IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified

Vol. 5, Issue 11, November 2016

Design of Secure File Transfer over Internet

Akanksha Srivastav[1], Ajeet Bhartee[2]

Department of Computer Science, Galgotia's College of Engineering and Technology, Gr. Noida[1, 2]

Abstract: Due to the recent innovations in the internet and the network applications and the wide spread of internet and networks, it is now completely possible to conduct electronic commerce on the internet or through the local area networks, and the wide spread of computer and communication network promoted many users to transfer files and sensitive information through the network, this sensitive data requires special deal. This work presents a security system that can provides privacy and integrity for exchanging sensitive information through the internet or the communication networks, based on the use of recently developed encryption algorithms, such as AES, IDEA and RSA. The aim of the work is to develop a simple file transfer system that can obtain privacy, integrity and authentication for the file transfer process. The proposed system uses symmetric cryptography system. File transfer must provide end-to-end visibility, security and compliance management.

Keywords: Cryptography, Encryption, Decryption, Network Security, File Transfer.

I. INTRODUCTION

As a lot of confidential data are being transferred day in day out to/from the companies, there are possibilities that the data may be lost accidently or stolen intentionally. This is not reliable as it could be a serious threat to the organizations. The project is an application to make sure that the data being transferred over the Internet is secured and confidential. It is very important that this data being transferred does not fall into wrong hands to avoid any financial or informative losses that can be harmful to the organization. Moreover, the storage of the data and its transfer are accessed by the authorized persons only hence providing a secure way to manage and transfer.

II. THE PROPOSED SYSTEM

The secured file transfer over the Internet is an effort which aims at providing security to the files being transferred over the Internet. The user is assured about the fact that no unauthorized person can access the file and misuse the information in the file. This project after development can be used for any type of enterprise need to transfer their files from one place to other at right time to the right person. This project after development can be used for any type of enterprise need to transfer their files from one place to other at right time to the right person. It requires active internet connection, without it the file would not be transferred. It can be used by any type of enterprise and businesses with little modification. This project can be made in such a way that, individual. Enterprise need not be given individual copies but single software on a server can be used by multiple enterprises.

Even if the file goes to the wrong person, he will not be able to access the data from that file because of the encryption and decryption strategy. An organization has to register to use this application. The activation will be done after the registration by e-mail validation. There would be session management, profile management. Private key generation (saved by user) and public key generation (stored on user profile). There would also be File Upload & encryption with symmetric encryption, key to be sent via e-mail, online file storage, list for users to select file/share recipient, notification to download via e-mail, add/delete/edit metadata for files, resharing of files uploaded multiple times.

One to one file transfer would simply consist of the sender uploading the file on the server with encryption and using its own private key and the recipient's public key. The recipient will then decrypt the file and use its private key and sender's public key to download it from the server.

III. USED ALGORITHMS AES (ADVANCED ENCRYPTION STANDARD)

In present day cryptography, AES is widely adopted and supported in both hardware and software. Till date, no practical cryptanalytic attack against AES has been discovered, AES has been discovered, AES built in flexibility of key length, which allow a degree of future – proofing against process in the ability to perform exhaustive key searches.

AES ALGORITHMS-
AES is a cipher ie a method for encrypting and decrypting information, whenever you transmit file over secure file transfer protocol like, HTTPS, FTPS SFTP, webDAVS. AES either use- 128, 192, 258.

AES belongs to the family of cipher known as block cipher. A block cipher is an algorithm that encrypts data as per block basis .the size of each block usually measured in bits.

AES require the use of key during the encryption and decryption process. AES support three key with strength

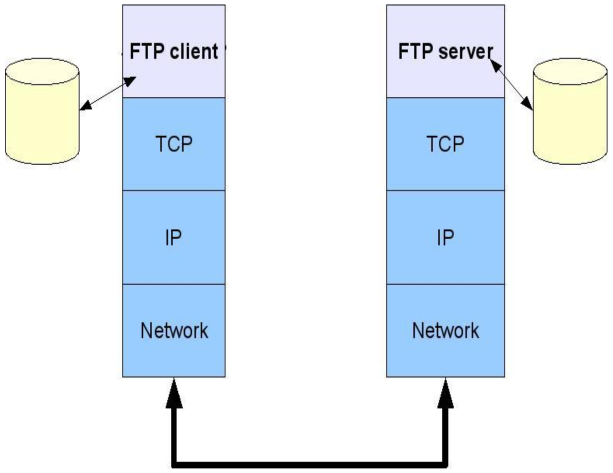
DOI 10.17148/IJARCCE.2016.511101

support -128, 192, 258. The longer the key stronger the encryption so AES 128 is least strong while AES 258 is strongest .encryption process during a typical secure file transfer secured by SSL/TLS.

IV. USED PROTOCOL

In this proposed work we use the FTP protocol. The File Transfer Protocol (FTP) is a standard network protocol used to transfer computer files between a client and server on a computer network. FTP is built on client-server model architecture and uses separate control and data connections between the client and the server.

The two mainstream protocols available for Secure FTP transfers are named SFTP (FTP over SSH) and FTPS (FTP over SSL). Both SFTP and FTPS offer a high level of protection since they implement strong algorithms such as AES and Triple DES to encrypt any data transferred.



V. ENCRYPTION/DECRYPTION

ENCRYPTION- In cryptography, encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption does not of itself prevent interception, but denies the message content to the interceptor.

In an encryption scheme, the intended communication information or message, referred to as plaintext, is encrypted using an encryption algorithm, generating cipher text that can only be read if decrypted. For technical reasons, an encryption scheme usually uses a pseudorandom encryption key generated by an algorithm.

It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, large computational resources and skill are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients, but not to unauthorized interceptors.

TYPES OF ENCRYPTION-

Symmetric key encryption-In symmetric key schemes, the encryption and decryption keys are the same. Communicating parties must have the same key before they can achieve secure communication

Asymmetric key encryption- In asymmetric key schemes the encryption and decryption keys are different one is private other is public.

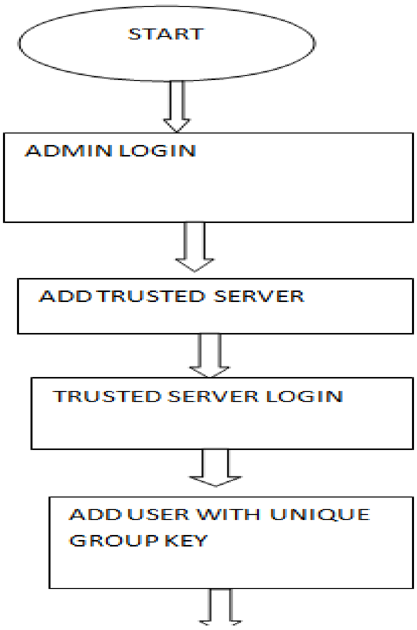
DECRYPTION- Decryption is the process of transforming data that has been rendered unreadable through encryption back to its unencrypted form.

In decryption, the system extracts and converts the garbled data and transforms it to texts and images that are easily understandable not only by the reader but also by the system. Decryption may be accomplished manually or automatically. It may also be performed with a set of keys or passwords.

VI. CONCLUSION

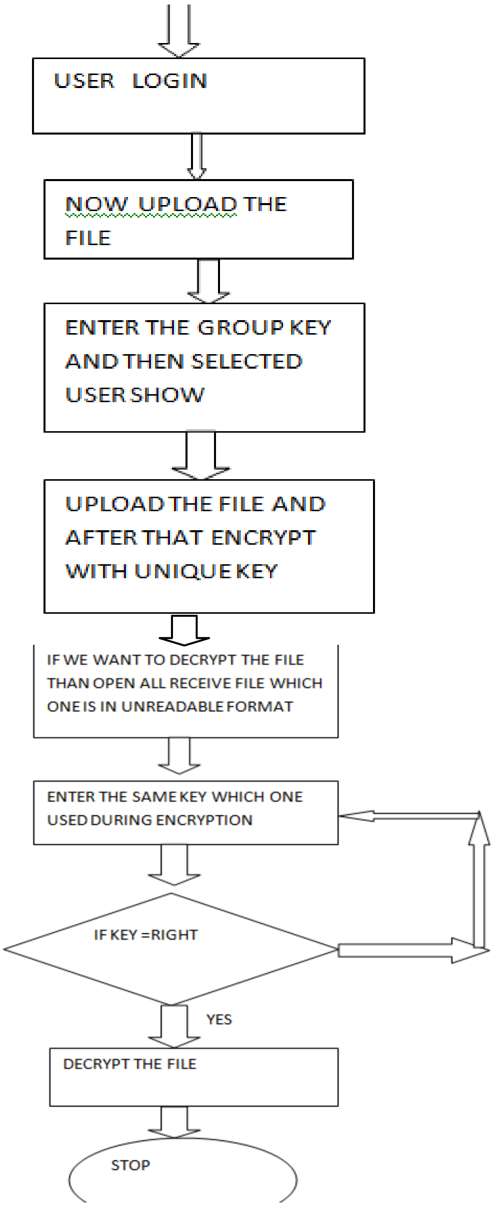
Here in this we send the file from one computer to other, file transfer with encrypted form. The entire computer connected through one server and we can share file and even access file from other computer through PC folder. In this research when we login then the main issue is the key. If we press wrong key three times then admin blocked that user. So always remember the key given at the login time. In this add security during file transfer after uploading the file first encrypt and after that decrypt the file for showing the receive data. And through Pc folder we can access files from different connected computer

FLOW CHART



Copyright to IJARCCE

DOI 10.17148/IJARCCE.2016.511101


USER LOGIN
NOW UPLOAD THE FILE
ENTER THE GROUP KEY AND THEN SELECTED USER SHOW
UPLOAD THE FILE AND AFTER THAT ENCRYPT WITH UNIQUE KEY
IF WE WANT TO DECRYPT THE FILE THAN OPEN ALL RECEIVE FILE WHICH ONE IS IN UNREADABLE FORMAT
ENTER THE SAME KEY WHICH ONE USED DURING ENCRYPTION
IF KEY =RIGHT
YES
DECRYPT THE FILE
STOP

REFERENCES

[1] P. Ford-Hutchinson. Securing FTP with TLS. Internet Draft (RFC 4217), 2005.

[2] Analytical framework for measuring network security using exploit Dependency graph by P. Bhattacharya, SGhosh(2012).

[3] Secure file management system over internet by Hua Zhang, Jun – Fen Diao, Qiao – Yan Wen, university of posts and telecommunication (2008)

[4] Secure File Sharing in JXTA using Digital Signature – Erita Skendag, Marenglen Biba – University of NY Tirana(2012)

[5] Information security of Remote File transfer with mobile Devices – Sami Noponen, Kaarina Karppnen(2008)

[6] Moving towards network security and firewalls for protecting and preserving private resources on Internet by Dr.S.S. Riaz Ahmed(2008)

[7] H. B. Pethe and S. Pande, "A Survey on Different Secret Key Cryptographic Algorithms," IBMRD's Journal of Management & Research, vol. 3, pp. 142-150, 2014.

DOI 10.17148/IJARCCE.2016.511101