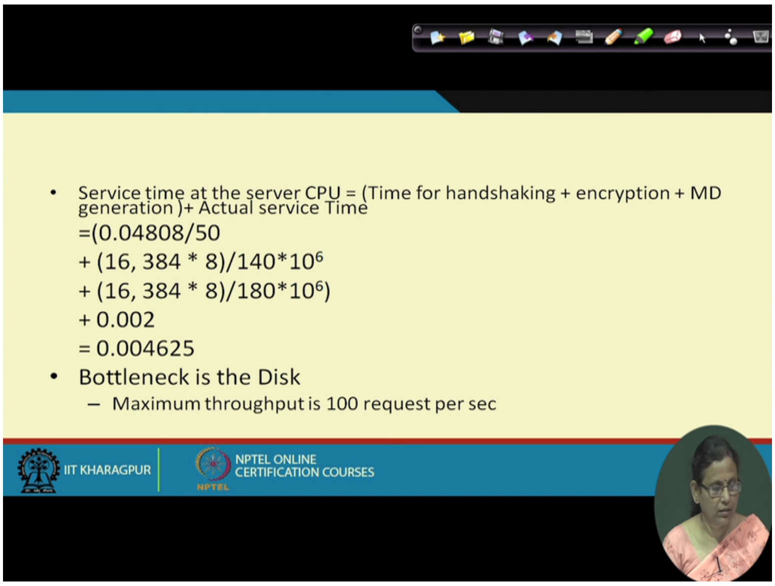
(Refer Slide Time: 23:28)

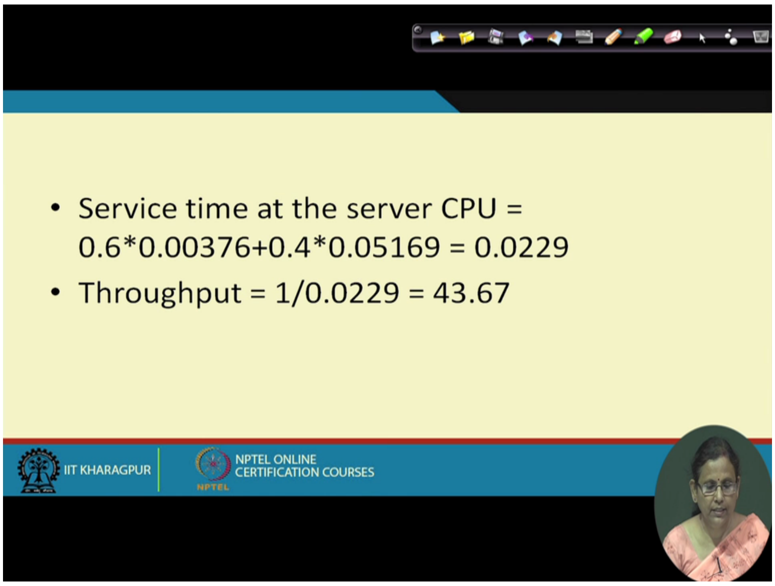


It will make your trans this thing faster than using the cached session state if we while discussing about our handshaking protocol last time we were showing that it actually you have to follow two path either you keep the session keys and session keys expired within a they they have a life and they expire and within when they are live you can actually use the session key.

So if you use session key assuming that 60% of connections are for the cached state you can increase the span of their life of this session keys so if assuming that 60% of connections are secured now the service time at the server is recomputed that is without that math processor you can do the computer since yourself and you can find that now the bottleneck.

(Refer Slide Time: 24:32)





You can now find that the service time at the server is now increased and it is higher than that of your disk so they are for the throughput is reduced so we can conclude that if you appropriately adjust the life of your session key then possibly you can have your throughput increased. So with this example we get the idea that how these the security protocols need to be managed so that your performance of the server is not hampered.

So much with this we finish this lecture thank you very much!