INTERNATIONAL JOURNAL FOR TRENDS IN ENGINEERING & TECHNOLOGY
VOLUME 36 ISSUE 1 – MAY 2019 - ISSN: 2349 – 9303

Design and Implementation of New Secure File Transfer Protocol Using Triple DES and MD5

Shaharban O[1]
Department of Computer Science,
Anna University

S. Sudhakar [2]
Department of Computer Science,
AnnaUniversity.

Abstract-There are several ways to transfer files from one computer system to another or from one user to another. But they are less secure. Secure File Transfer Protocol (SFTP) aimed at developing a secure file transfer system for fast and secure file transmission. This is a WinForms application in which, software on one system communicates with software on another remote system. It prevents passwords and other sensitive information from being transmitted in the clear over the network. Here the data as well the key used for the encryption will be encrypted by a software key. The 32- byte long private key is generated by SFTP, from the data and personal information of the user. It is again encrypted by using the static software key of SFTP and sent it along with the data. Software key and the sender's private key are hided from the clients, so it provides more security to the data. This key is required to decrypt the data at the receiver. SFTP allows a range of operations on remote systems such as remote file search and file lock. An SFTP client extra capabilities include directory listings, and screen share. SFTP provides an interactive screen sharing between clients.

Keywords – Security, Encryption, File Transfer, MD5,Secure Shell, DES

I. INTRODUCTION

File transfer may be a term for the act of transmission files over a electronic network just like the web. There are varied ways in which and protocols to transfer file over a network. Computers which offer a file transfer service are typically referred to as file servers. Reckoning on the client's read the info transfer is named uploading or downloading. There are 2 forms of file transfer pull based mostly file transfers wherever the receiver initiates a file transmission request, and push based mostly file transfers wherever a sender initiates a file transmission request. File transfer will happen over a range of levels like, clear file transfers over network file systems, file transfers from dedicated file transfer services like File Transfer Protocol, HTTP, and distributed file transfers over peer-to-peer networks like Bittorent or Gnutella. Secure communication is once 2 entities are act and don't desire a person to pay attention it. Similar to that the transfer of sensitive info through the network ought to be secured by avoiding the interference of the remote systems except sender and therefore the receiver. Transferring files between machines or users may be a common incidence. maybe you wish to send a category listing program to AN workplace assistant or a document containing a grant proposal to a colleague at another University. In every of those cases, it's vital to understand what choices are offered to induce your file from one purpose to a different point and to understand whether or not the tactic you decide on provides adequate security given the sensitivity of the info being transferred. In the interest of protective client information or securing trade secrets several corporations are modifying their mechanisms of transferring data across the net. There is variety of things to contemplate once raising the protection of knowledge transfer procedures; this includes User Authentication, information Security and information Privacy. To produce user authentication, File transfer has historically used clear text passwords. This weakens the protection as somebody will develop the parole that's used, and use it later to induce access to the info. Information privacy (encryption) is employed to limit intermediate systems to access the info. Information security (integrity or tamper prevention) prevents modification to the info whereas it's in transit.

II. LITERATURE REVIEW

Cyber-security isn't simply a applied science science issue any longer. As each trade has become passionate about data technology through on-line presence, social media, knowledge analytics, and cloud computing. As reported within the most up-to-date FBI web Crime Report, the monetary impact of cyber-crime is staggering

2.1 Dynamical Setting

There are varied government and industry-based best follow initiatives progressing in support of

cyber-security. The Obama Administration created a Comprehensive National Cyber-Security Initiative to integrate the fascinating assortment of initiatives promoted by Federal and law-enforcement wants. The trade LED Unified Compliance Framework's has tried to supply the identical form of minimizing conflicts of cyber-security compliance objectives.

2.2 Vulnerabilities

Vulnerability may be a weakness of a system that permits a hacker to cut back a system's data assurance. Vulnerability may be a mixture of 3 elements: a system flaw, wrongdoer access to the flaw, and wrongdoer ability to create use the flaw. to take advantage of vulnerability, an wrongdoer should have a minimum of one applicable methodology that may connect with a system weakness. During this case, vulnerability is additionally referred to as the attack surface. Vulnerability management is that the cyclic method of distinctive, classifying, and decreasing vulnerabilities. This follow in the main categorize to software package vulnerabilities in computing systems. These threats will sometimes be divided into one in all the categories:

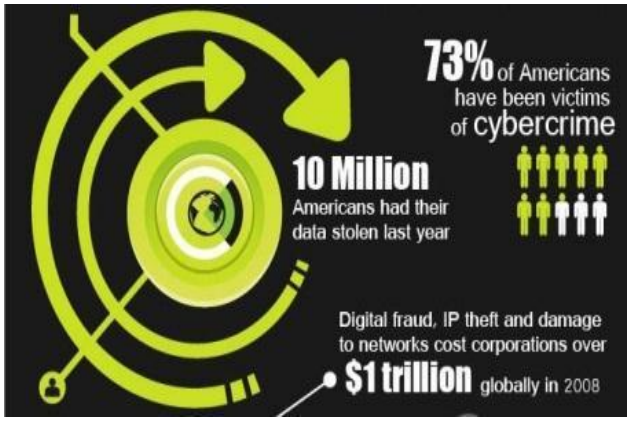

Figure 2.1 Cyber crime a challenging issue

2.2.1 Backdoors

A backdoor in an exceedingly automatic data processing system, a cryptosystem or associate algorithmic program, may be a methodology of overcoming traditional authentication, securing remote access, getting access to plaintext, whereas making an attempt to stay unobserved. A special type of uneven secret writing attacks, referred to as klepto graphic attack, resists being helpful to the reverse engineer even once it's detected and analyzed. The backdoor might take be associate put in program (e.g., Back Orifice), or may be a improvisation to associate existing program or hardware device. a selected type of backdoor may be a root kit, that replaces system binaries associated hook into the perform calls of an software to cover the presence of different programs, users, services. it's going to give wrong data concerning disk and memory usage.

2.2.2 Denial-of-Service Attack

Unlike different misuses, denial of service attacks isn't wont to gain unauthorized access or management of a system. They're really designed to render it unusable. Attackers will deny service to individual victims, like by deliberately coming into a wrong secret enough consecutive times to cause the victim account to be secured, or they will overload the talents of a machine or network and block all users without delay. These kinds of attack are tough to avoid, as a result of the full networks has to be analyzed, not simply tiny low items of code.

2.2.3 Direct-Access Attacks

An unauthorized user got physical access to a pc (or half thereof) will perform several functions or install differing kinds of devices to alternate security, together with software modifications, software package worms, key loggers, and listening devices. The wrongdoer may transfer massive knowledge onto backup media, like CD-R/DVD-R or transportable devices like flash drives, digital cameras or digital audio players. Another common methodology is also associate software cont ained on a fixed storage or different bootable media and skim the information from the exhausting drive(s) this fashion. the sole thanks to avoid this is often to write in code the storage media and store the key break away the system.

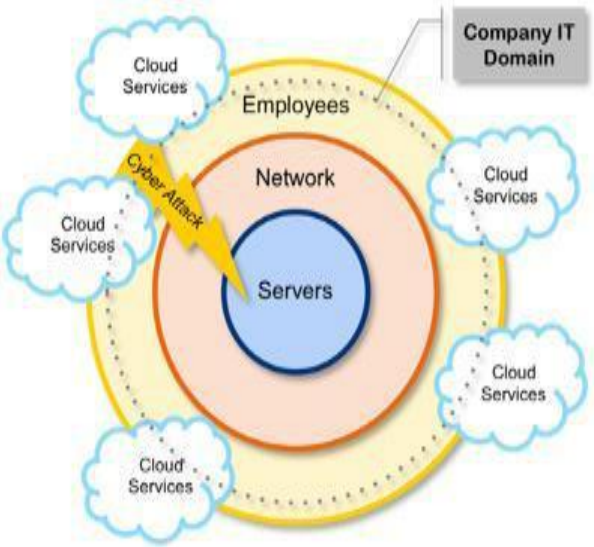

Figure 2.2 Cyber Attack criteria

2.3 Cyber Security Techniques

Cyber Security plays a crucial role in IT field. The dear data security had become one in every of the largest challenges within the gift day. Whenever consider the cyber security the primary factor that involves 'cyber crimes' that are increasing day by day. Not numerous measures cyber security remains a really massive concern to several. Numerous Governments and firms are taking several measures so as to forestall these cybercrimes. Not numerous measures cyber security remains a really massive concern to several. The following are a number of the techniques, are act as a preventing wall against attacks a couple of limit:

2.3.1 Malware Scanners

This is code that typically scans all the files and documents gift within the system for wrong code or harmful viruses. Viruses, worms, and Trojan horses are samples of malicious code that are sorted along and stated as malware.

2.3.2 Firewalls

A firewall could be a code program or piece of hardware that helps sort hackers, viruses, and worms that try and reach laptop over the net. All entities coming into or deed the net taste the firewall gift within the system , that check every message and blocks people who don't meet the desired security criteria. Firewalls play a crucial role in police investigation the malware.

Figure 2.3 Cyber attack trends

2.3.3 Anti-Virus code

Antivirus code could be a bug that detects, prevents, and takes action to disable or take away malicious code programs, like viruses and worms. Most antivirus programs embody auto-update feature that allows the program to transfer details of latest viruses so it will check for the new viruses as presently as they're discovered.

Figure 2.4 Cyber Security challenges in next 12 months

III. SYSTEM ANALYSIS

System analysis is that the method of gathering and analyzing acts, learning and victimization this info to supply enhancements to the system.

3.1 Existing System

The most essential tasks performed by a practicability Study are the identification and outline of candidate systems, the analysis of the prevailing systems and also the choice of the most effective one amongst them. The most effective system suggests that the system that meet performance and needs at the smallest amount price. The new system has no further expense to implement the system. The new system has blessings like quick access of files from any consumer within the Network, correct output for accurate input and this application ought to be a lot of users friendly. the appliance may be used not solely during a explicit firm, it ought to be ready to customize.

3.2 Separate coding before victimization

File Transfer Protocol Encryption of the information by a separate program before performing arts the transfer was in all

probability the primary technique accustomed solve this downside. Although this technique is instantly on the market, it doesn't solve all of the issues. This technique doesn't shield the user's word, therefore somebody attempt to get info on the transmission may get access to the information when it's been decrypted unless a separate mechanism is employed to limit the reusability of passwords. The need for manual coding may cause issues once the user is during a busy or discovers that there's a file that's required that wasn't encrypted before the transfer session was started.

3.3 Secure Shell File Transfer Protocol

Secure Shell File Transfer Protocol (SFTP) is wide on the market for variety of platforms and it solves the matter of securing the user's word and provides encryption and integrity on the fly. SSH conjointly authenticates the server concerned although the exchange of keys. SSH keys are in camera maintained and need external acceptance upon initial use or previous transfer through associate alternate technique

3.4 File Transfer Protocol over SSH

SSH may be accustomed produce a secure tunnel between 2 systems. It's doable to own one finish of this tunnel purpose to associate File Transfer Protocol server and supply a secure channel for File Transfer Protocol transfers. Some SSH servers and shoppers acknowledge the File Transfer Protocol PORT and PASV commands.

3.5 IP Security

IP Security (IPSec) provides secure communications (authentication, integrity, confidentiality) over IP-based networks between systems. Not all systems have IPSec on the market. Even once systems have it on the market, configuring differing kinds of systems to figure along may be a challenge. Since this must be designed on a per system basis it should lack flexibility once destinations or sources amendment oftentimes. Since IPSec protects the individual packets sent between nodes it will gift a controversy if one amongst the nodes is working behind a NAT device that doesn't support IPSec NAT traversal (RFC 3947, 3948). Relying upon however it's designed IPSec will offereach knowledge integrity and data security. If knowledge protection is desired, then it's necessary to put together IPSec to inscribe all traffic between the 2 systems as File Transfer Protocol could use associate absolute knowledge port for the transfer.

IV. PROJECT DESCRIPTION AND IMPLEMENTATION

The Secure File Transfer Protocol (SFTP), a more secured version of SSH FTP, is a WinForms application, in which software on one system communicate with software on another remote system. It prevents passwords and other sensitive information from being transmitted in the clear over the network. At the time of configuration the client has to be signup to the software. After that he can login to the software. The signup form is available only at the configuration time. The client can edit his signup details by the edit profile option. Before data transfer the client has to decide where the received file is to be stored. He can specify the default download location and the encrypted file download location. SFTP provides a file transfer mechanism which is much more secure than other encryption techniques.

Here the client can send files directly to the remote systems or in an encrypted form. In an encrypted transfer, the file content is encrypted by a private key. A private key is nothing but a 32 byte key generated from the client's personal information. The client has no role in the generation of private key. It is automatically generated by the software. In order to decrypt the encrypted file the target machine has to know the encryption key. So, the key has to be transferred along with the encrypted file. Therefore the key used for encryption is again encrypted by a software key. Software key is generated by the software itself. It will always be static. Here the software key and the sender's private key are hided from the clients so that it can provide more security to the file which is to be transferred. At the recipient, whenever a file is received a popup message is shown at its taskbar. The encrypted file can be decrypted at the time of its arrival by entering the client's login password. After that the file is automatically disposed.

To secure a specified file, SFTP provides file locking facilities. File locking means preventing access to a specified file in one client's system from other clients. This facility is implemented using cryptographic techniques. Once a file is locked it cannot be accessed by other clients. A locked file can be view by a client during searching operations in an inaccessible mode. If the client needs to share his locked file he can unlock it. Another feature of SFTP is file search. During file search, a client can search for a specified file or can list the entire files in a specified remote system. He can open the required file after completing the file search operation.

Another feature of SFTP is screen sharing. Screen sharing means sharing the screen of one client machine to other clients. Here screen of a client is considered as a file. This feature is most suitable for class rooms, conference rooms etc.

4.1 Module Description

A module description provides detailed information about the module and its supported components, which is accessible in different manners. The included description is available by reading directly, by generating a short html-description, or by making an environment check for supported components to check if all needed types and services are available in the environment where they will be used. This environment check could take place during registration/installation or during a separate consistency check for a component. SFTP has the following Modules:

4.1.1 Sign Up Module

At the time of software configuration on a system, the client has to sign up with his credential details. This sign up Form appears only at the time of configuration. SFTP saves the client details at the application settings of the software. After sign up, the client can login to the software.

4.1.2 Login Module

After sign up, the client can login to the software with his username and password. If the login is successful, the client can perform the operations provided by SFTP. Otherwise an error message will be displayed.

4.1.3 File Search Module

In the File Search module, the client can search for a particular file in his system or in a particular remote system. During the search process the related files are listed. After the completion of file search the client can open the required file with the help of a context menu. The client can list the entire files in a remote system with the help of remote file search.

4.1.4 File Transfer Module

In the file transfer module, the client can transfer files into a selected set of remote systems either directly or in an encrypted form. If the client opts for an encrypted file transfer, the file content is encrypted and is transferred through the network with its encrypted secure key. Whenever the file reaches the destination a popup message is displayed at the taskbar, and the recipient is asked to enter his login password for decrypting the file. He has an option to give the password three times. If he is failed to give his password, then the received encrypted file is automatically discarded from the system. Otherwise he can open the encrypted file in its original form.

4.1.5 File Lock and Unlock

SFTP can secure a specified file in a remote system by locking it. Locking means preventing access to open, move, modify, or to delete a file. If the client needs to share a locked file, then he can unlock it. Here locking and unlocking is done by cryptography techniques.

4.2.6 Screen Sharing Module

SFTP provide two way interactive screen sharing in which the screen of one client can be view by the selected remote systems. This feature is helpful for class room discussions and conferences.

4.3 Data Flow Diagram

The data flow design provides a systematic approach for the derivation of program substructure, the global view of the software and the under pinning of the architectural design. Beginning with the fundamental system model, information may be represented as a connection flow. Data flow oriented design defines a number of different mappings that transform the information flow into program structure. Data flow diagram is used to define the flow of a system and its resources such as information. It is a way of expressing system requirements in a graphical manner. It represents most of the important tools used for structured analysis. A data flow diagram is also known as a bubble chart. Data flow diagram at the simplest level is referred to as the context analysis diagram. These are expanded by level, each explaining its process in detail. Processes are numbered for easy identification and are normally labeled in block letters.

In SFTP, the client has to sign up at the time of software configuration with his credential details. This information is stored in the software application settings. After sign up, the client can login to the software with his username and password. If the login fails, then an error message is displayed. After successful login, the client can perform the required operations provided by SFTP. These include file transfer, file search, file lock and unlock, and screen share. During file transfer, the client has given two options, direct transfer and encrypted transfer. Direct transfer is suitable for regular files. Encrypted transfer is suitable for secure files. If the client chooses encrypted file transfer the file is encrypted with a private key. This key is again encrypted with a static software key and is transferred along with the encrypted file. This key is used to decrypt the data at the receiver side.

During file search, the client can search for a specified file or he can list the entire files in a remote

system. After completing the file search, he can open the required file from the list. File Lock is a mechanism which is used to provide security to a specific file. It is performed by the cryptography techniques. After a file is locked no one can access and modify it. If the client needs to share a locked file, he has to unlock it. During screen sharing, a client can share his screen as a file to a selected list of remote systems.

If a user want to use this particular software, just like many of other software have to install it first. At the time of software configuration on the system, the client has to sign up with his credential details like his name, address, username, and password. This Sign up Form only appears at the time of configuration and from the user details system itself generates users private key used for the encryption. The user details gets concatenated and will encrypted by TripleDES algorithm with client machine name as key, after that the encrypted content hashed with MD5 algorithm to convert it into 24 bytes. This 24 byte key will stored in the application settings as the user's private key, it is hided from the user.

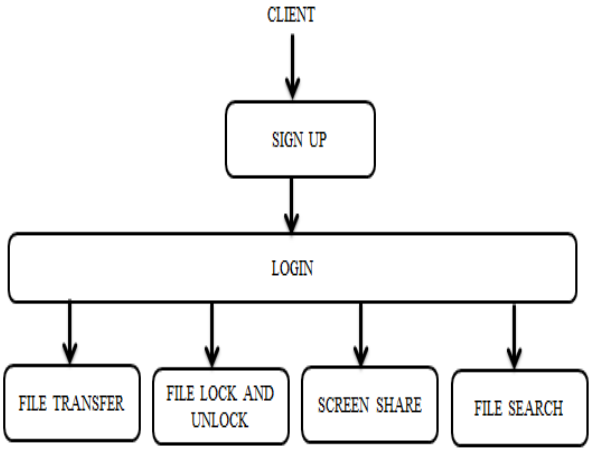

Figure.1 Module Description

When the client gets signed up the details will be stored in application settings. Also the software make uses a static software key for providing security in file transfer, which is also hided from the application users. After client gets signed up he can login to the software with the username and password given at the time of Sign Up. The details will be authenticated by the application settings. If the login is successful, the client can perform the operations provided by SFTP like file search, file transfer, file locking, screen sharing etc. Otherwise an error message will be displayed, so have to login with the correct username and password.

Files of the client system as well as from the remote system can be searched and list it. The user should enter the file to be searched and the client machine, from where it to be searched, after that the files on the same format will be listed. If the client wants to open any of the listed files it will temporarily store in the system and can open it. But it will open for little time, whenever the user logout from the application the file opened will be deleted.

The user can transfer files into the selected remote system with or without encryption. In the encrypted file transfer the file contents is encrypted and is transferred through the network with its encrypted key. The file transfer without encryption can simply do by browsing the file from the system and selecting the receiver systems. But in case of file transfer with encryption the application encrypts the file content with the user's private key available from application settings, and private key also encrypted with software key. Encryption algorithm used here is Triple DES. The file content with the encrypted personal key sends to the selected clients. At receiver side the private key automatically decrypted by software key, and if the user of the receiver system gets authenticates by application settings then the file will decrypted can access it, otherwise the file received be discarded.

The Data Flow diagram for SFTP is follows:

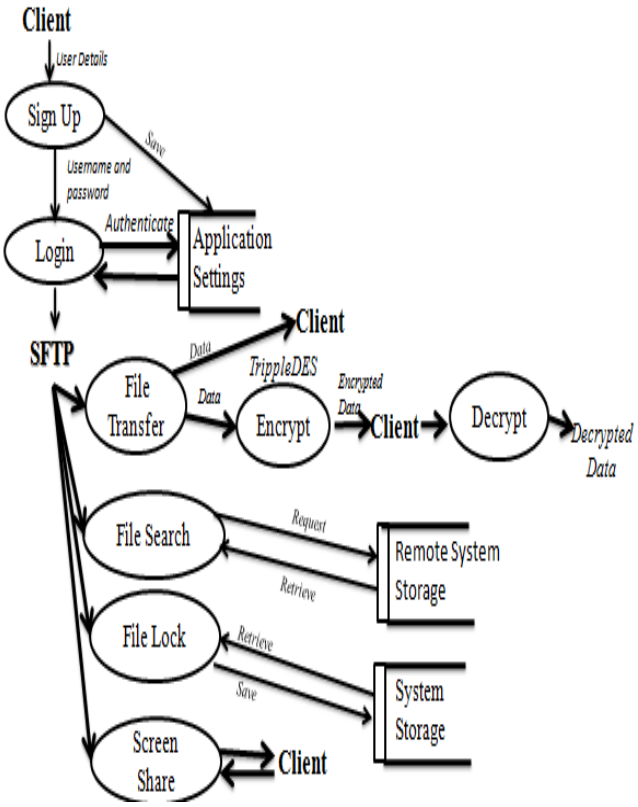

Figure.2 Data Flow Diagram

SFTP can secure the files on the client system by providing encryption. Then the locked file by encryption will be in its same location but it can't edit, delete, rename, or copy etc., and those locked files stored in a default temporary lock for easy access of the list of file to be unlocked. The unlocking done by decryption and that file gets deleted from the list locked files. Also the unlocked file again enabled for the operations like delete, rename, copy, edit etc. SFTP provide interactive screen sharing in which the screen of one user system can be view by the selected remote systems, also the remote system screens is also visible to user. The images of the user system screen will be taken and rendered to display the screen on the remote system and vice versa. The changes made by the user will be visible to the remote system at the same moment.

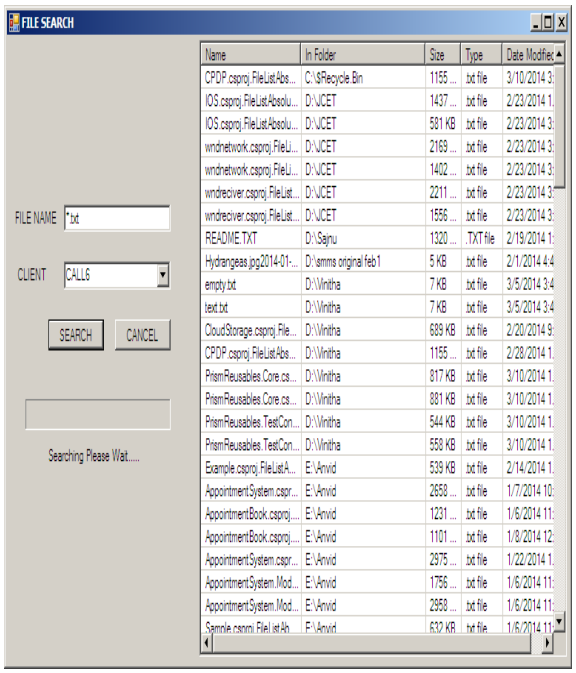

Figure.3 File search

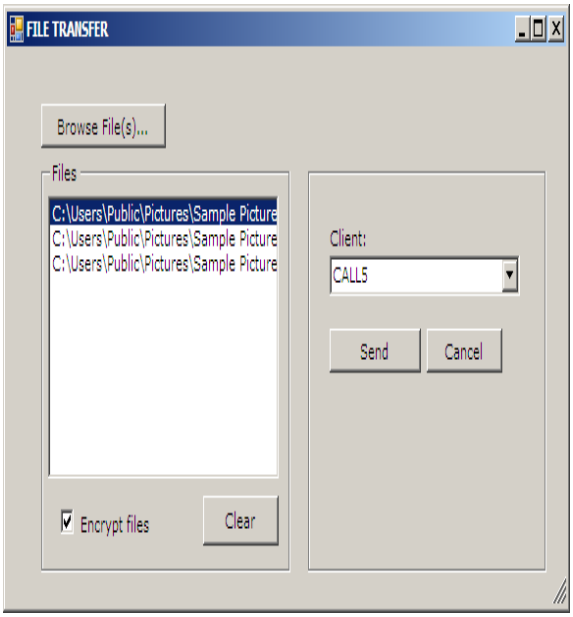

Figure. 4: File Transfer

4.4 Result and Discussion

4.4.1 File Search

The user can enter the file to be searched on the file name text box, and can select from where it to be searched by selecting a client from combo box. On search button click the file searched from the selected client machine and it details displayed on list box, also progress bar enables according to the entries in list box. While searching on cancel button click the searching gets suspended, and progress bar disabled. If user want to open any of the file on the list box entries, can open it by selecting and right clicking. But it will open for little time, whenever the user logout from the application the file opened will be deleted. When user tries to search another file the list box cleared for the new search items, and the progress bar enabled. If all the files of the selected format are displayed on the list box, will inform the user that file search has been completed.

4.4.2 File Transfer

This is the form for file transfer. Here the user can browse the files by clicking the browse button and the selected files will be displayed on the list box. The client, to whom the file to be transferred selected from the combo box. To check whether the files transferred with or without encryption a check box is used. When click on the send button the files transferred to the selected clients with or without encryption according to the check box value.

V. MORE ENHANCEMENTS

SFTP can be implemented in a wired network system or a wireless network system. Setting up a wired network is more costly since it requires

additional LAN Connectors and cables. With the help of a wireless network we can reduce the hardware cost. But the software requirements are still there. SFTP is a secure file transfer protocol in which software of one remote system can communicate with the software of other system. Hence, software implementation cost is there. In order to reduce the cost of implementation we can configure SFTP along with Wireless USB. With this we can increase the flexibility. Wireless USB is a short-range, high-bandwidth wireless radio communication protocol created by the Wireless USB Promoter Group. Wireless USB is sometimes abbreviated as "WUSB", although the USB Implementers Forum discouraged this practice and instead prefers to call the technology Certified Wireless USB to distinguish it from the competing UWB standard.

VI. CONCLUSION

Secure File Transfer Protocol is an intranet-based application which provides a more secure file transfer mechanism. Here encryption is done by the software itself. Therefore, the client has no role in encryption and decryption. SFTP automatically encrypts the file during file transfer and automatically decrypts the encrypted data at the receiver side. One of the important features of SFTP is that it provides key encryption. During encrypted file transfer, the file is encrypted by a private key. The private key is generated by the SFTP itself from the client's sign up information. In order to decrypt the encrypted file the sender has to inform the receiver about the key. So the private key is transferred along with the encrypted file. Here we secure the private key by encryption. That is, the private key is encrypted with a static software key. So, the receiver can easily decrypt the data with this key. Thus the encrypted transfer is comparatively faster than that of SSH FTP. SFTP provides file locking and unlocking mechanisms to make a file more secure. This is done by cryptography. Locked files are not available for modification. Another feature of SFTP is screen share. Screen share means sharing of screens between remote systems.

REFERENCES

[1] [Bha17] A Bhavana Daddala, Hong Wang, Ahmad Y Javaid, Design and Implementation of a Customized Encryption Algorithm for Authentication and Secure Communication between Devices, 2017.

[2] [Bha16] Bhavani Thuraisingham et al., Tim Finin et al. and Elisa Bertino et al., IEEE International Conference on Data Driven Approach for the Science of Cyber Security: Challenges and Directions, 2016

[3] [Cad12] T Cadenhead, V Khadilkar, M Kantarcioglu, B Thuraisingham, A cloud-based RDF policy engine for assured information sharing". SACMAT 2012.

[4] [Cam03] C Camerer, Behavioral Game Theory: Experiments in Strategic Interaction", Princeton University Press, 2003.

[5] [Car12] R Carmona, F. Delarue, A Lachapelle, Control of McKean-Vlasov Dynamics versus Mean Field Games, Working paper, 2012.

[6] [Che03] H. Chen et al. An ontology for context-aware pervasive computing environments. The Knowledge Engineering Review 18, 2003.

[7] [Che04] H. Chen. An Intelligent Broker Architecture for Pervasive Context-Aware Systems. PhD thesis, Univ. of Maryland, Baltimore County, Dec. 2004.

[8] [Chen14] Chen et al. Samsung: Knox Security Gap Not Specific to Galaxy Devices Wall Street Journal Digits, New York, NY, USA. Jan. 2014.

[9] [Cyb12] Cybersecurity IDS ontology. http://ebiquity.umbc.edu/ontologies/cybersecurity/ids/.

[10] [Dai08] C. Dai, D. Lin, E. Bertino, and M. Kantarcioglu, An Approach to Evaluate Data Trustworthiness Based on Data Provenance, Proc. of the 5th VLDB Workshop on Secure Data Management, Auckland, New Zealand, Aug. 2008.

[11] [Dea08] J. Dean and S. Ghemawat, MapReduce: Simplified data processing on large clusters, Communications of the ACM, 2008.

[12] [Dal13] Dallas et al., TX, USA. How Secure is Mobile Device Management Anyway, Apr. 2013.

[13] [Dal13]Dallas et al., Cloud Security Alliance, How Secure is Mobile Device Management mobile-device-management t-anyway, Apr. 2013.

[14] [Fre12] J. Freire, P. Bonnet, and D. Shasha, "Computational Reproducibility: State-of-the-Art, Challenges, and Database Research Opportunities," Sigmod'12, May 20-24, 2012, AZ.

[15] [Gar12] S. Garfinkel et al., A. Nelson et al., and J. Young et al., A General Strategy for Differential Forensic Analysis: http://www.journals .elsevier.com /digit al-investigation , 2012.

[16] [Hug13] J. Hughes et al. and G. Cybenko et al., Quantitative metrics and risk assessment: The three tenets model of cyber security, Tech. Innovation Manage., Aug. 2013.

[17] [Kel14] Kelce s. Wilson1 et al. and müge ayse kiy2 et al., IEEE Transactions on Some Fundamental Cyber security Concepts 2014.

[18] [Nsa11]http://www.informationweek.com/news/government/cloud -saas/229401646

[19] [Sef13] G. Seffers, Committed to Cloud Computing, SIGNAL Magazine, October 2013.

[20] [Ste13] Stern stein et al., Pentagon Disconnects iPhone, Android Security Service, Forcing a Return to BlackBerry for Some, Dec. 2013.

[21] [Wil13] K. Wilson et al., Conflicts among the pillars of information assurance," IEEE IT Prof., vol. 15, no. 4, pp. 44_49, Jul/Aug. 2013.

[22] [Liu10] Liu Xia et al., Design of Secure File Transfer Protocol system, published in Communications, Circuits and Systems (ICCCAS), International Conference 2010.

[23] [WuY13] Wu Y, Chen X C et al., File Transparent Encryption System Design Based on Security Directory[J]. Applied Mechanics & Materials, 2013, 433-435:1742-1746.

[24] [Xia09] Xiaosong Zhang, Fei Liu, Ting Chen, Hua Li et al., Research and application of the transparent data encryption in intranet data leakage prevention[C].Proceedings of the 2009 International Conference on Computational Intelligence and Security, 2009: (vol.2) 376-9.

[25] [Zha09] Zhang Xiaosong, Liu Fei, Chen Ting, Li Hua et al., Research and Application of the Transparent Data Encpryption In Intranet Data Leakage Prevention, 2009 International Conference on Computational Intelligence and Security