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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

SECURED FILE MANAGEMENT OVER INTERNET

Prof. Balasaheb B. Gite[1], Shailesh Navghare[2], Abhishek Gupta[3], Siddharth Jain[4]

Department of Computer Engineering, Sinhgad Academy of Engineering, Pune[1,2,3,4]

Abstract—Today's economy is increasingly based on information flow. Getting the right information to the right person at the right time is the key strategy for secured file transfer. It is critical that the execution of this strategy ensures that the storage and transfer of information is reliable and secure. File transfer must provide end-to-end visibility, security and compliance management. A secure and managed file transfer approach can help the user to meet the challenge of safely and reliably exchanging electronic information. The purpose of this project is to present an online platform to manage and share files. Different categories of users use various medium to manage and transfer files over internet. The project presents a solution so that users can communicate and exchange the important files in a secured way. The abstract presents Secured File Management and Sharing System over the internet developed using the J2EE technologies.

Keywords—primary key; public key; cryptography; digital signature; encryption; decryption

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 dataand its transfer are accessed by the authorized persons only hence providing a secure way to manage and transfer.

II. SCOPE

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, re-sharing 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. EASE OF USE

The user has to register first for transferring the file. The activation is done through a simple e-mail validation. Every user has a private key and a public key. Private key is stored by user and not on the server and public key is stored on the user profile. Files are transferred either in a symmetric way or asymmetric way.

For symmetric file transfer the sender should encrypt the file using its private as well as public key. The

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

receiver should know the sender's private key and its public key to download and decrypt the file.

For asymmetric file transfer the sender will have to encrypt the file and the receiver will download and decrypt the file using the same key.

The options to see the file upload details, to add the recipients, to delete the recipients are very easy to implement. Re-sharing of same file to other recipients has been made easy.

IV. SYSTEM FUNCTIONALITY

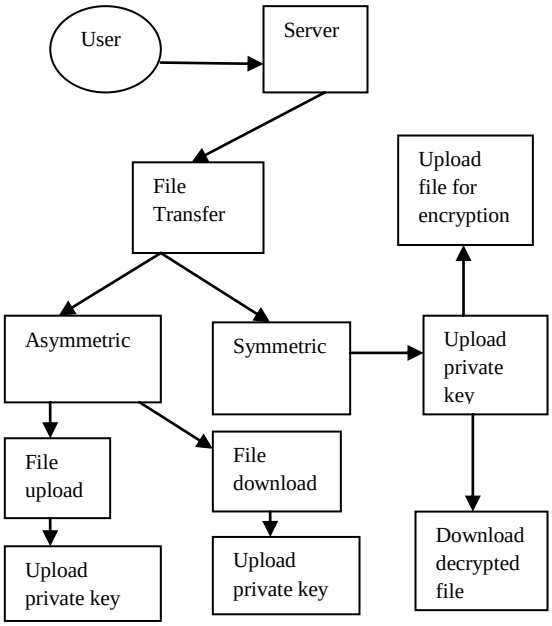

Fig.1 block diagram of system

A. Encryption and Decryption

This system is based on the 3 pillars of information security- Confidentiality, Integrity and Availability. The digital signature used here protects the integrity and authenticity of a message. However other techniques are still required to provide confidentiality of the message being sent. Encryption is the process of transforming information (referred to as plaintext) using an algorithm (called a cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The result of the process is encrypted information (in cryptography, referred to as cipher text).

In many contexts, the word encryption also implicitly refers to the reverse process, decryption, to make the encrypted information readable again (i.e. to make it unencrypted). For this project uses inbuilt package **'javax.crypto'**

To provide higher integrity and confidentiality project uses both the digital signature and encryption mechanisms. The document is digitally signed by the sender as well as the document is encrypted.

B. Generate Private and Public Keys:

The key pair generator class is used to generate pairs of public and private keys. Key pair generators are constructed using the getInstance factory methods. These are static methods that return instances of a given class. The key pair generator for a particular algorithm creates a public/private key pair that can be used with this algorithm.

C. Digital Signature

A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit. Any data/document which is sent through the system will require the sender to digitally sign the data before sending.

In the project, the sender uses its private key(Signing key) to digital sign the document or file. To authenticate the originator of the transfer the receiver uses the public key (authenticating sign). This allows the recipient to also check whether the data has been tampered during the transit.

D. Equations

Sign The Data:

The digital signature is created or verified using an instance of the signature class.

Signature dsa = Signature getInstance("MD5withDSA", "SUN");

DSA is a digital signature algorithm while MD5 is a message digest algorithm which is the message digest algorithm.

E. Verify The Signature:

Once all the data is supplied to the signature object, one can verify the digital signature of that data and report the result. Suppose that the alleged signature was read into a byte array called sigToVerify.

Boolean verifies=sig.verify(sigToVerify);
System.out.println("signature verifies : " + verifies);

The verified value will be true if The alleged signature(sigToVerify) is the actual signature of the specified data file generated by the private key corresponding to the public key.

V. USING THE APPLICATION

Security over the exchange of electronic information has been a concern since the invention of the same. Till date there have been many algorithms allowing security to the files being exchanged over Internet. These algorithms have their own set of advantages and disadvantages.

Generally the algorithms provide security by providing password to the files. This allows them to

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

protect the data in plain text. The receiver should know this password to access the data in the file. These files are vulnerable to the threats from the hackers. There is hardly any difficulty for the interpretation of the data thereafter.

This project uses the idea of encryption and decryption whereby the file being transferred is converted into non readable format. The receiver will then use a specific key or a combination of keys to convert it into readable format. Thus the hacker won't be able to decipher the text. This peculiarity enhances the security level to a great extent.

VI. CONCLUSION

The project plan discussed in the previous section gives a clear perspective that Secured File transfer gives a simple way to exchange files with security and integrity of the data maintained.

ACKNOWLEDGMENT

The authors would like to thank Department of Computer Engineering and indebted to our guide and HOD Prof. B. B. Gite (Department of Computer Engineering) for his guidance and sagacity without which this IEEE paper would not have been designed. He provided us with valuable advice which helped us to accomplish the design of IEEE paper. We are thankful to him for his constant encouragement and moral support.

Also we would like to appreciate the support and encouragement of our colleagues who helped us in correcting our mistakes and proceeding further to produce the paper with the required standards.

REFERENCES

[1] Secure file management system over internet by Hua Zhang, Jun – Fen Diao, Qiao – Yan Wen, university of posts and telecommunication (2008)
[2] P2P applied for CMS for advertising by Oliver Batz,Carston Kleiner-Arnekosehel FH Hannover – University of App. Sci and Arts(2009)
[3] Secure File Sharing in JXTA using Digital Signature – Erita Skendag, Marenglen Biba – University of NY Tirana(2012)
[4] Information security of Remote File transfer with mobile Devices – Sami Noponen, Kaarina Karppnen(2008)
[5] Network Traffic Monitoring Using Intrusion Detection System by Prof. Radha S Shirbate ,Prof. Pallavi Patil(2012).
[6] Analytical framework for measuring network security using exploit dependency graph by P.Bhattacharya,S K Ghosh(2012).
[7] Moving towards network security and firewalls for protecting and preserving private resources on Internet by Dr.S.S. Riaz Ahmed(2008)
[8] Research On File transfer task scheduling method Ingrid environment by wenshung wang, Nengfu Xie
[9] Three Tier encryption algorithm for secured file transfer by Bhargav balakrishnan(2010)
[10] Design and implementation of file transfer and web service guard employing cryptographically secured XML security labels by Andreas Thunnel, member,IEEE and Knut Eckstein(2006).