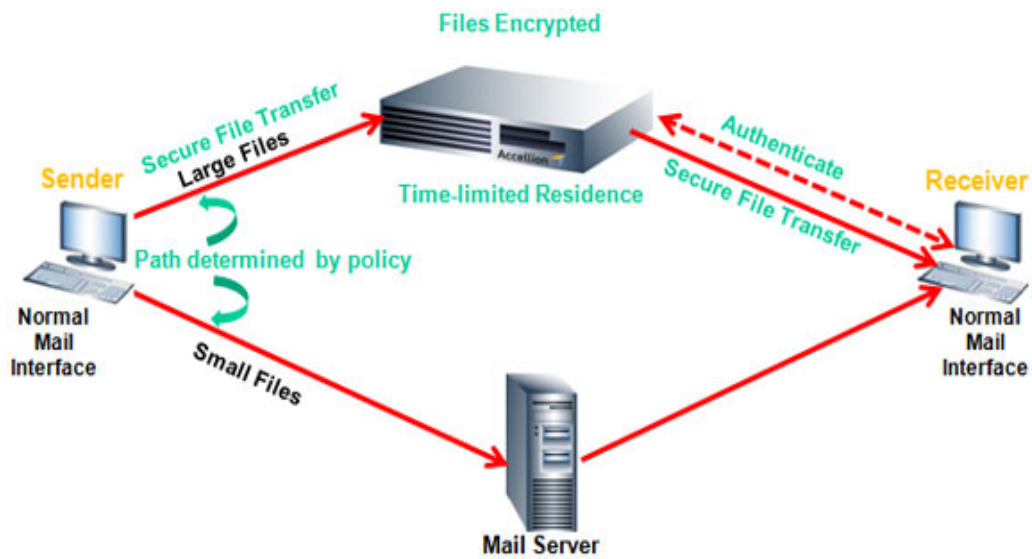
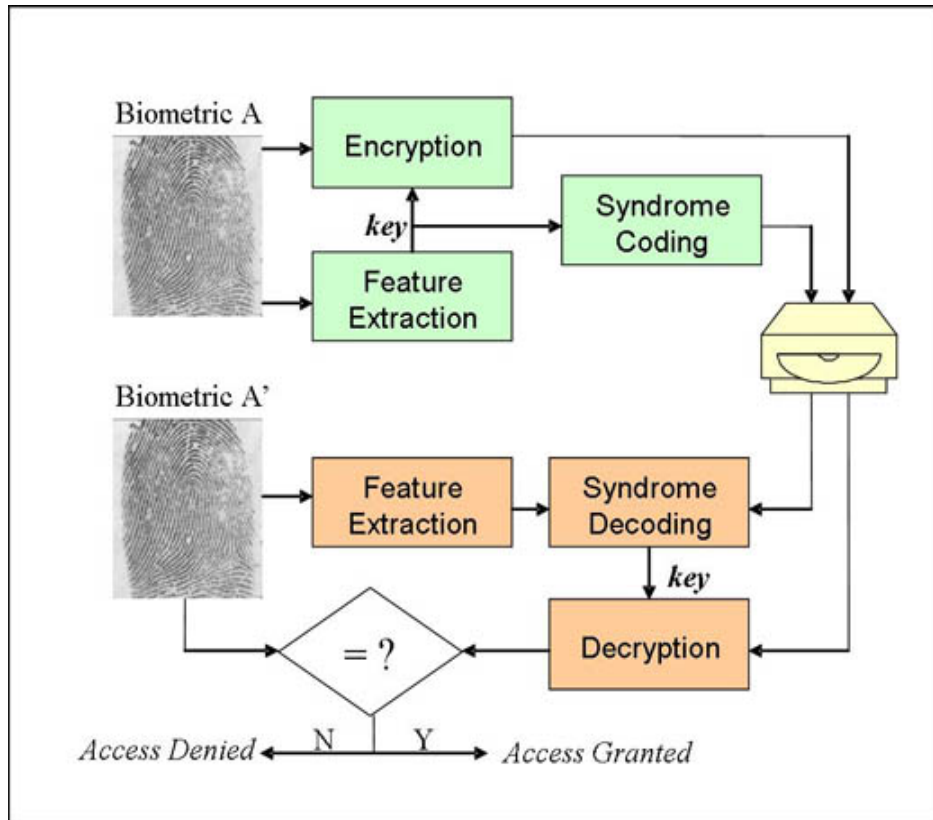


# BIOMETRICS

Among all the biometric techniques, fingerprint-based identification which has been successfully used in numerous applications. Everyone is known to have unique, immutable fingerprints. A fingerprint is made of a series of ridges and furrows on the surface of the finger. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutiae points. Minutiae points are local ridge characteristics that occur at either a ridge bifurcation or aridgeending.



File Transfer



### Secure Biometrics

Fingerprint matching techniques can be placed into two categories: minute-based and correlation based. Minutiae-based techniques first find minutiae points and then map their relative placement on the finger. However, there are some difficulties when using this approach. It is difficult to extract the minutiae points accurately when the fingerprint is of low quality. Also this method does not take into account the global pattern of ridges and furrows. The correlation-based method is able to overcome some of the difficulties of the minutiae-based approach. However, it has some of its own shortcomings. Correlation-based techniques require the precise location of a registration point and are affected by image translation and rotation.

Fingerprint Identification is the method of identification using the impressions made by the minute ridge formations or patterns found on the fingertips.

## **Learning**

Supervised learning rules require a 'teacher' to tell them what the desired output is given an input. The learning rules then adjust all the necessary weights (this can be very complicated in networks), and the whole process starts again until the data can be correctly analyzed by the network. Supervised learning rules include back-propagation and the delta rule.

Secure File Transfer System is a file transfer program. An authenticated user can upload and download files from a remote location, provided the other end has software running. Secure File Transfer System has been specially configured to provide security to files while transferring. For a company time is always constraint. By using this software, the company can save their precious time. If the any one tends to access the file in any other way, he finds the encrypted document (not the original one). Thus the leakage of the document is blocked perfectly in this system. The user with valid user name and password can access his data with out bothering about the encryption method and the key used (The key is automatically generated by the software according to each file transfer).

The project has been developed using Core Java, Using Swing for GUI creation and RMI for file transfer

## **PROPOSAL FOR DISSERTATION**

SFTS, or Secure File Transfer System, is a program that uses SSH to transfer files. Unlike standard FTP, it encrypts both commands and data, preventing passwords and sensitive information from being transmitted in the clear over the network. It is functionally similar to FTP, but because it uses a different protocol, you can't use a standard FTP client to talk to an SFTS server. An authenticated user can upload and download files from a remote location

**The project has the following modules.**

**1) G U I (user interface)**

This module containing all the forms for user interaction to the System. It includes login Form, display other forms for the application.

**2) Login/ User Authentication**

A user is allowed to enter the system if and only if the administrator allows him to do so. After the administrator allows him to enter the system he has to undergo his own login where he has to enter his own Username and Password Which are sent as encrypted text to the server where his validation is done. If valid he may access the features of SFTS.

**3) File Management/Folder Management**

The functionalities of this module are File/Folder creation in a specified drive in server. It also provides other file management operations like add edit delete files and also the user can drag and drop the files.

**4) Upload Module**

In this module upload the encrypted message to a specified location in the server have an upload interface which gets the source location and sent to the destination.

**5) Download Module**

In this module specify the source location in the server and the specified location to save that file in the client side. After getting the file from the server, which is in the encrypted format is subjected to decryption using RSA algorithm and is the saved to the system.

## **6) Encryption Module**

The main component of this module is the encryption algorithm. In SFTS system, implemented the AES algorithm to encrypt data. Its security is based on the difficulty of factoring large integers. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key.

Suppose Alice wants to send a message  $M$  to Bob. A

Alice then computes the cipher text corresponding to:

Alice obtains public key from Bob and keeps the private key secret.

1. Obtains the recipient B's public key  $(n, e)$ .

Represents the plaintext message as a positive integer  $m$ .

Computes the cipher text  $c = m^e \bmod n$ .

2. Sends the cipher text  $c$  to B.

## **7) Decryption Module**

On receiving the encrypted message from A to B does the following;

3. Uses his private key  $(n, d)$  to compute  $m = c^d \bmod n$ .

4. Extracts the plaintext from the integer representative  $m$ .

## **8) User Management**

The functionality of this module is to set the privileges for the users of the system. According to SFTS there are 2 types of users, Administrator and user. Only the administrator has the right to add users into the system. View the log etc. client user has the right to download particular file from server etc.

## Requirements:

### Hardware requirements

Number	Description	Alternatives (If available)
1	A server Machine with Min 10GB Hard Disk and 512 RAM	Not-Applicable
2	Client Machines Having Min 5GB Hard Disk and 256 Mb RAM	

### Software requirements

Number	Description	Alternatives (If available)
1	Windows 95/98/XP	Not Applicable
2	J2SE	
3	Mysql(DBMS)	