Multiple File Storage Server To Improve Data Security

A.Praveen[1], R.Raja Vijaya Kumar[2], M.Samuel[3], S.Vimal[4], M.Vaidhehi[5]
[1, 2] Department of Computer Science and Engineering
[1, 2] Saranathan College of Engineering

Abstract- *As we have seen so many software's related to data security which provides security to data by storing it in a server with a password or by storing the data in multiple servers, in the above scenario, there may be chances of hacking the particular server for information extraction. In this case, there is no security for the data. In our proposed system we are rectifying this problem by splitting the data we want to store into three parts and storing it in three different servers. And it can be retrieved back into a single file if we want. Here we are using three different servers to store three parts of data, if the hacker hacks a server he/she will get only the single part of the data it is useless unless he/she gets the other two parts of the data. Thus, our software provides security to data we want to upload.*

Keywords- Data Security, Split and merge, Upload, Download

I. INTRODUCTION

In this chapter, the main aims, objective, importance and contents of the project are illustrated in details.

"Data Security" is an important domain that must be concentrated today as internet is growing in every aspects of human terminology. Everything we do on the internet leaves us with a high risk in terms of our privacy where information extraction, hacking, and information stealing is becoming more and more common nowadays. We must secure our data in order to avoid the above situations.

Securing the data is a important thing where there are chances of intruders stealing the file. To overcome this many data security methods are used to store the files safely i.e. the file would be hack proof. They use several encryption methods such as AES, DES, Digital Signature, etc. where these technologies read the file and encrypt it using a particular algorithm and store it in a single server. If we download those files the technique will decrypt it using a particular algorithm and it will bring back the original file.

There are different types of computer files, designed for different purposes. A file may be designed to store a picture, a written message, a video, a computer program, or a wide variety of other kinds of data. Some types of files can store different several types of information at once. Having important files on your computer is certainly something that everyone does but it seems like people do not know how to take care of them. You will find that people will rarely secure their files and then go through the pain and stress of getting leaked their files in Social Medias and various forums. This is something that most people ignore yet they complain once it happens to them. There are several reasons why it is crucial to secure your files and to make sure that you always stored it safer.

Uploading is an activity used to store a file in the internet which is backup operation. Once Uploading is an activity used to store a file in the internet which is backup operation. Once we upload a file it will be stored in a single server if we want to download or see the file we uploaded a request will be made to the server and the server in response will retrieve the file. If the server fails there may be chances of losing the data. Using the encryption techniques we can encrypt our files and store it somewhere but what if someone hacks the particular server and steals all our files. What if we use use multiple servers to store the same data still the hacker can steal the file from any one of the server. What if we split the file and store in several servers.

II. SPLIT AND MERGER MECHANISM

1. Algorithm

The split and merge algorithm that we have used in this application is unique and this algorithm is what makes this application more secure than the traditional server applications. Here while splitting the file is taken in an ByteArrayOutputStream class and the file is represented in bytes. For example a file that is of size 8 bytes is taken in a byte array of length 8 each containing only one byte. Now three files will be created and the writing process starts.

The first byte of the file will be writed to the first file that is created and the second byte to the second file and the third byte to the third. For example take the 8 byte file. The Bytes 0,3,6 will be written to the first file. The bytes 1,4,7 will be written on the second file and the bytes 2,5,8 will be written on the third file. So each file will be read as a corrupted file if it opened individually. This is how the splitting mechanism takes place on the clients end.

2. Existing System:

The current existing traditional systems will store all the files on the single server. The client will request the server for the file or it will upload the file to the servers. While uploading the file to the server encryption and decryption is being done on the client side or the server side or both. The server will be equipped with traditional security feature that is the firewall. The only improvement that is available for the system is to build a strong firewall. Then the client will establish a connection to the server and the client will then request for the file or upload the file to the server. The server will then accept the connection if all the connections are from a valid client.

The single server will then start to accept all the requests from the client. Single server is responsible for the file transfer, file storage and for the deletion of the file from the server itself if the user specifies a delete request.

No modifications to the file other than the file encryption will be done to the files. Other than that the file will be as a whole. Once the file operations have been done then the connections will be closed on the client and the servers will the stop the connection.

Limitations:

- To improve the security for the files there is only one way that is to improve the firewall. No other method can be used to improve the security to the files.
- All of the files will be present on one server where successful hacking of that one particular server will serve all the files in that server can be extracted.

3. Proposed System:

The system that we propose will have three dedicated servers. Here file will be separated into three parts. Each part will be uploaded to its own dedicated servers. The file will be encrypted by splitting the file itself. The splitting of the files will be done by a special split and merge algorithm where each file will be splitted equally with the bytes in a random manner.

In our system three file servers will be up and running. So the client will be sending requests to all the three file servers. Each file server will be numbered such as server 1, server 2, server 3. The file splitting will be done only on the client side. In upload request after the successful splitting of the files each of the files will be sent to each of the servers. Each server will be waiting to accept the connection from the client. While processing a request the server checks if the client is valid. If the client is valid then the server will start to accept all the requests from the client. All the servers will now store all the files in its Memory.

To retrieve a file that is already uploaded a receive request will be sent to all the three servers simultaneously. Then all the three servers will process the request and will get ready to send the file. The servers will then send the file to the client. Three parts of the file will be received at the client's end where all the files should now be merged.

The merge process will also be done at the clients side only. The client will now start to merge all the three parts into a single file that is the requested file. All the temporary file that is being received will now be removed. After all the operations have been performed the connections will now be closed.

Merits:

- File will be safe even if the hacker manages to hack one server completely.
- To improve the file security increasing the number of servers and the splitting the files into many parts will improve the data security by many folds.
- All types of files including audio files, video files, exe files, pdf files can be successfully split and merged using our system.

III. IMPLEMENTATION

Login:

This is the first module that appears on the screen when we run the application. This has a username filed and a password field where the user is allowed to enter his/her credentials and log in to his/her personal files. Another option called create new account is provided for the new user to create a new account. After the log in is successful the user will be sent to the next module where he/she can either upload a new file or he/she can retrieve back the already uploaded file.

File Upload:

There are a total of three servers that is running. Here when the user presses the upload button, a dialog box appears asking us to select the file. Users are allowed to

navigate to that specific file location and select that file. After the file is being selected the user will click ok where the split and merge function will take its toll.All the split and merge functions will take place on the client side only where the file that the user selected will be splitted into three parts. Now from here each of the file will be uploaded to each of the server. Each server has a part of the uploaded file. After the successful upload of the file the module will show the name of the file that has been recently uploaded having the upload and downloaded buttons.

File Download:

Now when the user selects the download button a request will be sent to each of the servers requesting the file. The request includes the name of the file that is to be retrieved. The Server then searches for the file that is to be sent. If the file is not found the server will return a error code to the client. If the file is found the server will get ready for the file transfer. All the three parts of the file will be sent to the client computer. After the successful retrieving of all the three parts of the file then the merging process will take place. The merging process will take place in the client side only. After the file is being successfully merged the file will be saved on the user's specified location.

Delete file from the Server:

After retrieval of the file it will be still present on the servers end. It is up to the user to either keep the file or delete the file from the server. So if the user decides to delete the file from the server the user first have to click the file download button. After the user clicks the file download button a table will be displayed on the screen which contains all the uploaded file. Now the user can click on the file and select the get button to download the file. So if he wishes to delete the file he will simply click the delete button where a delete request will be sent to the server. If the file is found on the servers end the server will delete the file and conformation will be sent to the client.

Split and Merge Algorithm:

The split and merge algorithm that we have used in this application is unique and this algorithm is what makes this application more secure than the traditional server applications. Here while splitting the file is taken in an ByteArrayOutputStream class and the file is represented in bytes. For example a file that is of size 8 bytes is taken in a byte array of length 8 each containing only one byte. Now three files will be created and the writing process starts.

The first byte of the file will be writed to the first file that is created and the second byte to the second file and the third byte to the third. For example take the 8 byte file. The Bytes 0,3,6 will be written to the first file. The bytes 1,4,7 will be written on the second file and the bytes 2,5,8 will be written on the third file. So each file will be read as a corrupted file if it opened individually. This is how the splitting mechanism takes place on the clients end.

File Server:

The file server will be running indefinitely on the Apache Tomcat server. This file server has three functions. The Receive request, The Send request and The Delete request. These three requests will be on a switch case waiting for a request from the Clients end. The server will now accept the connection and receive a request. If the received request is Receive then the server will get ready to receive the file. After the successful receiving of the file, the server will send a confirmation to the client.

In the send request the client will request for the file that has been uploaded to this server. The request will contain the file name that is to be sent by the server. After the Successful transferring of the file the server will return a confirmation.

In the delete request the client will request the server to delete the file from its server. If the file has been found on the server then the server will delete the file from its database. Then the server will return a success message to the client.
MySQL role:

Here mysql plays a role of storing all the names of the files in the database. Whenever a file is being uploaded to the server the name of the file will be stored in the local mysql server. So whenever the user wish to see the uploaded file he/she need not send any sort of request to the servers. He can view all the uploaded file names from the local server itself.

IV. APPLICATION

This application can be used in any type of data security oriented applications as well as cloud servers. By using our file split and merger algorithm users cannot be worried about the security of their data any more.

V. CONCLUSION

It is proposed that splitting the files and uploading it to multiple servers will increase the security of the data. The

splitting mechanism also is like an encryption to those files which will provide additional security to the files.

REFERENCES

[1] Wikipedia. www.wikipedia.com

[2] Tutorialspoint. www.tutorialspoint.com

[3] Stack Overflow www.stackoverflow.com

[4] Mkyong. www.mkyong.com

[5] CodeJava. www.codejava.net