International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 04 | Apr-2018 www.irjet.net p-ISSN: 2395-0072

Adopting Encryption for Intranet File Communication System

Dr. Sunil Bhutada[1], Sravani Baswaraj[2], Y. Ram Chaitanya[3]

[1]Professor, Dept. of Information Technology, Sreenidhi Institute of Science and Technology, Telangana, India
[2,3] Student (Final year), Dept. of Information Technology, Sreenidhi Institute of Science and Technology, Telangana, India

---

Abstract - It is necessary for organizations to have a way to share all virtual documents with each other. This is generally done through a file communication application such as email. The report talks about the various ways to implement a file communication system on an intranet, doing so in the most secure way possible. Some important considerations to keep in mind while designing the system are implementing the measures to allow for different types of users, different controls, querying on the database should yield quick results and choosing a database structure for the same and even the display of files sent or received if one party, that being receiver or sender, deletes the mail. The following application has been implemented in the apache framework, using Xampp's phpMyAdmin server as a database. The application has been coded in various CGI scripts such as python and php. The selection of python for the application is mainly due to its highly extensive libraries, particularly its cryptology package called "pycrypto". The application is designed to be deployed on either a LAN network or a WAN.

Key Words: File Communication, File Transfer, Apache Framework, Encryption

1. INTRODUCTION

A vital part to becoming a successful organization is to have good communication between all sectors of the organization. Most organizations achieve this by sending electronic mail services managed and provided by a third-party service. These services are extensive and provide many security features which make them a perfect choice. However, there are certain organizations which wish to have complete control over the data being passed around and do not wish to avail the services of a third party. Moreover, they wish for these services to be deployed on their intranet and to be developed and managed by the company itself. As an additional layer of security, companies implement policies which allow few authorized personnel to carry phones or USBs. Access to the internet is restricted as well. For an organization which has its campus buildings placed kilometers apart, there is a necessity to build a communication system on the organization's intranet. The scope of this report is the part of the communication system designed to store and share files among the users of the intranet. To access this application, users are required to login into the portal. If the user does not have an account, he can sign up for one. The key differentiating factor for each user is their employee id. Once the user has signed up, he can send, receive and store his data. The application is to be designed so as to offer several layers of security.

2. LITERATURE SURVEY

Dr. Prerna Mahajan et al. [1] showed that AES algorithm which is a symmetric algorithm is comparatively faster than the other algorithms such as DES algorithm and RSA algorithm. "Encryption calculation assumes essential part in correspondence security. Our exploration work reviewed the execution of existing encryption procedures like AES, DES and RSA calculations. In light of the content records utilized and the test result, it was inferred that AES calculation expends slightest encryption and RSA devour longest encryption time. We additionally watched that unscrambling of AES calculation is superior to different calculations. From the re-enactment result, we assessed that AES calculation is vastly improved than DES and RSA calculation"

Ahmed Fathy et al. [2] stated in their paper that, "Advanced Encryption Standard (AES) calculation is one of the symmetric key piece figures with square size differs from 64 to 256 bits as the processors turn out to be more complex. Notwithstanding, the AES can acknowledge obstruct to 256 bits, its speed still ease back contrasted with the stream-based figures in the season of all applications are looking for quicker encryption process, for example, web servers and Automatic Teller Machines (ATMs). In this manner, the encryption speed and usage region are the two essential variables for real time deployment of AES calculation."

M. Pitchaiah et al. [3] explained the implementation of AES algorithm, "In encryption mode, the hidden key is added to the data regard at unquestionably the beginning stage, which is called a basic round. This is trailed by 9 cycles of a normal round and closes with to some degree balanced last round. In the midst of one regular round the going with errands are performed in the going with ask for: Sub Bytes, Shift Rows, Mix Columns, and Add Round key. The last round is a characteristic round without the Mix Columns phase."

M. Yang et al. [4] stated in their paper that, "Peer-to-peer (overlay) systems are an ideal place to apply organize coding because of two reasons: the topology of a distributed system is built subjectively. It is anything but difficult to tailor the topologies to encourage arrange coding; the hubs in a distributed system are end has which can perform more mindboggling activities, for example, unraveling and encoding, than essentially putting away and sending messages." They also described peer-to-peer networks as "Peers interested in the file form an overlay network through which the file is distributed. The construction of the overlay network is based on the idea of combination networks. A

peer that is a relay node in a combination network may be a receiver node in another combination network. Each peer is a receiver node in one combination network. The server is always the source node in any combination network"

Michel Gien [5] in his paper explained simple FTP architecture as, "An arrangement of record administration tasks, which includes one control point and one (or two) benefit point (s) is called: Transaction. Keeping in mind the end goal to finish a transaction, a discourse happens between a control procedure (the Controller) at a control point and a server procedure (the Server) at an administration point."

Taner Arsan et al. [6] explained two modes of file transfer, "There are two modes for constituting data connection, for example, active and passive, and FTP utilizes the two modes. TCP control association from a non-particular port N to the FTP server charge port 21 will be made by customer. In active modes, approaching information associations on port N+1 from the server will be gotten by customer. Port N+1 is utilized for report the server when FTP charge is sent by customer. In passive mode there is customer behind a firewall and furthermore not accessible for approaching TCP associations. In this mode PASV order is sent to the server by customer through the control association. A short time later server sends a server IP address and server port number. Along these lines customer can utilize it for opening an information association from arbitrary customer port to the server IP address and server port number."

Wikipedia [7] defined file transfer/sharing as, "File sharing is the act of circulating or giving access to advanced media, for example, PC programs, sight and (sound, pictures and video), archives or electronic books. File sharing might be accomplished in various ways. Normal strategies for capacity, transmission and scattering incorporate manual sharing using removable media, concentrated servers on PC systems, World Wide Web-based hyperlinked records, and the utilization of conveyed distributed systems administration."

Dr. Mazin Sameer Al-Hakeem et al. [8] stated the applications of FTP as, "The application layer contains all the more elevated amount protocols which include client cooperation, and one of these protocols is FTP protocol which is constructed from TCP/transport layer to give an approach to move information proficiently starting with one machine then onto the next. FTP is based on customer/server engineering for transfer records, site pages and different reports from a private advancement machines to open documents and web-facilitating servers. FTP utilizes isolate control and information associations for exchange records amongst customer and server. The main FTP customer applications were intuitive command-line apparatuses, yet today FTP customer applications have GUI (Graphical User Interface), including general website composition projects, and master FTP customers. FTP login utilizes a 'clear-content sign-in' validate convention, typically as a username and secret key, for conceding access yet can associate namelessly if the server is designed to permit it, and the session will begin."

3. PROBLEM STATEMENT METHODOLOGY

To design the application in the most efficient way possible, there are several things that have to be taken into account. Each of these design issues have been discussed in the following sections:

A: Schema Design

The biggest discussion was on choosing the most ideal database schema to design the application. When designing such an application, we listed two potential solutions. The first solution that was proposed was to create a record of every transaction in one table. This solution is easy to implement and a straight forward way of designing the schema. However, the disadvantage of this design is that in a company, the transactions will number in ten thousand, perhaps even lakhs. Querying in a database that large will take time and produce very slow results. Such a setback is not conducive to a company's productive environment. The second solution that was proposed was to create a new table for each and every user. This solution overcomes the disadvantage of the previous solution, i.e., in this manner querying and retrieval from the database are easier and quicker. However, this solution has the obvious disadvantage that it will not only create a large number of tables, but also, it will store two records of the same information, one in the sender's table and one in the receiver's table. This disadvantage being huge, this solution was not deemed feasible.

Finally, the solution that was decided as most suitable was a modification of the first solution. In this method, we refresh the data after a suitable interval. Refreshing implies that older record of transactions is cleared due to a certain criterion of time or maximum records. This means that after every month, we refresh the database and clear the older the transactions or we can define a maximum number of transactions. For every new transaction, we can delete an old one. A possible disadvantage of this solution is that data maybe lost. This can be overcome by regularly backing up the data.

B: File Storage

The second discussion that occurred was to decide on how to store the files which are being uploaded by the users. The first and most straight forward solution that was proposed was to use phpMyAdmin's "blob" datatype to store the file in the database itself. A disadvantage of this solution is that storing files in the blob format. When the file is stored, it done so with the .bin extension. The original file extension is lost and additional code would be necessary to convert it into its original form. The second solution proposed was to store the file on the server connected to the Apache Framework. This was the most feasible solution and the one that was implemented in the application.

C: Encryption Algorithms

The main purpose of this application is to transfer and store files in the most secure way as possible. The files which are being stored in the server are done so in an encrypted format.
They are decrypted when there is a request for downloading the file. To perform encryption, the application uses python's extensive cryptology library, PyCrypto. PyCrypto offers several packages for implementing secure hash functions such as SHA256 and RIPEMD160, along with its packages for encryption algorithms such as AES, DES, RSA and EIGamal, etc.

The top choice encryption algorithms for encryption of the files are RSA, DES and AES. DES, an acronym for Data Encryption standard, was a standard followed in the seventies and its disadvantages, such as the fact that it has a smaller key size, which we discovered with a bit of investigation doesn't provide for good security. The key used in DES, can also be brute forced. The next encryption algorithm RSA, which is an acronym for the three people who designed it, is an asymmetric encryption algorithm. This means that it will contain two keys, a private key and a public key, both being able to encrypt and decrypt. The disadvantage with this algorithm is that it takes a longer encryption time than the others and hence it will drive the application to enforce a smaller file size limitation. AES, which is an acronym for Advanced Encryption Standard, is the next version of DES. It has a key size of 128 and 256 bits which are more compatible for encrypting today's files with file sizes ranging in the Gigabytes. It also has the quickest encryption time compared to the other two. The application adopts an AES encryption algorithm with key size 256.

4. SYSTEM ARCHITECTURE

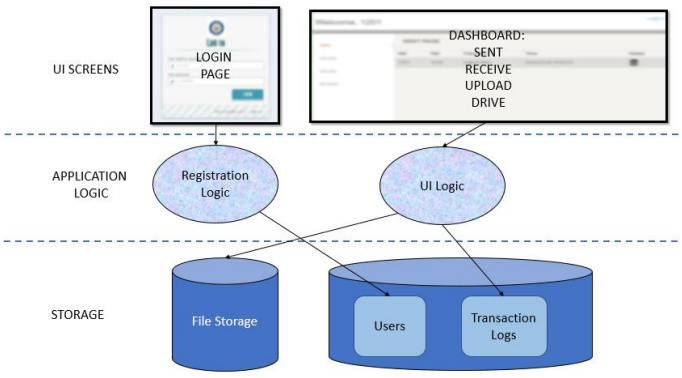

Fig -1: Architecture diagram

The architecture diagram describes the way the various components of the system interact with each other. This architecture diagram comprises of three main layers: The User Interface layer, the application logic layer and the storage or the database layer. Let us discuss each layer in detail along with their components in detail.

A. UI Layer

The user interface layer is generally concerned with the output screens or in simpler terms, the screens or interface which the user directly interacts with. These have to be seamlessly designed to give the users of the application a pleasant vibe as well as experience. The application consists of two distinguishable sets of screens as discussed below:

1. *Login and Registration:* The first page which the users interact with is the login page, where users need to authenticate themselves to access the file transfer services. In the occasion that users do not hold an account, they may register themselves in the registration page provided. However, the admin user needs to activate the user's account before they are allowed to prevail themselves of the services of the application. Entering of wrong credentials will deny the user interaction with the application's dashboard.
2. *Dashboard:* The dashboard of the application consists of four tabs labelled: sent, receive, upload and drive.
   - 2.1. *Sent:* The application has to query the database to fetch all the files which have been sent to the user. If the user wishes to download the file, the file has to be decrypted first then downloaded.
   - 2.2. *Receive:* The application has to query the database to fetch all the files which have been received by the user. If the user wishes to download the file, the file has to be decrypted first then downloaded
   - 2.3. *Upload:* When the user uploads the file, a record has to be created of the transaction. Besides that, the file has to be stored on the server in an encrypted format
   - 2.4. *Drive:* The application allows the user to store and save files onto the server. The application simply interacts with the server to insert, retrieve and display the files which the user has stored

B. Application Logic

The application logic or the business logic layer is the layer where you specify what has to be done with the inputs provided by the user. It is usually in this layer that a programmer codes in his or her logic. This application implements apache framework for displaying the user interface. It uses CGI scripts such as python and php to implement its application logic. The application consists of two distinguishable sets of code as discussed below:

1. *Registration Logic*: This part of the code authenticates the user credentials and displays error messages in the occasion that the credentials are incorrect. It retrieves user information stored in

the database and compares it for authentication. When a user registers himself or herself, a new record is added into the user table. A status variable controls the activation of the account. If the account is not activated, then the application is debarred from accessing the dashboard.

2. *UI Logic*: The UI Logic is the part of the code which is associated with each part of the dashboard screens:

   2.1. *Sent:* The application has to query the database to fetch all the files which have been sent to the user. If the user wishes to download the file, the file has to be decrypted first then downloaded.

   2.2. *Received:* The application has to query the database to fetch all the files which have been received by the user. If the user wishes to download the file, the file has to be decrypted first then downloaded.

   2.3. *Upload:* When the user uploads the file, a record has to be created of the transaction. Besides that, the file has to be stored on the server in an encrypted format.

   2.4. *Drive:* The application allows the user to store and save files onto the server. The application simply interacts with the server to insert, retrieve and display the files which the user has stored.

C. Storage Layer

The storage layer, as the name suggests is where we store non-volatile data or permanent data. The application consists of two distinguishable sets of storage as discussed below:

1. *File Storage:* The files which have been uploaded are stored on a local server, in an encrypted format. The application uses an AES encryption standard as studies show that it offers the highest security as compared to the other encryption formats.

2. *Relational Database:* The application uses Xampp's phpmyadmin as its relational database. There are two tables which are used to design the logic as mentioned below:

   2.1. *Users:* This table contains all the user credentials and is used during the authentication process. The schema used by the table is users (uid, uname, pass, status)

   2.2. *Transaction:* This table contains all the transactions which are made by the different users. The schema used by this table is logs (sid, rid, filename, date, remarks)

5. EXPERIMENTAL SETUP

1. Xampp Installation: Open any browser of choice and search for the link: https://www.apachefriends.org/download.html and download the software with php version 7.22 and navigate through the process

2. Now install python to provide server-side programming, the link to download is given by https://www.python.org/downloads/ and for the application being deployed it is important that python 2.7 version is to be selected while downloading.

3. Once python is downloaded under system properties– Environmental Variables – User Variables – add Path – C:\Python2.7 (Location of python installation)

4. Add Path variable in System Variable so that it allows easy access Path – C:/Python27

5. In order to run .py, cgi scripts, follow the steps below:

   - Open the httpd.conf file in apache by clicking config but do not start apache yet.
   - Look for AddHandler cgi-script .cgi .pl .asp and add .py to it.
   - Now start apache
   - To run your files type localhost/ enter in name of file. Ex: localhost/hello.py
   - We need to make sure to have the location of the python file on top of python files which shows the location of where python.exe is. Ex#!C:/Python27/python.exe
   - Python files need print("content-type: text/html/n/") below in order to print html content in its pages.

6. We need to make sure that phpMyAdmin is working properly as it's important to check whether the database is able to store records into tables existing in the database. The port number by default will be 3306 we must make sure that no other application is using the same port as it will not allow this software to run.

7. Once the environment is setup it's time to install the required packages for running the application, this can be installed by the default process of using pip but still we can install them using .exe files from python official website.

8. The list of packages to be installed is to be executed in the cmd – C:/Python27/Scripts

   - To establish connection with the MySQL database a package is to be imported

named as MySQLdb, this can be done by downloading the .exe file from the link: https://pypi.python.org/pypi/MySQLpython/1.2.5 and once this file executes the requirement is satisfied.

- To install winapi32: pip install pypiwin32
- To install cookie: pip install cookies
- To install boto: pip install boto
- To install pycrypto: pip install pycrypto

9. Once everything is installed and setup accordingly run a basic python program with .py extension kept in htdocs ex: hello.py, run the link localhost/hello.py if the program executes the required setup is successful.

6. RESULTS AND OBSERVATION

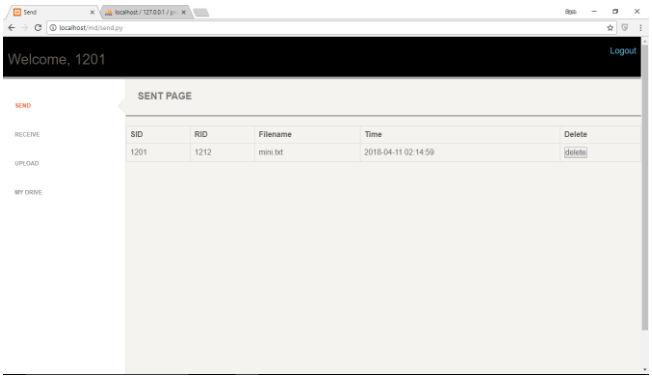

Fig -2: Sent page of the application

Based on the credentials the user provides, he or she is authenticated at the login. In the case that the credentials are false, he is denied access form the services of the system. Once the user logins in, he or she can see the files which have been sent to the user.

The users can use the upload tab to draft and upload files of his choice:

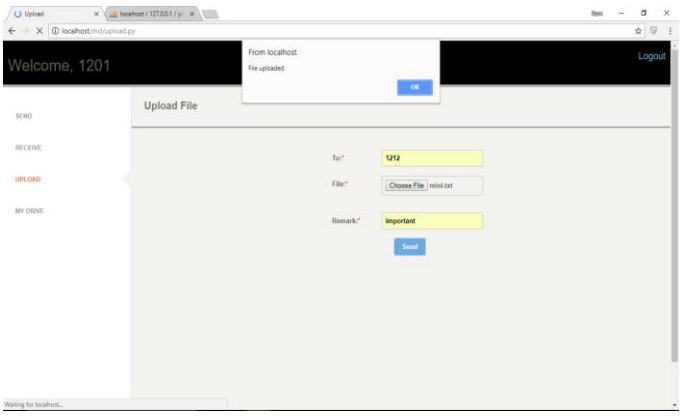

Fig -3: Upload page of the application

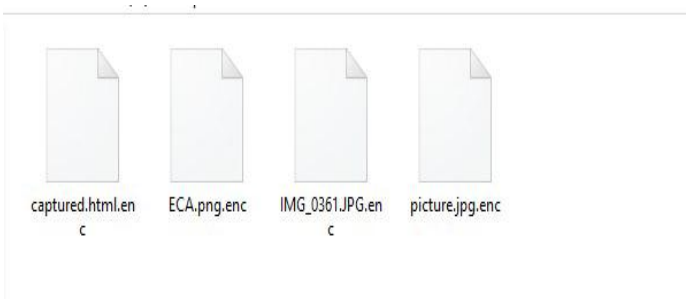

Fig -4: Encrypted files

The file on being uploaded to the server is stored in an encrypted format.

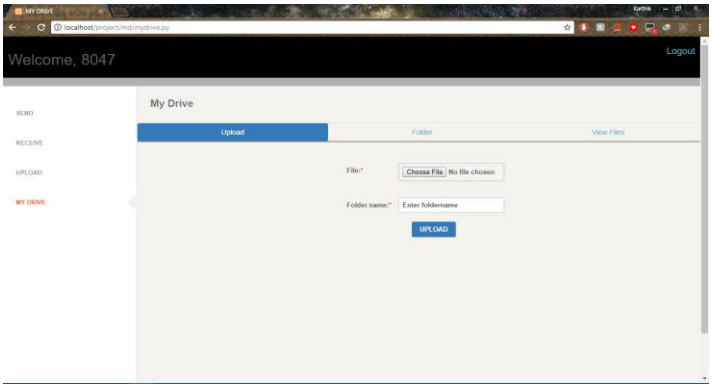

Fig -5: My Drive to upload

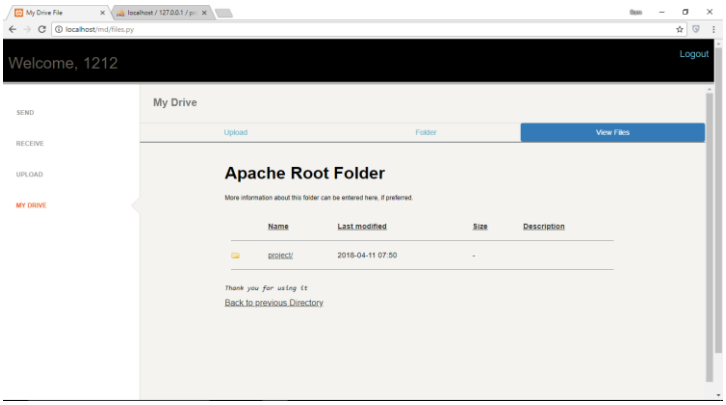

Fig -6: My Drive to view

7. CONCLUSION

The application intends to deliver data in the most secure way possible and it achieves its target by security measures described by the paper. The computational world is a dynamic place and new security standards and measures are announced periodically. These changes need to be incorporated so as to provide the most security to the data. New encryption algorithms can be incorporated or a combination of them. A shift from a symmetric encryption to an asymmetric encryption can also be implemented. It is also in the application's future scope to search for algorithms which offer faster encryption for higher file sizes.

REFERENCES

1. Dr. Prerna Mahajan and Abhishek Sachdeva, "A Study of Encryption Algorithms AES, DES and RSA for Security", Global Journal of Computer Science and Technology Network, Web and Security- Volume 13 Issue 15 Version 1.0 Year 2013.

2. Ahmed Fathy, Ibrahim F. Tarrad, Hesham F.A. Hamed, and Ali Ismail Awad, "Advanced Encryption Standard Algorithm: Issues and Implementation", Advanced Machine Learning Technologies and Applications- pp516-523, 2012.

3. M. Pitchaiah, Philemon Daniel and Praveen, "Implementation of Advanced Encryption Standard Algorithm", International Journal of Scientific and Engineering Research- Volume 3, Issue 3, March 2012.

4. Min Yang and Yuanyuan Yang, "Peer-to-peer File sharing based on Network Coding", International Conference on Distributed Computing Systems, IEEE, June 2008.

5. Michel Gien, "A File Transfer Protocol", Computer Networks, 2(4- 5):312-319, September 1978.

6. Taner Arsan, Fatih Guney and Elif Kaya, "Implementation of Application for Huge Data File Transfer", International Journal of Wireless and Mobile Networks- Vol 6, No 4, August 2014.

7. File Sharing- Wikipedia (English) https://en.wikipedia.org/wiki/File sharing

8. Dr. Mazin Sameer Al-Hakeem, Suhiar M. Zeki and Sarah Y. Yousif, "Development of Fast Reliable and Secure File Transfer Protocol", Al- Mansour Journal- Issue 19, 2013.

9. Lei Wang and Qing Wang, "Secure-Network-Coding-based File Sharing via Device-to-Device Communication", Journal of Electrical and Computer Engineering- Volume 2017, 2017.