

# CENTRALIZED HOST CONTROL SYSTEM

MANTU KUMAR

*Department of Computer Science and Engineering, Maharishi Markandeshwar University, Mullana,  
Ambala, Haryana, India  
mantuonline@gmail.com*

NEERA BATRA

*Department of Computer Science and Engineering, Maharishi Markandeshwar University, Mullana,  
Ambala, Haryana, India  
batraneera1@gmail.com*

## **Abstract:**

This paper is based on the client server technology, in which different clients are connected to a centralized host machine to share files and folders. Clients should login to the server and they can upload, download and delete file from the server machine. Server also perform the monitoring of clients and can restrict the activity of any client by blocking its IP address. It is cost effective to manage and share files or data on single system instead of multiple systems.

**Keywords:** *Computer network, File Transfer Protocol (FTP), Centralized Host Control System (CHCS).*

## **1. Introduction**

The computing environment of the internet is based on client/server model [1] [3]. A client/server network has two roles for computers: clients and servers. The server is a computer that responds to requests for its services. The client is a computer that requests a service from a server. As shown in Fig. 1, in a client/server network, the server can be considered as the host and the client can be considered as the guest. When guest asks for something, the host tries to full fill the request.

Computer network provides facility to connect computers and other resources like printers, memory, files stored at different places in the network. Computer network is created with the help of default operating systems such as Window 2000, XP, NT and 2007 along with networking devices like router, switch and LAN cables etc. When using window's features to connect computer, it requires lot of time and it is difficult to maintain security on data of computer. In CHCS, we can make one machine as server by installing server software and other client software of CHCS has to be installed at client machine. After installation of appropriate softwares, clients are able to use provided memory space at server machine for data uploading and downloading. CHCS implementation is done using various File Transfer Protocol (FTP) commands [1] [2]. It uses TCP/IP protocol suite for connection oriented features [13].

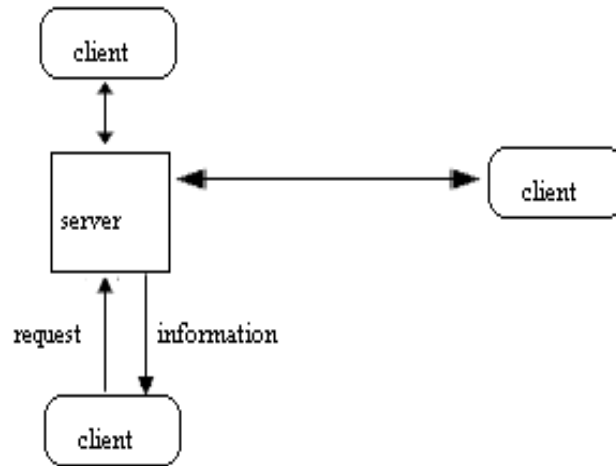


Fig. 1: Client Server Model

## 2. Literature Review

The early 1980's saw tremendous expansion in the area of network deployment. As companies realized the cost benefits and productivity gains created by network technology, they began to add networks and expand existing networks almost as rapidly as new network technologies and products were introduced. By the mid-1980's, certain companies were experiencing growing pains from deploying many different (and sometimes incompatible) network technologies.

The problems associated with network expansion affect both day-to-day network operation management and strategic network growth planning. Each new network technology requires its own set of experts. In the early 1980s, the staffing requirements alone for managing large, heterogeneous networks created a crisis for many organizations. An urgent need arose for automated network management (including what is typically called network capacity planning) across diverse environments.

With the introduction of the Internet, came a new and extensive network system, packed with new features. Communications and file transfers are simpler and easier than ever before. The Internet indirectly connects any computer on the Internet to every other computer on the Internet. Access is immediately possible to growing millions of computers and files. The administrator of each computer on the Internet grants permission to access their computer.

The current techniques to transfer data include the Windows built-in features and also the traditional HTTP [7] [8] [9]. Although Windows provides good transfer capabilities, it supports only intranet data transfer rather than transfer of data across the internet because it uses a customary protocol which is not supported on Internet. HTTP protocol, on the other hand, is considered to be very ineffective as it is a stateless protocol. Due to this reason, it turns out to be a resource consuming technique. It is also insecure in the sense that it doesn't require any user authentication prior to sharing of data.

Distributed computing [10] [11] [12] deals with hardware and software systems containing more than one processing element or storage element, concurrent processes or multiple programs, running under a loosely or tightly controlled regime.

In distributed computing, a program is split up into parts that run simultaneously on multiple computers communicating over a network. Distributed computing is a form of parallel computing, but parallel computing is most commonly used to describe program parts running simultaneously on multiple processors in the same computer. Both types of processing require dividing a program into parts that can run simultaneously, but distributed programs often must deal with heterogeneous environments, network links of varying latencies and unpredictable failures in the network or the computers.

### 3. Problem Statement

Not so long ago, the easiest and the simplest way to transfer files from one desktop computer to another was via the “sneaker net” – walking a diskette between machines. Later, modems and serial connections made it possible to transfer files between two computers using telephone lines. Setting up both computers for serial communication requires some preparation and time considerations.

Once more modern computer networks made their debut, transferring files became as simple as retrieving or saving a file. Communications within such networks are done over high-speed network cables.

### 4. Proposed Model

Centralized Host Control System (CHCS) is the client/server based system developed to centrally store files of all clients, who wish to store at server machine [4] [5] [6]. Client should log on server using authorized user name and password. Fig. 2 shows that multiple clients logged on server machine and performing files related work. This model enhances the file or data transfer over the network and it is cost effective for the organization. System Administrator can see different activity of the client in statistics of server machine, if administrator find users doing anything wrong, then, they can block that user by IP address. Fig. 2 shows client doing different files related work like file uploading, downloading, deleting, making new folder, renaming the folder and deleting the existing folder.



Fig. 2: Architecture of Centralized Host Control System.

## 5. Design and Development

### 5.1. Design and Architecture

As shown in Fig. 3, server control client from its location by capturing client to his location and clients automatically transfer their files (data and programs) to server and hence server updates statistical components like uploading and downloading of files, total size of data uploaded and downloaded, number of clients login and currently login to server etc.

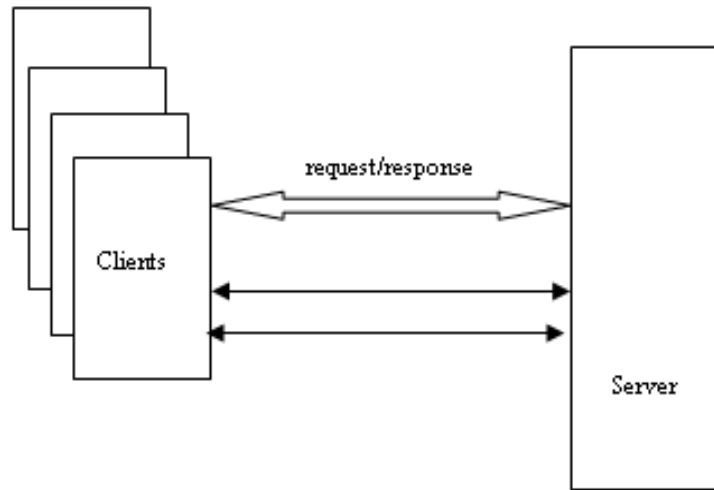


Fig. 3: Client Server Architecture

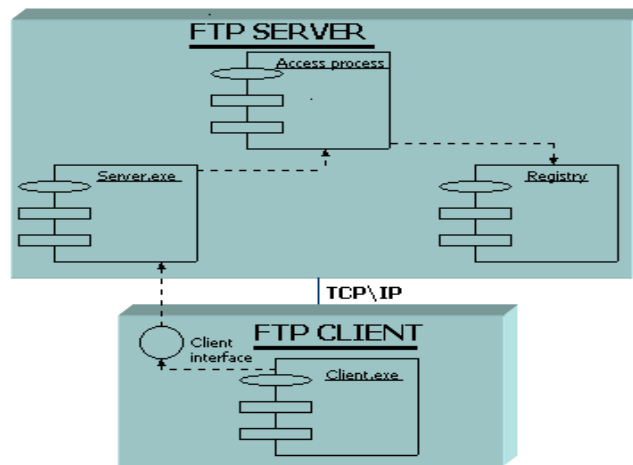


Fig. 4: Component and Deployment Diagram of CHCS

As shown in Fig. 4, the CHCS has two components to deploy, one is server.exe and another one is client.exe. The server.exe is FTP server component of the CHCS that runs on server machine to listen client request according to their access permission and manages log files for all operation performed by the client. The client.exe is FTP client component of the CHCS that runs on client machine. Client should connect to server machine with the help of connection window by providing IP address, user ID and password. After user authentication, client directly communicates with the server machine to perform file related operation.

**5.2. Modules**

Fig. 5 gives an overview of the functionality of two main modules i.e. FTP server and FTP client of CHCS.

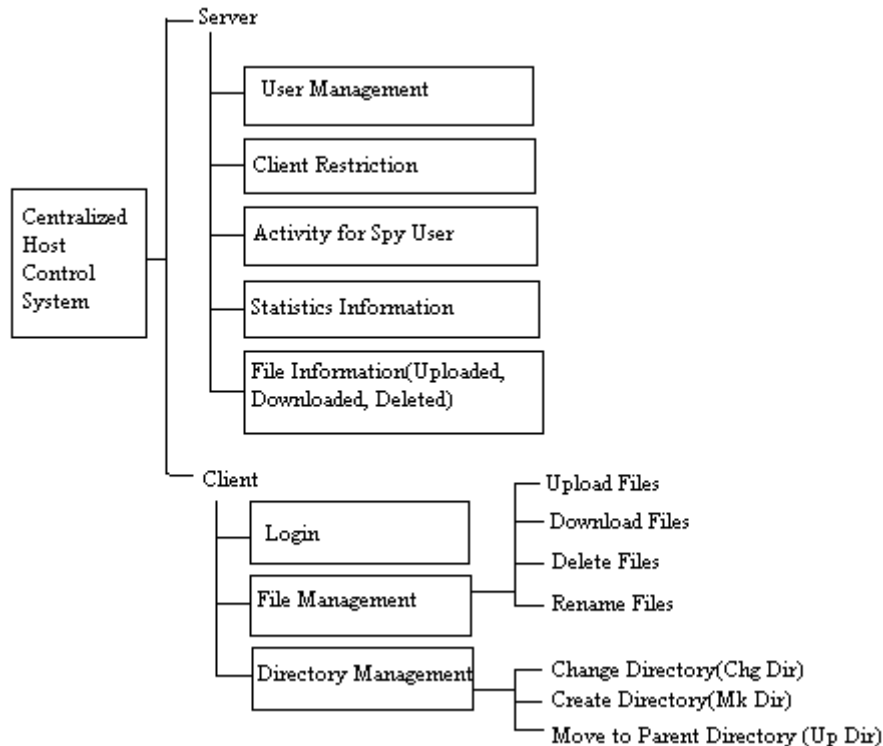


Fig. 5: Centralized Host Control System and its Modules

### 5.2.1. FTP Server

This application is a Graphical User Interface based FTP Server. FTP Server is a server socket which will be listening for clients and accept the request through authentication by asking the user name and password, then giving permission to the users according to their privileges. The main feature of this FTP Server is a frame which is used to display status messages like date and time when the client logged in and number of clients connected to the server. It has following sub-modules:

- User Management: New user created and they should login using user ID and password after authentication.
- Client Restriction: Client should be restricted to login to server
- Activity for Spy User: If one wants to hide the activity of the particular user, system will make that user as spy user. It can make various users as spy users.
- Statistics Information: It display the client activity report like how many files uploaded, downloaded, and also about how many client login to the server etc.
- File Information: (Uploaded, Downloaded, and Deleted): It gives information about files uploaded, downloaded and deleted etc.

### 5.2.2. FTP Client

It should connect to the server for uploading and downloading the data. It has following sub- modules:

- Login: User should login to server using user name and password. User name and password are provided by the administrator.
- File Management: User can manage file and folder on the server. It includes following activity:
  - Upload File: This option along to upload of files to server machine.
  - Download File: This option allow user to download files from server machine to user machine.
  - Delete File: This command causes the file specified in the pathname to be deleted at the server site. If an extra level of protection is desired (such as the query, "Do you really wish to delete?"), it should be provided by the user-FTP process.
  - Rename File: This option allows user to rename file.
- Directory Management: It manages directory related activities. Such as:
  - Change Directory: This command allows the user to work with a different directory or dataset for file storage or retrieval without altering his login or accounting information. Transfer parameters are similarly unchanged. The argument is a pathname specifying a directory or other system dependent file group designator.

- Create Directory: This command causes the directory specified in the pathname to be created as a directory (if the pathname is absolute) or as a subdirectory of the current working directory (if the pathname is relative).
- Move to Parent Directory: This command is a special case of current working directory and is included to simplify the implementation of programs for transferring directory trees between operating systems having different syntaxes for naming the parent directory.

### 6. Fundamentals of CHCS Framework

In this paper, we assume that the clients are privacy conscious. This is, the clients do not want to expose their genuine point location of the file to avoid theft and other security reasons.



Fig. 6: Client Login

As shown in Fig. 6, client machine wants to connect with server by authentication scheme in which client have to provide IP address of the FTP server machine followed by user ID and password. User ID and password are unique i.e. provided by the administrator after successful creation of the client login. Administrator assigns working area or memory space on server with related privileges. After successful login to server, client gets all services on own client window to perform all file related operations.

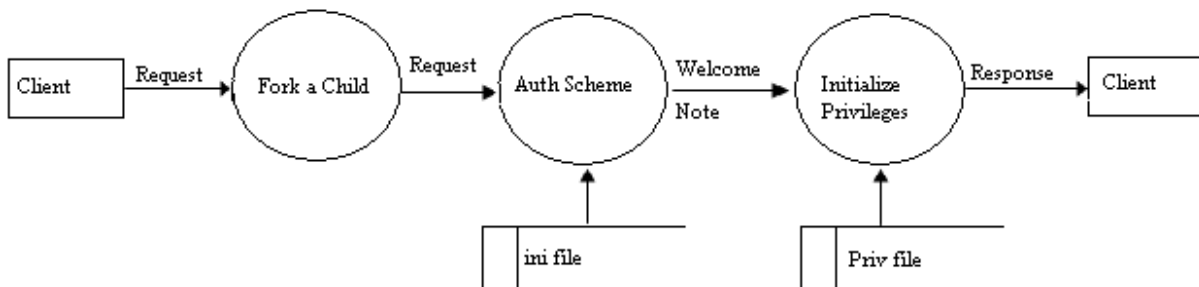


Fig. 7: steps involved in creation of New Process for client

As shown in Fig. 7, whenever, any client wants to connect to server machine, they have to send request to the server for resource allocation required for performing different operation. FTP server component of CHCS provide concurrent login to different client. For each client, when client request comes for connection, server create new child process and on that port, they listen the client request. After getting client request for connection, server checks authorization of the user from their database. In this scenario, ID and password of the user are retrieved from .ini (user’s profile) file of the user stored at the server machine at the time of user creation. After validation of the user, server retrieves user related privileges from privileges file or database and assigns it to the client. Now, client gets full access to the server for performing all file related works.

### 7. Results and Analysis

As shown in Fig. 8, administrator creating new client user and providing work space at server machine and related privileges to work in that allotted area.

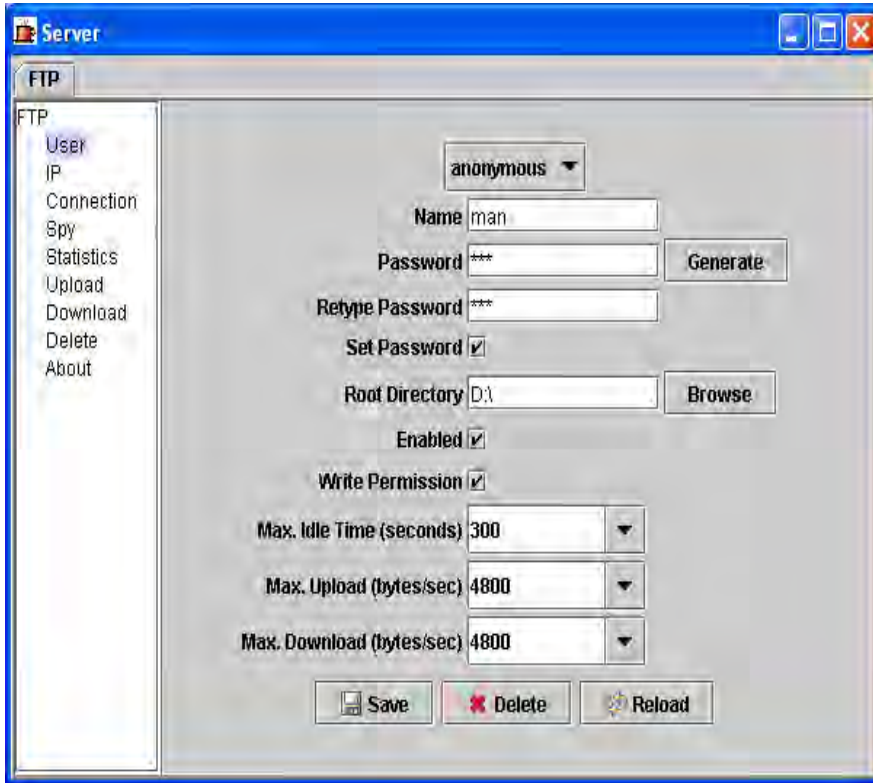


Fig. 8: Creation of user window

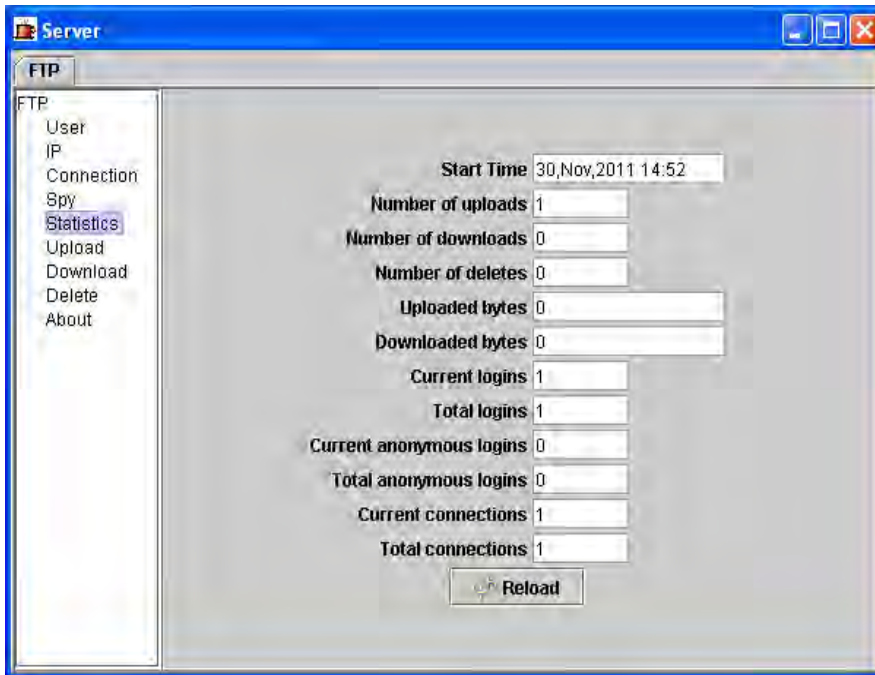


Fig. 9: Server machine

Fig. 9 shows server machine statistics window providing information regarding the number of clients connected till now, number of files uploaded and downloaded to the server machine by all clients, how many clients are currently login to the server, in the total size of uploaded and downloaded files separately.

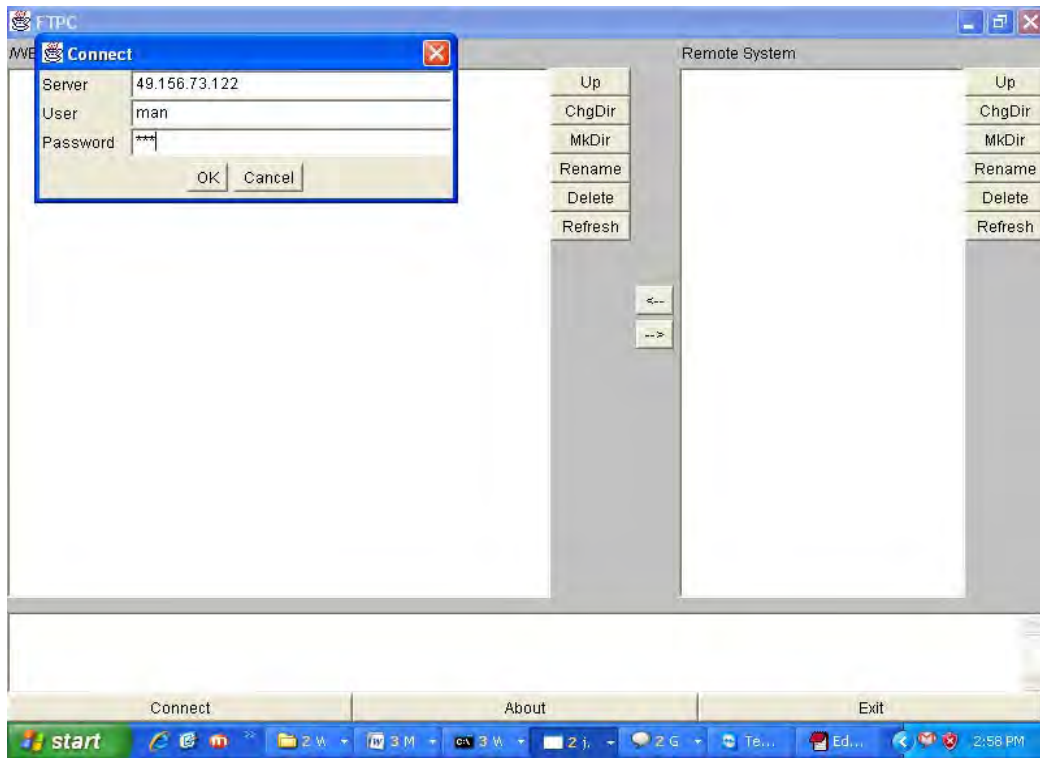


Fig. 10: Client Login Window

As shown in Fig. 10, client is making an attempt to the server machine after providing server machine IP address followed by client user ID and password. After authentication of user ID and password, user will get main screen of the client to perform all operations. If user ID and password are wrong, then, error message will display, and it does not become possible to connect to the server. If user wants to change anything related to user privileges, then they have to contact with administrator.

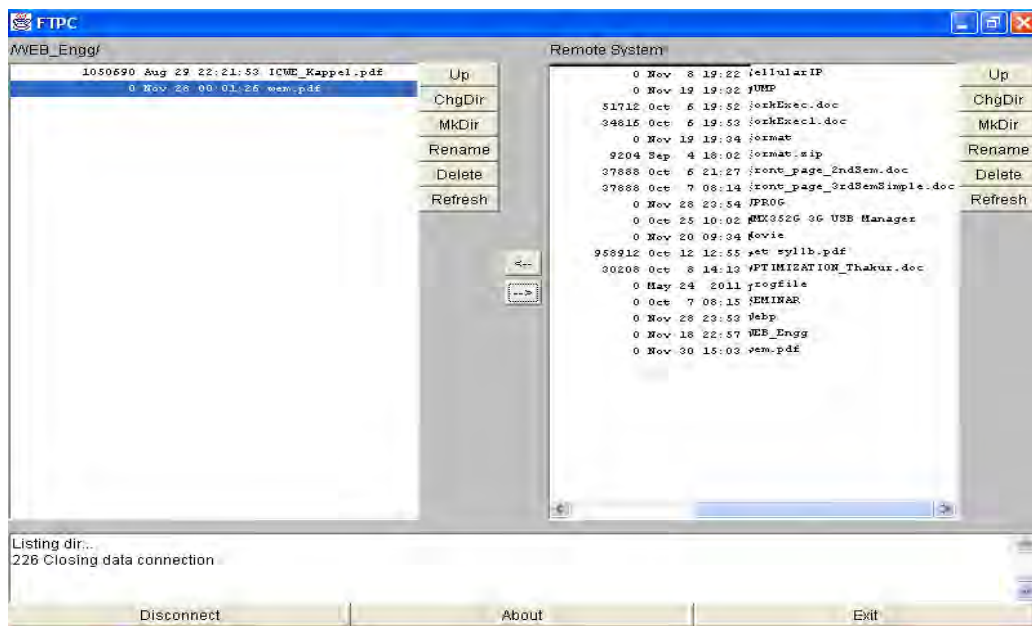


Fig. 11: Client Window



Fig. 11 shows client window in which left side window is client machine working area, listing current directory contents and the right window shows server machine working area and listing all contents of that area along with the privileges associated with file and folders. Now, client can perform various activities like create of a new folder and deleting a folder. They are performing file related works like uploading files to server machine, and downloading files from server machine. Client can delete own uploaded files at server machine also.

When user performs any operation related to the files and folders like uploading , downloading , delete, renaming of file, creating new folder and moving to parent directory, some response code and message will be displayed in lower part of the client window for every successful and unsuccessful operation. These codes are returned by the FTP commands.

## 8. Conclusion

This paper proposes a framework for data and file sharing between client and server. The framework is the first to holistically address the file or data securely stored at server machine by the client. It encourage indirect or implicit (via programs) use of remote computers into the organization for cost effective data sharing.

As for future work, there are different types of files to be uploaded to the server which may be harmful to the server. This may result in wastage of memory if the files being uploaded are not relevant to the works being performed on the server. So, in future, there is need to restrict users by not providing them files extension privileges to avoid uploading of the files to server.

## References

- [1] Bill Cheswick, "The Design of a Secure Internet Gateway", USENIX proceedings, 1990
- [2] David Presotto, Upas, "A simpler approach to network mail", USENIX proceedings, pp. 533-538, 1985
- [3] D. Tennenhouse, J.M. Smith, W. D. Sincoskie, D. J. Wetherall, G. J. Minden, "A survey of active network research", IEEE Communications Magazine, vol. 35, pp. 80-86, 1997.
- [4] J. Funasaka, M. Bito, K. Ishida, K. Amano, "PFTP: an FTP proxy system to assure the freshness of files", IEEE Proceedings of International Conference on Distributed Computing Systems Workshops, pp. 57-62, 2002.
- [5] Guanlin Chen, Mingming Chen, "Design and Implementation of FTP Search Engine Based on Lucene", IEEE International Conference on Internet Technology and Applications, pp. 1-4, 2010.
- [6] Niu Yan, Li Dong, Li Lala, "The Design on FTP Search Engine Model Based on Customer Feedback", IEEE International Workshop on Intelligent Systems and Applications, pp. 1-3, 2009.
- [7] J. Heidemann, K. Obraczka, J. Touch, "Modeling the performance of HTTP over several transport protocols", IEEE /ACM Transactions on Networking, vol. 5, pp. 616-630, 1997.
- [8] V. Parsiegla, S. Rein, A. Wolisz, "A network aware protocol for switching HTTP streams between devices", IEEE International Conference on Consumer Electronics-Berlin (ICCE-Berlin), pp. 74-78, 2011.
- [9] Qi Shen, Ji Hongbo, Li Wang, "Design and Implementation of Window Service Client Based on HTTP", IEEE International Conference on E-Business and E-Government (ICEE), pp. 3868-3871, 2010.
- [10] Swati Gupta, Kuntal Saroba, Bhawna, "Fundamental Research of Distributed Database", International Journal of Computer Science and Management Studies, vol. 11, pp. 138-146, 2011.
- [11] Ghazi Alkhatib, Ronny S. Labban, "Transaction Management in Distributed Database Systems: the case of Oracle's Two-phase commit", Journal of Information Systems Education, vol. 13, pp. 95-104, 1995.
- [12] A. F. Cardenas, "Heterogeneous Distributed Database Management: HD-DBMS", IEEE proceedings, vol. 75, pp. 588-600, 1987.
- [13] G. Huston, "TCP Performance", The Internet Protocol Journal, vol. 3, 83-95, 2000.
- [14] Internet Engineering Task Force (IETF) Forum: <http://www.ietf.org/>