Congestion Control and Protected Broadcast of Data Using FTP and TELNET in a Cloud Network

[1]Kapil Vyas, [2]Tarun Shrimali
[1]PhD. Research Scholar, [2]Research Analyst
[1]Career Point University, Kota, Rajasthan, India
[2]JRN Vidyapeeth University, Udaipur Rajasthan
Email: [1]kapilnvyas@yahoo.com, [2]shrimalitarun@gmail.com

ABSTRACT

This paper presenting all security issue related to an open network. When two parties communicate in insecure environment that time all the private information is accessed by unauthorized user or client so, if a network have a proper security on all devices or secure private information and restricted unauthorized activity or access. The main aims of this paper enhance the security in network when two parties communicate or transfer the information. We need to work with many security techniques and ways by which we can prepare a secure network model for user authentication. The security architecture of network protocol widely accepted as being a good abstraction for network device and user security functionality. Significant work has been done to develop efficient techniques for network security, but most of the work has concentrated on securing protocol over congestion control. The base of work is providing security when network is distributed and based on cloud network. FTP and TELNET is enhancing security in network for user authentication and secure the entire device when two or more nodes communicate. The design method is referred to as network security design depend on protocol. Protocol security allows us to make better secure of network and all network devices by FTP and TELNET security protocol. This technique restricts unauthorized user or unwanted activity by third party.

General Terms

Secure term, congestion Control, Secure Channel, Encryption, FTP,TELNET

Keywords

Congestion Control Protected Broadcast, FTP, TELNET, Cloud Network, Securing Cloud network

1. INTRODUCTION

1.1. Secure Transmission

Secure Transmission is referring of the transfer of data as secret or proprietary data over a securing channel. This method requires a type of Encryption. The common E-mail Encryption is known as PKI. Secure Transmission is preventing attacks like ARP spoofing and Data loss. Other infrastructure (like Banks) relay on secure transmission protocol to prevent a catastrophic breach of security. Software and Hardware is attempt to identify and check the unconstitutional conduction of information from the system to an organization on the outside refer to as ILDP (information leak detection and prevention), ILP (Information leak prevention) , CMF (Content Monitoring and Filtering) and Extrusion Prevention system is used in connection with other.

1.2. Secure Channel

A Secure channel is a way of transfer data of challenging to overhear and tamper and A Confidential Channel is a way of transfer data that is resistant to overhearing but not to required opposite to tampering and last is Authentic Channel is a way of transmit information that is protection over to tampering but no necessary resistant to overhearing.

1.3. Encryption

Encryption is the Technique of encoding message or information to prevent by the Eavesdroppers and Hackers is cannot read message or stolen data but the authorize person or client can read information. In the encryption the message (Also called plaintext) is encrypted using encryption algorithm convert in to unreadable format (also called Cipher text). This process is done using by encryption key, which specifies how the information is to be encoded. Any hacker that can see cipher text should not be able to determine about original message or information. When the information is received by the authorized client or parties he is able to decode the cipher text using a decryption algorithm. it generally requisite a secret decryption key that adversary do not have access . An encryption method is need a key generation algorithm to erratically or randomly produce keys.

2. CONGESTION CONTROL

Congestion Control is controlling mechanism that is used to adjust & control the web traffic entry into a communication network and avoids Congestive Collapse by an attempt to avoid oversubscription. It keeps the traffic burden below the level of capacity. It uses against flow control, which prevent sender from overwhelming the receiver. Congestion Control occurs when a node is carry so much data that is quality of service deteriorates. It includes typical effects queuing delay, packet loss or blocking new connection. The consequence is that latter two incremental increases in offer load also only to minimum increase in system throughput or real reduction in network throughput.

3. FILE TRANSFER PROTOCOL (FTP)

File Transfer Protocol is the customary network protocol use for transfer files from one client to another client or host-to-host using TCP network, like Internet.FTP is made for a Client-Server design and use separate control and data connection between the server and the client or client to server.FTP users can validate themselves using a clear text log-in protocol, with the help of username and password FTP client login, but can connect in secret if the server is configured to permit it. Secure communication server hide the username and password, and encrypt the contented, FTP is secured with SSL/TLS (FTPS).The first FTP client application was command line application developed before operating systems have GUI and still ship with Windows, Unix and Linux OS .Much of FTP client and automation utilities have develop for server, mobile device, desktop and hardware and hundreds of productivity application (web page editors).

4. TELNET

Telnet is a collection of connection used on the local Area Networks and Internet to provide bidirectional interactive text based communication using virtual terminal connection. Client data is interspersing in-group with Telnet manage information in an 8-bit byte tilting data connection over the TCP (Transmission Control Protocol).Telnet is a user dominion and an original TCP/IP protocol for access remote computers. By Telnet, an administrator or another client is access computer remotely. HTTP and FTP allow us on the web to request specific file by remote computer. with the help of Telnet, a regular user privileges have granted to desired application and information on the computer. Telnet is referring to the software implement the client side of the protocol. Telnet client applications are accessible for virtually for all computer platforms. Telnet is used like a verb its mean to create a new connection with the Telnet protocol with using command line client and programmatic crossing point.

5. CLOUD-BASED NETWORKING

The cloud is transforming IT transportation and make it regularly for purpose of business to accept and afford enterprise class apps,density, computing, storage with cost, constraint of network. cloud network is share many benefits of cloud IT service like rapid development, no new hardware to install, on updating new software, subscription pricing, scalability, rapid development, easy maintenance and access services any where using internet.Cloud network is used for build and manage secure or private network over the local network using global cloud infrastructure. In this network services and traditional network function include security, management, connectivity, control is push cloud and deliver the service. Cloud network is dividing in two categories.

6. THE NETWORK ACCESS SECURITY

6.1. Access control list

The Access control list is a computer file system or a list of permission attach with an object. ACL describe which system or client process is granted access of object with operation is allowed on object. ACL describe two types of security models

A. MAC filtering

MAC Filtering provides a security access control method for 48-bit address allocate for each network card use to access network. Each card have a unique MAC address using MAC filtering on the network permission and service denial to specific device by using blacklist and white list.

B. IPaddress blocking

IP address blocking avoids or checks the connection between server and website. It effectively bans unauthorized connection from the client using affected address from a website, server, mail and internet connection. It is also used to protect against Brute force attack and censorship.

C. Tunneling protocol

Tunneling protocol used by computer network when one deliver protocol summarizes another payload protocol. It carry payload over unsuited delivery network and provide secure path by unstructured network. It is different from layer protocol model like TCP/IP or OSI. The Tunneling protocol has two main parts such as payload and delivery protocol set. It uses data encryption for transport unconfident payload over internet provides VPN functionality.

A. SSL VPN (Secure Sockets Layer Virtual Private Network)

SSL VPN is a part of VPN and used with Web browser. It not required installing of special client software on user computer. It remotely uses web application client-server application and network connection of internal. It provides secure communication process for data and other transmission between two clients.

B. Virtual private network

The VPN extend a private network over public network like internet. It allows to a computer send or receive data over shared network if it directly connected to private network with providing functionality such as security and all management policies of VPN. This process is done by stable virtual point to point connection with use dedicated connection with encryption of two computers.

C. Point-to-Point Tunneling Protocol

The PPTP is a way of implementing VPN network .it is use for control over TCP and GRE tunnel operate and encapsulating PPP packet. It provides security with encryption and remotely access level comparing with VPN products.

D. IPSec

IPSec is a security protocol for secure IP communication by encryption and authorizing every packet of transmission time. It is end to end security for operating on internet layer protocol. It is also used for protecting data between security gateway and between host and security gateway.

Conclusion

According to literature survey find out characteristics of network security, TELNET, FTP, Cloud network and Congestion control is able to secure any network. All security is able to provide security and enhance quality of service in the existing network. TELNET and FTP is able to preventing unauthorized access or secure all the information between communications. Cloud networking provide the facility to authorized client access servers or machines anywhere in the network with the valid used-id or password. Network access method provides the types of security of network when network is not able to recognize authentication person. All security issue provides better and reliable performance in the network. Encryption includes the different types of to create password or safely deliver the data form node to node or client to server.

Problem formulates

The problem with the previous literature survey, there is no privacy or security when user or client communicates with another server. The sending information or data is not secure because there is no restriction of accessing data for anyone. When the data is sent in unsafe environment the data is not sent to appropriate location, the private data is lost in the middle way or access by another person. The main problem with the last work there is no security issue for protecting data or devices.

7. PROPOSED WORK

In this paper we proposed a network security including TELNET and FTP protocol security. Using this technique only authorizes or registered user access the services or network otherwise he/she is not able to access information. Using Direct Access security no one directly use any wireless device or network without user-id and password. When the network is jam or packet sending failed there is I include Console security, using this technique a system directly uses routers as an admin or reset all the oldest work and reconfigure system. Cloud networking registered user login the system from anywhere in the network or access all the information or communicated with every node. Congestion is used when network is not able to send any packet to the appropriate location or sending failed then the congestion control is able to reduce the network traffic over internet or resending the data without loss. In this network I include five types of security like TELNET security, FTP security, Console security, Direct Access security, Access Point security for better secure environment and safe communication between two or more nodes.

8. TOOL FOR PRACTICAL WORK

8.1 Introduction of Cisco Packet Tracer

Packet Tracer is providing a way of fidelity, network capable, and simulation based learning environment for networking novices to design, configure, and troubleshoots computer networks at a CCNA level of t complexity. It supports an array of simulation application layer protocol and support basic routing with RIF, OSPF, EIGRP. The main aim of packet tracer provides a realistic simulation of functional network. In the Packet Tracer application utilizes number of features found with the actual hardware running on current Cisco version. Packet tracer is providing an integrated simulation, visualization, collaboration, and assessment environment. It supports the much of tasks like Creation of Simulations, Visualizations, and Animations of Networking Phenomena. It implemented on a simplified model of networking devices and protocols. It provides real computer networks, Experienced both in person/hands on and remotely.Packet tracer is creating to help address the digital divide in networking education, where students and teachers access the equipment, bandwidth, and interactive modes of learning networking.

9. EXPERIMENTAL WORK

9.1 FTP Commands for Access Network Service: -

FTP command sent the instruction to an FTP server including RFC 959 standard by the IETF. FTP provides some following command. These are the following with description.

Command	Description
ABOR	Abort an active file transfer.
ACCT	Account information of FTP.
ADAT	Securing Data or Authentication.
ALLO	Allocate disk space to receive a file.
APPE	Append.
AUTH	Security Mechanism /Authentication.
CCC	Clear Command Channel.
CDUP	Change to Parent Directory.
CONF	Confidentiality Protection Command.
CWD	Change working Directory.
DELE	Delete a File.
ENC	Privacy Protection Channel.
EPRT	Specifies an extended address and port.
EPSV	Enter extended passive mode.
HELP	General Help related to document.
LANG	Language Negotiation.
LIST	Returns information of a file.
LPRT	Specifies a long address and port.

LPSV	Enter Long Passive mode.
MIC	Integrity Protected Command.
MKD	Making Directory.
MLSD	Lists the content of directory.
MODE	Set the transfer mode.
NOOP	No operation.
OPTS	Select option for features.
PASS	Authentication password.
PBSZ	Protection Buffer Size.
PWD	Print Working Directory.
QUIT	Disconnect.
REIN	Re initializes the connection.
RESET	Restart transfer from point.
RETR	Transfer a copy of file.
RMD	Remove Directory.
RNFR	Rename form.
RNTO	Rename to.
SIZE	Returns the size of file.
SMNT	Mount file str.
STAT	Returns current status.
STOR	Accept and store data as a file on the server.
STOU	Store File uniquely.
USER	Authentication username.
XMKD	Make directory.
XCUP	Change the parent of current directory.
XPWD	Print current directory
XRMD	Remove directory.

(Table 1: FTP commands with description)

10. TELNET COMMAND FOR ACCESS NETWORK SERVICES

The Telnet permit a client or system communicate witha another computer remotely using Telnet Protocol. We can run Telnet without parameter enter context indicate by Telnet prompt. With the help of Telnet prompt we use the following command to manage a computer Telnet client.

The **tlntadmn** command permits us to remotely manage a computer running Telnet Server. This command is run from the command prompt. Without use parameter, **tlntadmn** show local server settings. User use **telnet** commands on the Telnet prompt and start Telnet Client and to enter the Telnet prompt.

11. PRACTICAL WORK OF THE NETWORK

The Packet tracer is a medium fidelity, network-capable, simulation-based learning environment for networking novices to design, configure, and troubleshoot computer networks. Its environments are very easy to work on this. it providesa real-time connection (wired or wireless), devices (routers, switches, web server, pc or laptops, cables) or communication between node to node using cloud network (Internet service Provider) and provide much of ways to inbuilt a security in a network (FTP, TELNET, console security, enable Security, direct access security, password security, encryption & decryption security, data hiding security).

Using this tool,we design a network for security purpose or user verification. In this network A Main head office is located in the Mumbai city. And its five branches located in another city (Jaipur, Delhi, Pune, Kolkata and Ahmadabad). The concept behind design this network, there is a one main server and five client servers also exist at another location and provide the much of security of every client server, routers, switch, Wi-Fi server or and main server (all web servers, server Routers, Switches) And Cloud Network (Internet service provider) because all client routers are connected by the cloud network (Internet Service Provider).

At the Head office Server a Switch is connected with all city Web Server and computers that is also lactated at the client system. This Switch is connected to the Router by the Cable.At the client office that is located in another city the Switch is connected by the workgroup computer and Web server and direct access devices (used for Wi-Fi).An Another Router is connected with 5 department or Section (DRY, WAT, COLLECTION and IT ACCOUNT), every departments have workgroup System and Web Server. All Client Routers, Department routers and Head Office Routers are connected by the cloud network (ISP).

This is the basic structure of the network. Now I explain every security inbuilt in the network.The oldest network not follow the major security concern, there is no security for head office servers, everyone (that exist in the network) check, update delete or overwrite the server data.

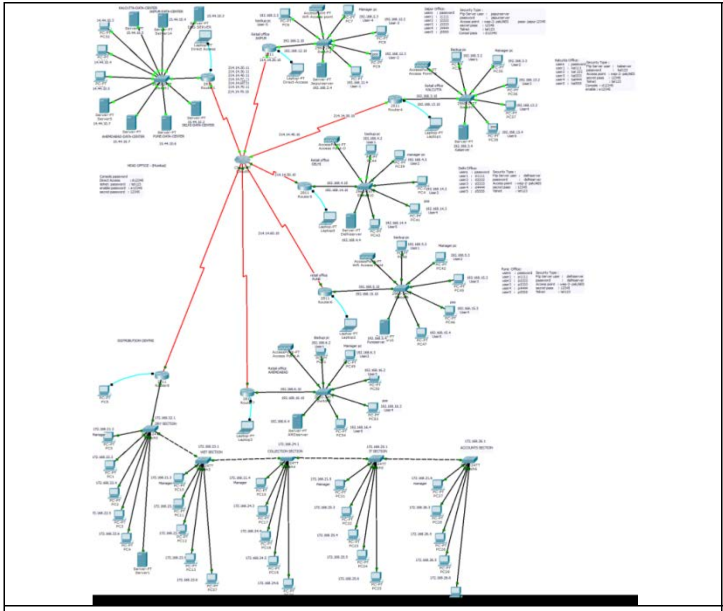
So,we give enhance security in this network, in this network every system is safe or secure, they can communicate without any problem. In this network of client level, every system or user has a user-id or encrypted password. Without id or password no one can access web Server. At every level FTP and TELNET protocol provide the security, without using this protocol user not ping or send the data of the server. User can access or check data only self-server not head office server because the security is not granted to access another server. Every computer a client system is register with ID and password on the web server. With the help of ID and password user can communicate update write delete or overwrite the data at the client level.

At the head office, main server has every client web server. Head office or main web server registered the entire client web server with user id or Encrypted Password. Without ID or password web server cannot access head office web server. In this network every router has enable security, console security and Line vty 0 security. That is using for user verification and user authentication. In this network every Switch has a special encryption algorithm password. That enables all unauthorized access or fake users (cybercriminal). At all the node a direct access device is also connect that is used for wireless devices, all wireless devices is connected in this network using direct access service. So direct Access device also protected in this network, if the wireless user has specific or registered with the web server then he/she is able to access the web server.

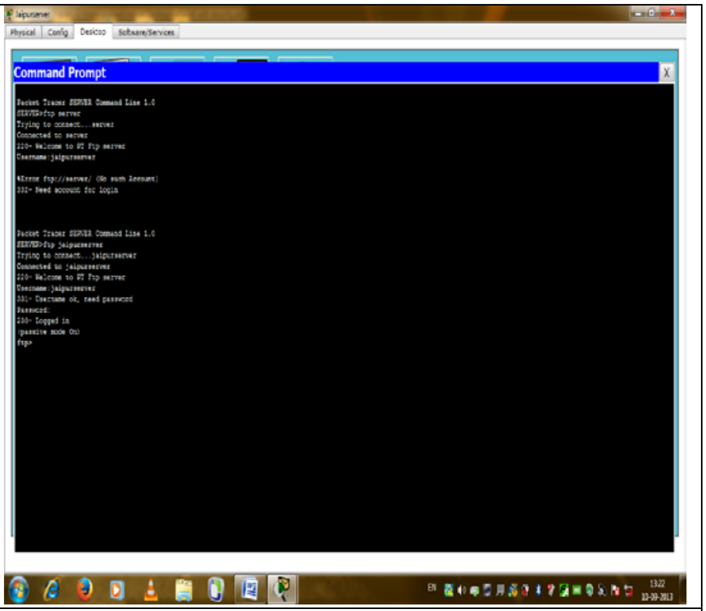
The main base of this architecture of this network is cloud network, it provides or communicate with every router in the network. It has much of security. It provides services only authorized routers. It provides the secure transmission in every node. After establish all security, every client ping self-web server using FTP Protocol or TELNET protocol and every client web Server ping head office web Server with the help of user name and password.

At the head office router,we create a direct access security that is use terminal configuration. This security is used when all system is not accessible web server or router. When network is jam or conjunction server is failure. Then terminal security direct access the router as an administrator with encrypted Terminal password or router password and solve the all issue relater accessing the system.Using FTP, client web server login the head office, after login client check all directory by using command (dir), download a file from head office server to client server (using get command) or upload a file from client server to head office server to client server (using put command).Same as FTP, TALNET work is same but there is access method is different. It is more securable compare FTP. it mostly using by larger group or big corporate sector because it has more capacity to handle all the security (IP security or better encryption and decryption technologies) small group or Small company not supported this based architecture.

11. Result (Generated output)

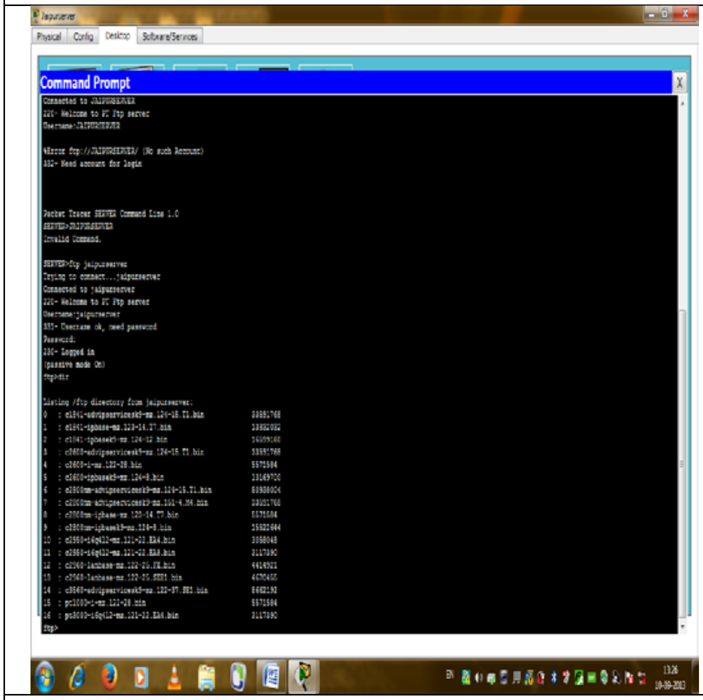


(Fig.1 - The Complete network Design Structure)



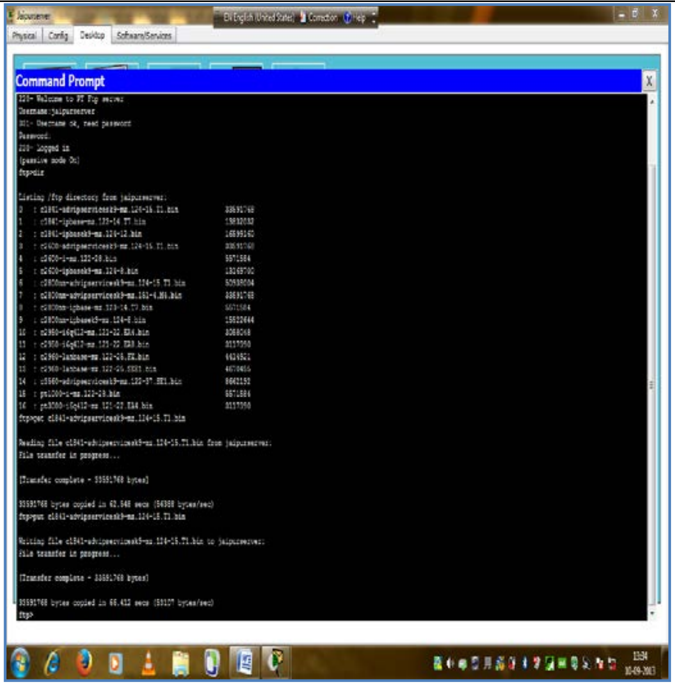
```
Packet Tracer SERVER Command Line 1.0
SERVER>ftp server
Trying to connect...server
Connected to server
220- Welcome to PT Ftp server
Username:jaipurserver

%Error ftp://server/ (No such Account)
332- Need account for login



Packet Tracer SERVER Command Line 1.0
SERVER>ftp jaipurserver
Trying to connect...jaipurserver
Connected to jaipurserver
220- Welcome to PT Ftp server
Username:jaipurserver
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

(Fig.2 - Command prompt window) (Login by the client on the server)



```
Connected to JAIPURSERVER
220- Welcome to PT Ftp server
Username:JAIPURSERVER

%Error ftp://JAIPURSERVER/ (No such Account)
332- Need account for login



Packet Tracer SERVER Command Line 1.0
SERVER>JAIPURSERVER
Invalid Command.

SERVER>ftp jaipurserver
Trying to connect...jaipurserver
Connected to jaipurserver
220- Welcome to PT Ftp server
Username:jaipurserver
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>dir

Listing /ftp directory from jaipurserver:
0   : c1841-advipservicesk9-mz.124-15.T1.bin          33591768
1   : c1841-ipbase-mz.123-14.T7.bin                   13832032
2   : c1841-ipbasek9-mz.124-12.bin                    16599160
3   : c2600-advipservicesk9-mz.124-15.T1.bin          33591768
4   : c2600-i-mz.122-28.bin                           5571584
5   : c2600-ipbasek9-mz.124-8.bin                     13169700
6   : c2800nm-advipservicesk9-mz.124-15.T1.bin        50938004
7   : c2800nm-advipservicesk9-mz.151-4.M4.bin         33591768
8   : c2800nm-ipbase-mz.123-14.T7.bin                 5571584
9   : c2800nm-ipbasek9-mz.124-8.bin                   15522644
10  : c2950-i6q4l2-mz.121-22.EA4.bin                  3058048
11  : c2950-i6q4l2-mz.121-22.EA8.bin                  3117390
12  : c2960-lanbase-mz.122-25.FX.bin                  4414921
13  : c2960-lanbase-mz.122-25.SEE1.bin                4670455
14  : c3560-advipservicesk9-mz.122-37.SE1.bin         8662192
15  : pt1000-i-mz.122-28.bin                          5571584
16  : pt3000-i6q4l2-mz.121-22.EA4.bin                 3117390
ftp>
```

Fig.3 - Update or check all the directory by the client that exist on the main server or (head office))



```
220- Welcome to PT Ftp server
Username:jaipurserver
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>dir

Listing /ftp directory from jaipurserver:
0   : c1841-advipservicesk9-mz.124-15.T1.bin          33591768
1   : c1841-ipbase-mz.123-14.T7.bin                   13832032
2   : c1841-ipbasek9-mz.124-12.bin                    16599160
3   : c2600-advipservicesk9-mz.124-15.T1.bin          33591768
4   : c2600-i-mz.122-28.bin                           5571584
5   : c2600-ipbasek9-mz.124-8.bin                     13169700
6   : c2800nm-advipservicesk9-mz.124-15.T1.bin        50938004
7   : c2800nm-advipservicesk9-mz.151-4.M4.bin         33591768
8   : c2800nm-ipbase-mz.123-14.T7.bin                 5571584
9   : c2800nm-ipbasek9-mz.124-8.bin                   15522644
10  : c2950-i6q4l2-mz.121-22.EA4.bin                  3058048
11  : c2950-i6q4l2-mz.121-22.EA8.bin                  3117390
12  : c2960-lanbase-mz.122-25.FX.bin                  4414921
13  : c2960-lanbase-mz.122-25.SEE1.bin                4670455
14  : c3560-advipservicesk9-mz.122-37.SE1.bin         8662192
15  : pt1000-i-mz.122-28.bin                          5571584
16  : pt3000-i6q4l2-mz.121-22.EA4.bin                 3117390
ftp>get c1841-advipservicesk9-mz.124-15.T1.bin

Reading file c1841-advipservicesk9-mz.124-15.T1.bin from jaipurserver:
File transfer in progress...

[Transfer complete - 33591768 bytes]

33591768 bytes copied in 62.548 secs (54388 bytes/sec)
ftp>put c1841-advipservicesk9-mz.124-15.T1.bin

Writing file c1841-advipservicesk9-mz.124-15.T1.bin to jaipurserver:
File transfer in progress...

[Transfer complete - 33591768 bytes]

33591768 bytes copied in 66.412 secs (53107 bytes/sec)
ftp>
```

(Fig.4 - Download or Upload a file by the client on the main server)

12. CONCLUSION& FUTURE WORK

Here we conclude the report starting that when the FTP and TELNET protocol is used in network security all the information is send for client to server or node to node without any losses. Both protocols secure all the transmission on communication time. Cloud network after enabling security is granting permission only registered or authorize user, if the unauthorized client or user want to access check data or information he/she is not able to check because all the password or data is encrypted with high level security. FTP and TELNET provide the USER-ID or Encrypted password to every user. To help this ID and password user access the server or all network equipment's. FTP and TELNET enhance the better security after establishing a network or provide a safe environment for user secure transmission over cloud network or any other network. The FTP security preventing unauthorized activity over the network and TELNET provide the remotely accessing method for one machine to another machine in safe or secure environment. The other security like access point security provides the security for wireless network, using this security unauthorized user or hacker does not able to access any device or not able to attach her device in this network environment because all wireless severs or devices register every wireless node with user-id and encrypted password so with user-id and password other user not able to access network or its services. Other security in this network is direct access security, this security use in the condition when all network server are jam or network traffic, when no routers response against client queries and no transmission between two routers mean router is going to dead condition reason behind it network traffic, in this condition direct access security provide a way to direct access routers by a system and disable all transmission process or end all network traffic and no losses important information. This service provides high level security only for administration because if this security is brake by hacker he/she is able to destroy all network security and theft all private data when communication over router to router so this security provides high level encryption password security with user-id to admin. After using this service admin is able add or remove authorize client or all type of devices in the network or clear all the transmission in the network jam condition. This network is a fully secure with all security but a main security is providing a quality of an admin when a user or clients forget user-id or password, this security is called Enable security. This security uses when a client or user forget her verification method or password then the admin using this security enable all password or recreate a new user-id or password or block last using password. This technique is also uses in Bank ATM, when a client is forget her ATM password then a Bank admin take a new password or block last password. If last password is not block then anyone access all network service so all new parameter provide to the authorize client using this security.

Finally analyzing the factors responsible for increasing security and no of nodes or authorize client in network and restricted unauthorized activity. We came to this conclusion that network security must give emphasis on the measures taken to increase capability of network and all security like FTP security, TELNET security, Direct access security, Console security, enable security provide a batter secure environment for communication and using this all security all device or all-important data is safe by external person or unauthorized client.

The future scope of my work is enabling or provides high level security for IP Security. When the network is able to access IP Sec no one check IP configuration of any client system and no one is check the machine configuration. The benefit of this security user has self-machine information no one guess which user communicate to server with which machine and all data is better secure transmit from sender to server or node to node. Another work is also including in types of password Encryption, using strong encryption unauthorized user not estimate the actual password. The future work is intended to improve the efficiency and reliability of network and it does improve its capability.

13. REFERENCES

[1]. Helen Fouché Gaines, “Cryptanalysis”, 1939, Dover. ISBN 0-486-20097-3
[2]. David Kahn, The Code breakers - The Story of Secret Writing (ISBN 0-684-83130-9)
[3]. Abraham Sinkov, Elementary Cryptanalysis: A Mathematical Approach, Mathematical Association of America, 1966. ISBN 0-88385-622-0
[4]. Preneel, Bart, "Advances in Cryptology — EUROCRYPT 2000", Springer Berlin Heidelberg, 2000, ISBN 978-3-540-67517-4
[5]. T. Kohno, J. Viega, and D. Whiting. "The CWC Authenticated Encryption (Associated Data) Mode". NIST. Retrieved March 12, 2013.
[6]. Failures of secret-key cryptography". Daniel J. Bernstein. Retrieved March 12, 2013.
[7]. 19772:2009. ISO/IEC. Retrieved March 12, 2013.
[8]. NIST. Retrieved April 17, 2013.
[9]. Retrieved March 12, 2013.
[10]. M. Bellare and C. Namprempre Retrieved April 13, 2013.
[11]. H. Krawczyk. Retrieved April 13, 2013.
[12]. Forouzan, B.A. (2000). TCP/IP: Protocol Suite. 1st ed. New Delhi, India: Tata McGraw-Hill Publishing Company Limited.
[13]. Kozierok, Charles M. (2005). "The TCP/IP Guide v3.0". Tcpiguide.com.
[14]. Dean, Tamara (2010). Network+ Guide to Networks. Delmar. pp. 168–171.
[15]. Clark, M.P. (2003). Data Networks IP and the Internet. 1st ed. West Sussex, England: John Wiley & Sons Ltd.
[16]. Postel, J., & Reynolds. J. (October 1985). . In The Internet Engineering Task Force.
[17]. Active FTP vs. Passive FTP, a Definitive Explanation". Slacksite.com. (see http://webcache.googleusercontent.com/search?q=cache:http://slacksite.com/other/ftp.html if the original web page is not available).
[18]. Parker, Don (September 2005). "Understanding the FTP Protocol". Windowsnetworking.com.
[19]. Allman, M. & Metz, C. & Ostermann, S. (September 1998). RFC 2428. In The Internet Engineering Task Force.
[20]. P. &Emtage, A. & Marine, A. (May 1994). "RFC 1635". The Internet Engineering Task Force.
[21]. Gleason, Mike (2005). "The File Transfer Protocol and Your Firewall/NAT". Ncftp.com.

[22]. Kurose, J.F. & Ross, K.W. (2010). Computer Networking. 5th ed. Boston, MA: Pearson Education, Inc.

[23]. Matthews, J. (2005). Computer Networking: Internet Protocols in Action. 1st ed. Danvers, MA: John Wiley & Sons Inc.

[24]. Berners-Lee, T. &Masinter, L. &McCahill, M. (December 1994). "RFC 1738". The Internet Engineering Task Force.

[25]. Accessing FTP servers | How to | Firefox Help". Support.mozilla.com. 2012-09-05. Retrieved 2013-01-16.

[26]. How to Enter FTP Site Password in Internet Explorer". Support.microsoft.com. 2011-09-23. Retrieved 2013-01-16.

[27]. Securing FTP using SSH. Retrieved from http://www.nurdletech.com/ftp.html

[28]. Allman, M. & Ostermann, S. (May 1999). "RFC 2577". The Internet Engineering Task Force.

[29]. Deploying a Cloud". Dell.com. Retrieved 2012-03-27.

[30]. Mariana Carroll, Paula Kotzé, Alta van der Merwe (2012). "Securing Virtual and Cloud

[31]. Environments". In I. Ivanov et al. Cloud Computing and Services Science, Service Science: Research and Innovations in the Service Economy. Springer Science+Business Media. doi:10.1007/978-1-4614-2326-3.

[32]. The NIST Definition of Cloud Computing". National Institute of Standards and Technology. Retrieved 24 July 2011.

[33]. Amazon Web Services. 2013-3-19. Retrieved 2013-3-20.

[34]. Baburajan, Rajani, "The Rising Cloud Storage Market Opportunity Strengthens Vendors," infoTECH, August 24, 2011". It.tmcnet.com. 2011-08-24. Retrieved 2011-12-02.

[35]. Oestreich, Ken, (2010-11-15). "Converged Infrastructure". CTO Forum. Thectoforum.com. Retrieved 2011-12-02.

[36]. Strachey, Christopher (June 1959). "Time Sharing in Large Fast Computers". Proceedings of the International Conference on Information processing, UNESCO. paper B.2.19: 336–341.

[37]. Simson Garfinkel (3 October 2011). "The Cloud Imperative". Technology Review (MIT). Retrieved 31 May 2013.

[38]. Ryan; Falvey; Merchant (October 2011). "Regulation of the Cloud in India". Journal of Internet Law 15 (4)

[39]. July, 1993 meeting report from the IP over ATM working group of the IETF". CH: Switch. Retrieved 2010-08-22.

[40]. Corbató, Fernando J. "An Experimental Time-Sharing System". SJCC Proceedings. MIT. Retrieved 3 July 2012.

[41]. "Jeff Bezos' Risky Bet". Business Week

[42]. "Amazon's early efforts at cloud computing partly accidental". IT Knowledge Exchange. Tech Target. 2010-06-17

[43]. B Rochwerger, J Caceres, RS Montero, D Breitgand, E Elmroth, A Galis, E Levy, IM Llorente, K Nagin, Y Wolfsthal, E Elmroth, J Caceres, M Ben-Yehuda, W Emmerich, F Galan. "The RESERVOIR Model and Architecture for Open Federated Cloud Computing", IBM Journal of Research and Development, Vol. 53, No. 4. (2009)

[44]. D Kyriazis, A Menychtas, G Kousiouris, K Oberle, T Voith, M Boniface, E Oliveros, T Cucinotta, S Berger, "A Real-time Service Oriented Infrastructure", International Conference on Real-Time and Embedded Systems (RTES 2010), Singapore, November 2010

[45]. Keep an eye on cloud computing, Amy Schurr, Network World, 2008-07-08, citing the Gartner report, "Cloud Computing Confusion Leads to Opportunity". Retrieved 2009-09-11.

[46]. Gartner Says Worldwide IT Spending On Pace to Surpass Trillion in 2008, Gartner, 2008-08-18. Retrieved 2009-09-11.

[47]. "Launch of IBM Smarter Computing". Retrieved 1 March 2011.

[48]. Andreas Tolk. 2006. What Comes After the Semantic Web - PADS Implications for the Dynamic Web. 20th Workshop on Principles of Advanced and Distributed Simulation (PADS '06). IEEE Computer Society, Washington, DC, USA

[49]. "Cloud Computing: Clash of the clouds". The Economist. 2009-10-15. Retrieved 2009-11-03.

[50]. "Gartner Says Cloud Computing Will Be As Influential As E-business". Gartner. Retrieved 2010-08-22.

[51]. Gruman, Galen (2008-04-07). "What cloud computing really means". InfoWorld. Retrieved 2009-06-02.

[52]. "The economy is flat so why are financials Cloud vendors growing at more than 90 percent per annum?". FSN. March 5, 2013.

[53]. Figure 8, "A network 70 is shown schematically as a cloud", US Patent 5,485,455, column 17, line 22, filed Jan 28, 1994

[54]. Figure 1, "the cloud indicated at 49 in Fig. 1.", US Patent 5,790,548, column 5 line 56-57, filed April 18, 1996

[55]. Antonio Regalado (31 October 2011). "Who Coined 'Cloud Computing'?". Technology Review (MIT). Retrieved 31 July 2013.

[56]. HAMDAQA, Mohammad (2012). Cloud Computing Uncovered: A Research Landscape. Elsevier Press. pp. 41–85. ISBN 0-12-396535-7.