Secure Backup Software System  
  
  
A Report submitted   
in Fulfillment of the Requirements  
 for the lab practical examination of  
**Master of Technology** in  
**Computer Science Engineering Department**  
  
  
 by  
 Nitish kumar (2018IS09)  
 Harshit Kumar (2018IS04)  
 Ashutosh Jha(2018CS16)  
  
  
to the  
 **Computer Science Engineering Department**MOTILAL NEHRU NATIONAL INSTITUTE OF TECHNOLOGY ALLAHABAD  
26 April 2019

**UNDERTAKING**We declare that the work presented in this report titled "Secure Backup software", submitted to the Computer Science and Engineering Department, Motilal Nehru National Institute of Technology Allahabad, Prayagraj. We have not plagiarized or submitted the same work for the award of any other project. In case this undertaking is found incorrect. We accept that our project may be unconditionally withdrawn.

April 25, 2019

Nitish kumar (2018IS09)  
Harshit Kumar(2018IS02)  
 Ashutosh Jha(2018CS16)

**CERTIFICATE**Certified that the work contained in the report titled "Secure Backup Software System" has been carried out under my supervision and that this work has not been submittedelsewhere for a project

Project Member:-

Nitish Kumar (2018IS09)Harshit kumar(2018IS02)(**Dr. Mayank Pandey**)  
Ashutosh Jha(2018CS16) Associate Professor,CSED

MNNIT-ALLAHABAD

(**Er. Nitin shukla**)  
 MNNIT-ALLAHABAD

**Acknowledgements**We wish to express my sincere gratitude to **Dr.Mayank pandey** and **Er.Nitin Shukla** for providing us an opportunity to work in this project and for his guidance and encouragement at every step of project.

He exposed us to the intricacies of relevant topics through proper counselingand discussions and always showed great interest in providing timely support and

suitable suggestions.

We would also like to thank other groups which willing to share information about study of android operating system and android application development. We would like to express our gratitude to all our friends in the Department of ComputerScience for their constant support and encouragement.

**Contents**

**Preface  
  
Acknowledgements   
  
1. Introduction   
 1.1 Need and Motivation**

**2. Module   
 2.1 Admin Management  
 2.2 User Management**

**3.Methodology  
 3.1 SFTP Server  
 3.2 Proposed system**

**3.2.1 System Administrator**

**3.2.2 Users**

**4. Implementation**

**5. Conclusion**

**6. Refrences**

1. **Introduction**In today’s computing era, with the increase in the computational power and bandwidth, people fid it more feasible to store their data online so that they can access it from the remote places. It helps them to safeguard their data from accidental damages, various security threats. So, here in this project we will try to make a web service of (SFTP) where different users can register themselves and can upload their data, files, photos, videos, documents, etc. We will try to safeguard their data from various security threats, unauthorized access, accidental damage, etc.

Data Integrity, confidentiality and authentication will

be the three primary focus of this application. This

application will ensures that they can access their

data at any time as per their requirements.

* 1. **Need And Motivation**There are various reasons for having Secure backups Software they are as given below:-  
     1.**Simple Recovery :-**People are not infallible. They make mistakes, and actually, they make them quite often. Emails containing viruses are accidentally opened every day and important files are often mistakenly deleted. There’s no reason to fear these issues if you take frequent incremental snapshots of your systems. You can simply restore to a snapshot taken before the virus happened. Or you can recover the file from a time before it was deleted.  
       
     2.**Deadly Downtime**:-A Survay of 2007 University of Texas [study](http://www.businessweek.com/stories/2007-09-02/data-lost-data-found) showed that 43 percent of businesses that suffer major data loss never reopen. Many of these companies end up closing their doors for good within two years of a major data loss. And even large data loss scenarios aren’t always the result of a disaster. Human hands are very capable of destroying a business through silly mistakes or oversights.

1. **Modules**This project aims to Enhance “SECURE BACKUP SOFTWARE SYSTEM”, keeping in mind the safety and comfort of USER.  
   Through this application admin can access the whole information that is getting through the site

There are basically two modules we have used in the project  
2.1 Admin Management  
2.2 User Management

Admin management where, An admin control all the activities going through the website, If the user found to be unauthorized by the admin, then admin can block a user and also can unblock it whenever required.

User module, where user registers himself, and also user can store documents and files in any format which is kept in a separate folder made for each user in a secure manner

This project has the most secure and advanced client panel where client after Upload their data they can encrypt the data by choosing various algorithmAES Key and secure their data.Intergrity can be obtained using Hashing Function.  
  
  
3. **Methodology**

* To transfer the data from the customer’s computer to the server we will use SFTP (SECURE FILE TRANSFER PROTOCOL).
* To store the data at the server, all the data will be encrypted with the algorithms (AES) chosen by the User.
* To ensure the confidentiality all the data will be stored after encrypting it by various encryption algorithms like DES.
* To safeguard the secret key used for encryption we will use hashed password with a dash of salt. Salting a hash means adding a random string of characters called “salt”. It is added to the beginning or end of your password before hashing it.
* To ensure the accidental damage of the data, data will be copied to various servers and their synchronization algorithm will be taken into consideration.

**3.1 SFTP (SECURE FILE TRANSFER PROTOCOL)  
SERVER**

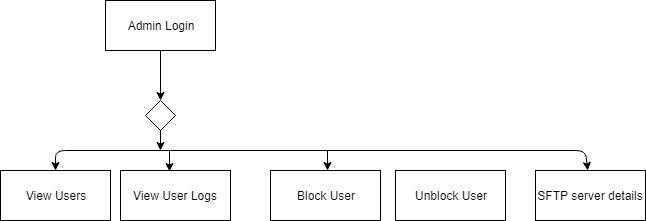
Secure SFTP server helps users with transferring files over secure file transfer protocols such as SSH File Transfer Protocol or SFTP with SSL/TLS. The transfers can be achieved through server-to-server or client-to-server configurations. A secure SFTP server helps enterprises in sending confidential files securely over the internet orinsecure networks.SFTP server needs an SSH clientfor communication.A secure SFTP server supports many actionson files such as file transfers comprised of multiple files, remote file management activities, creations of directories and deletions related to directories and directory listings. A secure SFTP server also makes use of protocols to provide security features such as authentication, encryption or data integrity, password management and access control mechanisms. Certain advanced secure SFTP servers such as JSCAPE MFT server often provides both SFTP and FTPS protocols along with other file transfer protocols

Here we use OpenSSH server on windows to create SSH server.

**3.2 Proposed System**

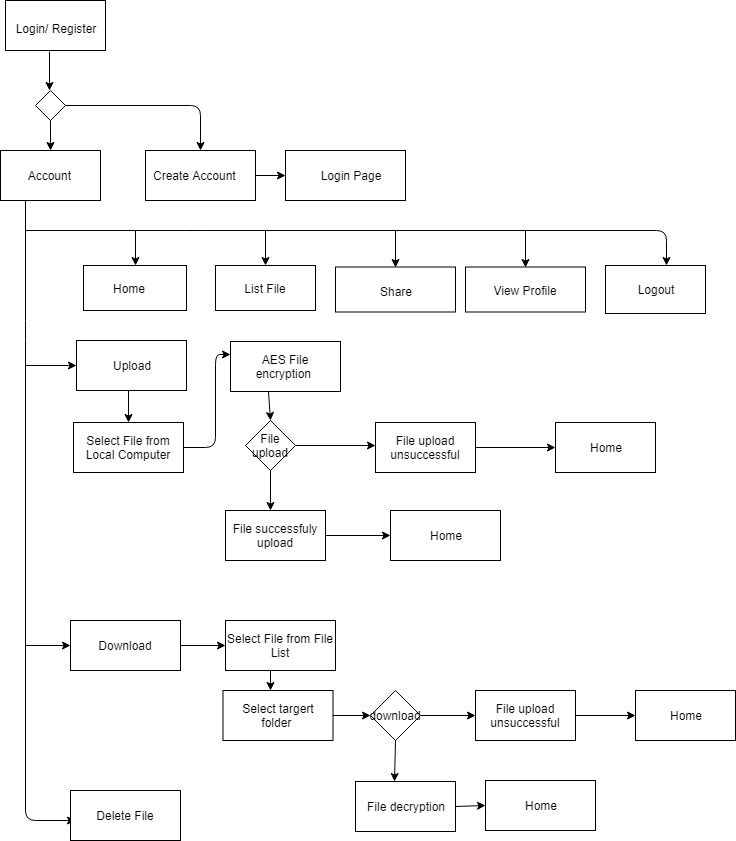
This software creates backup of all the files uploaded by the user.User can store files, documents, images, video presentations, etc.

**3.2.1 System Administrators:** They will configure and deploy the SFTP servers. They check all the activities of the user and can block them in case of suspicious activity.



* To transfer the data from the customer’s computer to the server we will use SFTP.
* Admin can change the SFTP server details.
* To ensure safety from accidental damage we maintain two sftp servers.
* Admin keeps an eye on the activities of the user and can block them in case of any suspicious activity.
* Admin can unblock a user into the system.

**3.2.2 Generic Users:** They use application to transfer upload, delete, and download files securely on the server.



* User need to validate their login credentials while login**. T**his system is designed to allow users to upload and download files from this application.
* The main objective of this project is to stores files and will be access to the registered authorized users only.]
* As user registers himself, a new folder is created on the SFTP server.
* When the registered user uploads a file, the file will get stored into respective user’s folder on the sftp servers.
* Users can also download the uploaded file, which will be restored from the user’s folder.
* The user can also log into the system any time and he/she can delete the existing files.
* File is encrypted with AES before uploading to the server.
* This system uses MD5 hashed value of password of the user as the key for encryption.
* To safeguard passwords, in case of attack on data server, passwords are hashed and stored with a dash of salt. This prevents attacks like rainbow table (It is a table which maps hash value to its text.).

**4. Implementation**

We use the following technologies to implement this system.

**Java:**Java is a general-purpose programming language that is class-based, object-oriented, and specifically designed to have as few implementation dependencies as possible. In this we use

* JDBC: To connect SQL database.
* Jcraft.Jsch: Library for sftp functions.

**Java Swing:**Swing is a GUI widget toolkit for Java. It is part of Oracle's Java Foundation Classes – an API for providing a graphical user interface for Java programs. Swing was developed to provide a more sophisticated set of GUI components than the earlier Abstract Window Toolkit. We use it to provide GUI interface.

**Open SSH Server:**OpenSSH is a suite of secure networking utilities based on the Secure Shell protocol, which provides a secure channel over an unsecured network in a client–server architecture. It is preinstalled in ubantu and can be easily installed on windows to start the sftp server. It generally runs on port 22.

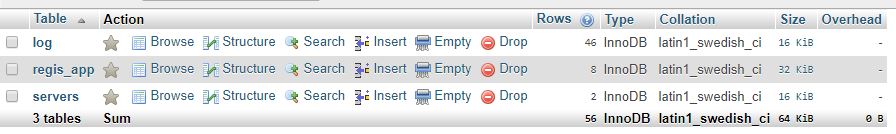
### **My SQL:** MySQL is an open-source relational database management system. We use it as a component of xampp server. We use it create our database where all the users and their activities are registered.

**AES:**AES is based on a design principle known as a [substitution–permutation network](https://en.wikipedia.org/wiki/Substitution%E2%80%93permutation_network), and is efficient in both software and hardware. Unlike its predecessor DES, AES does not use a [Feistel network](https://en.wikipedia.org/wiki/Feistel_network). AES is a variant of Rijndael which has a fixed [block size](https://en.wikipedia.org/wiki/Block_size_(cryptography)) of 128 [bits](https://en.wikipedia.org/wiki/Bit), and a [key size](https://en.wikipedia.org/wiki/Key_size) of 128, 192, or 256 bits. By contrast, Rijndael *per se* is specified with block and key sizes that may be any multiple of 32 bits, with a minimum of 128 and a maximum of 256 bits.

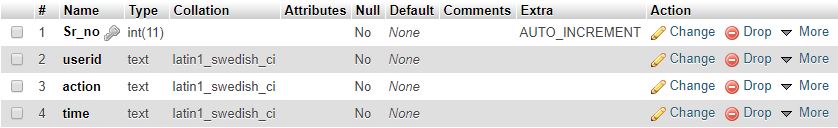
**Snapshots:**

**Databases**

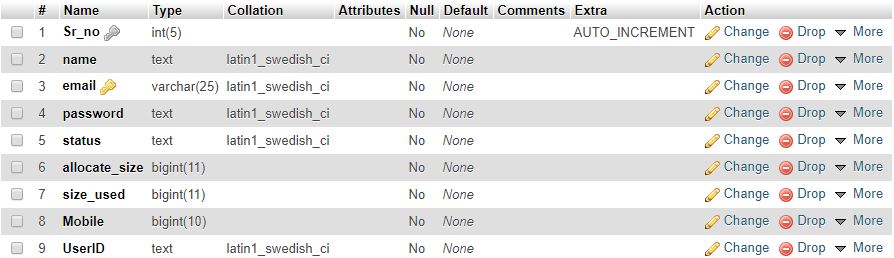
We make three tables as:

****

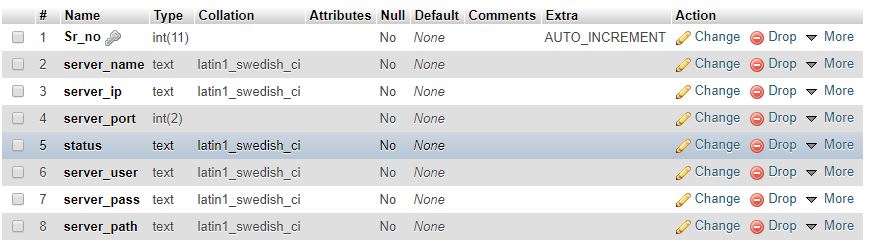
**Table 1: Log Table**

****

**Table 2: Register App**

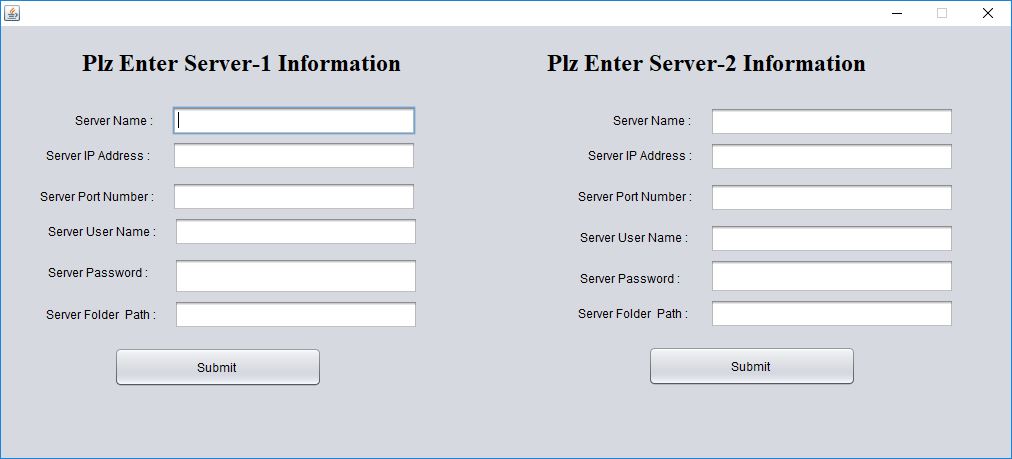
****

**Table 3: Servers**

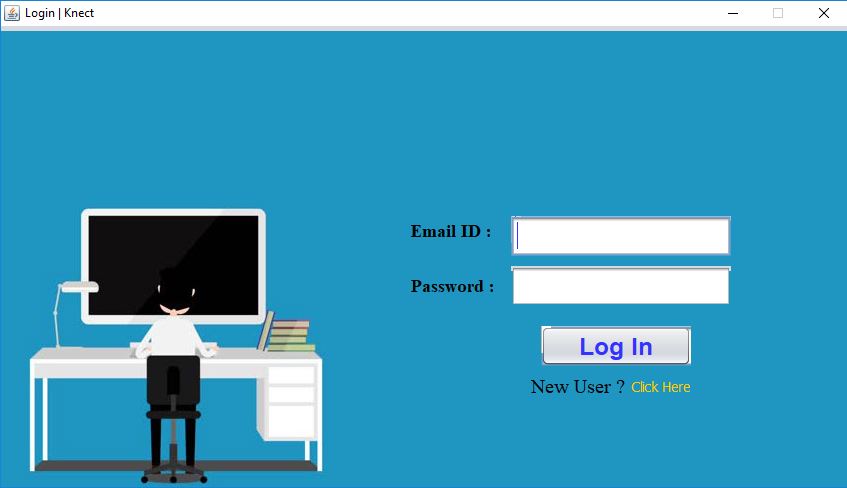
****

**Snapshot of Desktop Application:**

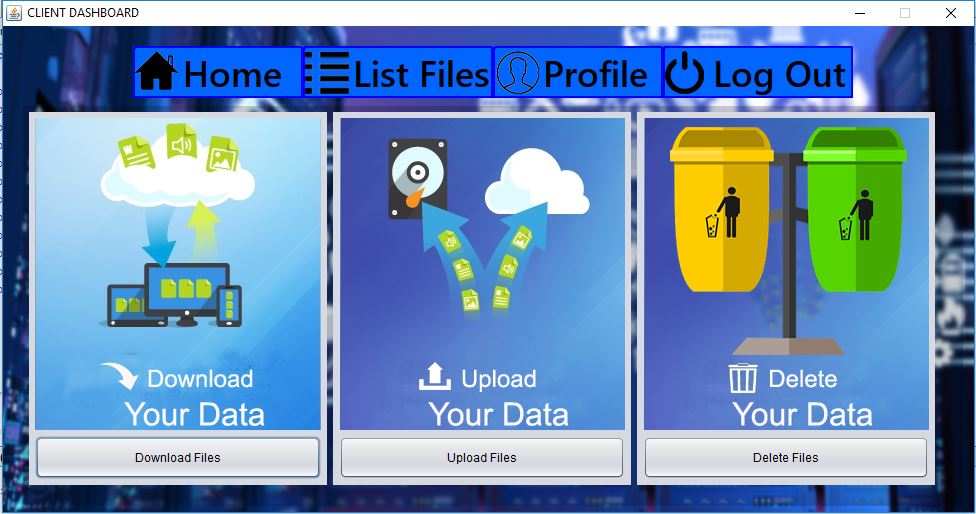
SFTP Server Information:

****

Client Login:

****

Client Home Page:

****

**5. Conclusion**

In this project we successfully create sftp client application through which users can safely upload, download files of any format. This project helps us to understand various security threats that can occur while transferring file and storing them on the remote server. We implement AES algorithm and MD5 hashing algorithms to provide confidentiality and password protection. We also use the concept of salt pruning. This system has simple GUI.

**Advantages**

* Easily create a backup of any file by uploading it.
* Ease to download the uploaded file.
* Hackers will not be able hack the system.
* Secure and Robust

**Limitations:**

1. For this application to work user should be connected to the network.
2. As we use password as AES key for encryption and decryption So, if the user forgets his/her password, it can’t be recovered.

**Reference:**

* IEEE, “IEEE recommended Practice for Software Requirement Specification”.
* Password security – CSC journals by Danuvasin Charoen