Secure Cloud Service Provider With Biometric Authentication And Multiple Cloud Storage System

Raghav R[1], Praveen Kumar R[2], Umapathi S[3], Elaiyaraja S[5]
[1, 2, 3, 4] Dept of Information Technology
[5] Assistant professor, Dept of Information Technology
[1, 2, 3, 4] Valliammai Engineering College, TamilNadu, India.

Abstract- *Cloud platform provides storage services to both individuals and organizations. However, some security concerns may impede users to use cloud storage. Among them, the integrity of outsourced files is considered as a main obstacle, since the users will lose physical control of their files after outsourced to a cloud storage server maintained by some cloud service provider (CSP). Thus, the file-owners may worry about whether their files have been tampered with, especially for those of importance.Hence to address integrity, controllable outsourcing and origin auditing concerns on outsourced files, we propose an* ***identity-based data outsourcing (IBDO) scheme****. Thus IBDO provides desirable features advantageous over existing proposals in securing outsourced data. Our IBDO scheme provides following advantages, Allows a user to authorize dedicated proxies to upload data to the cloud storage server on her behalf, e.g., a company may authorize some employees to upload files to the company's cloud account in a controlled way. To make the machine identify the data owner and dedicated proxies, we use an* ***auditor*** *to audit the incoming packets, efficient* ***fingerprint analysis****,* ***MAC address****,* ***file type****, consistence of outsourced. Eliminates complex cryptographic certificates.*

Keywords- Cloud Service Provider(CSP), Fingerprint analysis,MAC address,

I. INTRODUCTION

Cloud platform provides powerful storage services to individuals and organizations[1]. It brings great benefits of allowing on-the-move access to the outsourced files, simultaneously relieves file-owners from complicated local storage management and maintenance[2]. However, some security concerns may impede users to use cloud storage. Among them, the integrity of outsourced files is considered as a main obstacle[3], since the users will lose physical control of their files after outsourced to a cloud storage server maintained by some cloud service provider (CSP). We observe two critical issues not well addressed in existing proposals. First, most schemes lack a controlled way of delegatable outsourcing. One may note that many cloud storage systems (e.g., Amazon, Dropbox, Google Cloud storage) allow the account owner to generate signed URLs using which any other designated entity can upload, and modify content on behalf of the user. However, in this scenario, the delegator cannot validate whether or not the authorized one has uploaded the file as specified or verify whether or not the uploaded file has been kept intact. Hence, the delegator has to fully trust the delegatees and the cloud server. In fact, the file-owner may not only need to authorize some others to generate files and upload to a cloud, but also need to verifiably guarantee that the uploaded files have been kept unchanged.Second, existing PoS-like schemes, including PDP[4] and Proofs of Retrievability (PoR), do not support data log related auditing in the process of data possession proof. The logs are critical in addressing disputes in practice. For example, when the patient and doctor in EHS get involved medical disputes, it would be helpful if some specific information such as outsourcer, type and generating time of the outsourced EHRs are auditable. However, there exist no PoS-like schemes that can allow validation of these important information in a multi-user setting.

1.1 OBJECTIVE OF THE PAPER

To address the above issues for securing outsourced data in clouds.This paper proposes an identity-based data outsourcing (IBDO) system in a multi-user setting. Thus, the file-owners may worry about whether their files have been tampered with, especially for those of importance.pared to existing PoS like proposals, our scheme has the following distinguishing features

II. PREVIOUS WORKS

We observe two critical issues not well addressed in existing proposals. First, most schemes lack a controlled way of delegable outsourcing. One may note that many cloud storage systems(e.g. Amazon, Dropbox, Google Cloud storage) allow the account owner to generate signed URLs using which any other designated entity can upload, and modify content on behalf of the user. However, in this scenario, the delegator cannot validate whether or not the authorize done has uploaded the file as specified or verify

whether or not the uploaded file has been kept intact. Hence, the delegator has to fully trust the delegates and the cloud server.Second, existing PoS-like schemes, including PDP and Proofs of Retrievability (PoR), do not support data log related auditing in the process of data possession proof. Second, existing PoS-like schemes, including PDP and Proofs of Retrievability (PoR), do not support data log related auditing in the process of data possession proof. Third, no biometric based authentication is been integrated for secure authentication of the users. Fourth, Multiple cloud storage invoking split and merge concept is not in existence, thus leading to many security threats.

III. SYSTEM OVERVIEW

Identity Based Data outsourcing with auditing clouds **(IBDO)** is file store to secure cloud storage. Fingerprint device used to verify and identifying the login page. Fingerprint is scanner of technology. Purpose of unauth orized person not access the system. Finger print scanner is to scan the pattarn method to allocate point by poin .It's top side for Ridge Burification(Starting point) and bottam side for Ridge Termination(Ending point). Fingerprint process is three stage are, Thinning image, Binarized image, Line Extraction. Data owner has been register and login to send file to designation entity(Data Assestent). After designation Entity as register and login to persnal account to access and send to admin. Designation Entity not access the one system, so each time to send file Proccesing to be automatic allocate Ipaddress and MAC adress. Admin has been register and login to persnol account and recieve file list to check and verify after upload to clouds then processing files can be split the File after convert to encrypt format. Purpose of additional security means not access the unautherized persan. After to store splite file1 for cloud1(**CloudMe**) and splite file2(**DropBox**) . SHA (**Secure Hahe Alogarithm**) is used to encrypt the file after to generate key. Admin can be download file from clouds to merge files automatically and convert decrypt format after download files. Minutiae algorithm is used for Fingerprint verification. It's produce two stages are,

1.Minutiae Matching
2.Minutiae Extraction

Minutiae Matching –To matching point values.
Minutiae Extraction- To extrac the Fingerprint verification

Identity Management – Data Owners / Dedicated Proxies

Fingerprint based biometric authentication is an important and widely used biometric type authentication because of its cost, accuracy and feasibility. In our proposed system, the user fingerprint feature are extracted and verified using Minutiae Map algorithm (MM) [1]. Minutiae Map algorithm identifies the fingerprint ridges and extracts the bifurcation and termination values from the input fingerprint image. Ridge termination is the point at which ridge ends. Bifurcation is the point at which ridge splits into two halves which is shown in the below figure. Our proposed system provides the respective user fingerprint total bifurcation, termination values along with its location (X, Y coordinates) and stores in the database during user registration. In our proposed system, ideal thinned ridge is considered. We assume usually a thinned ridge will have a value 1 or 0. The algorithm uses 3*3 windows to scan the image and the bifurcation and termination in the final output image shall be represented by a dot. Let's consider (x,y) denote the pixel on the thinned ridge and N_0, n_1, ……N_7 denote its neighbours.

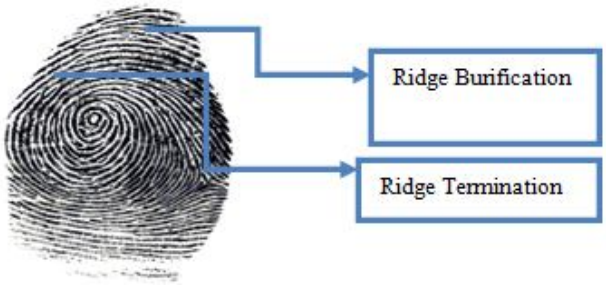

Fig. 1 Fingerprint Extraction

A pixel (x,y) is a ridge ending if,

$$\sum_{i=0}^{7} Ni = 1$$

A pixel (x,y) is a ridge bifurcation if,

$$\sum_{i=0}^{7} Ni > 2$$

Data Owner / Dedicated Proxies Behaviour Analysis

In this module the data owner / dedicated proxies behavior is been analyzed. For this we keep a log of origin, file types, consistence of outsourced. We use techniques to detect the MAC address whenever the data owner dedicated proxies access. If they access from different machines or upload / access different file types an alert e-mail would be sent to the data owner. On approval by the data owner the dedicated proxies would be allowed to access inside the application.

Split And Merge Technique

Cloud Storage usually contains business-critical data and processes, hence high security is the only solution to retain strong trust relationship between the cloud users and cloud service providers. Thus to overcome the security threats, this paper proposes **multiple cloud storage**. Thus the common forms of data storage such as files and databases of a specific user is split and stored in the various cloud storages (e.g. Cloud A and Cloud B). Databases consists of tables, rows and columns. Databases are easy to store in multiple cloud storages. Our application will act as a combiner and store different parts of the table such as rows and columns in multiple clouds using **Vertical fragmentation** and **horizontal fragmentation**. These rows and columns will be converted into hash value using **hash function** algorithm and stored in each clouds. During response our application combines the data and sends to the verifier. Files are stored in multiple clouds using cryptographic data splitting. The file is split into fragments and stored in distinct cloud servers with encrypted key. Thus once the authorized token for the specific file is requested, searchable encryption allows keyword search on encrypted data and combines the fragments. This is sent to the verifier.

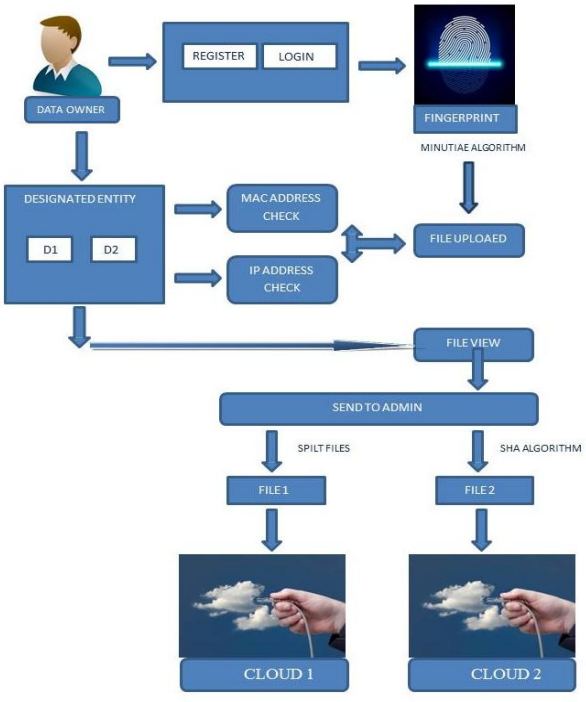

Fig. 2 Architecture Diagram

Data Storage

A cloud server is defined as an entity which contains huge data storage managed by cloud service provider. This paper focuses on providing high security for user data in public cloud storages because there is a huge demand of security prospects in public cloud storages. Security threats may include some authorities (i.e., coercers) may force cloud storage providers to reveal user secrets or confidential data on the cloud and cloud based attacks. For Cloud storage we have configured public clouds. Public clouds is a personal cloud storage service (sometimes referred to as an online backup service) that is frequently used for file sharing and collaboration. The service provides 2 gigabytes (GB) of storage for free and up to 100 GB on various for-fee plans. cloud storage as mostly used two storage are, (**CloudMe,DropBox)**. File to split and store to encrypt formats.

Elimenating Cryptographic Certificate

To eliminate complex cryptographic certificates we used SHA algorithm for converting the plain text to cipher text.

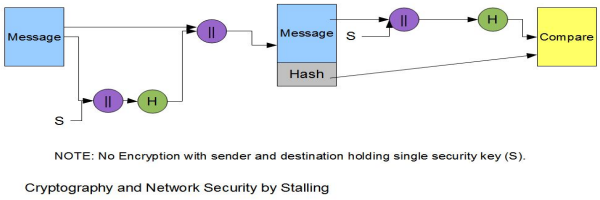

Fig.3 Elimenating cryptographic certificate

1. Append padding bites.
2. Appanding lenght
3. Prepare processing function
4. prepare processing constant...
5. Initializing buffers...
6. Processing messege as 512-bit blocks
7. Pseudo code

IV. ALGORITHM USED

SHA Algorithm

SHA is stand for “Secure Hash Algorithm”. SHA1 is currently the most widely used SHA hash function, although it will soon be replaced by the newer and potentially more secure SHA2 family of hashing functions. It is currently used in a wide variety of applications, including TLS, SSL, SSH and PGP. SHA1 outputs a 160bit digest of any sized file or

input. In construction it is similar to the previous MD4 and MD5 hash functions, in fact sharing some of the initial hash values. It uses a 512 bit block size and has a maximum message size of 2^{64} 1 bits.

Steps:

1. Append Padding Bits….

Message is "padded" with a 1 and as many 0's as necessary to bring the message length to 64 bits less than an even multiple of 512.

2. Step 2: Append Length....

64 bits are appended to the end of the padded message. These bits hold the binary format of 64 bits indicating the length of the original message.

3. Prepare Processing Functions….

SHA1 requires 80 processing functions defined as:

f(t;B,C,D) = (B AND C) OR ((NOT B) AND D) (0 <= t <= 19)
f(t;B,C,D) = B XOR C XOR D (20 <= t <= 39)
f(t;B,C,D) = (B AND C) OR (B AND D) OR (C AND D) (40 <= t <=59)
f(t;B,C,D) = B XOR C XOR D (60 <= t <= 79)

4. Prepare Processing Constants....

SHA1 requires 80 processing constant words defined as:

K(t) = 0x5A827999 (0 <= t <= 19)
K(t) = 0x6ED9EBA1 (20 <= t <= 39)
K(t) = 0x8F1BBCDC (40 <= t <= 59)
K(t) = 0xCA62C1D6 (60 <= t <= 79)

5. Initialize Buffers….

SHA1 requires 160 bits or 5 buffers of words (32 bits):

H0 = 0x67452301
H1 = 0xEFCDAB89
H2 = 0x98BADCFE
H3 = 0x10325476
H4 = 0xC3D2E1F0

6.Processing Message in 512-bit blocks (L blocks in total message)….

This is the main task of SHA1 algorithm which loops through the padded and appended message in 512-bit blocks.

Input and predefined functions:
M[1, 2, ..., L]: Blocks of the padded and appended message
f(0;B,C,D), f(1,B,C,D), ..., f(79,B,C,D): 80 Processing Functions
K(0), K(1), ..., K(79): 80 Processing Constant Words
H0, H1, H2, H3, H4, H5: 5 Word buffers with initial values.

7.Pseudo Code….

For loop on k = 1 to L
(W(0),W(1),...,W(15)) = M[k] */* Divide M[k] into 16 words */*
For t = 16 to 79 do:
W(t) = (W(t-3) XOR W(t-8) XOR W(t-14) XOR W(t-16)) <<< 1
A = H0, B = H1, C = H2, D = H3, E = H4
For t = 0 to 79 do:
TEMP = A<<<5 + f(t;B,C,D) + E + W(t) + K(t) E = D, D = C,
C = B<<<30, B = A, A = TEMP
End of for loop
H0 = H0 + A, H1 = H1 + B, H2 = H2 + C, H3 = H3 + D, H4 = H4 + E
End of for loop.

Minutiae Alogorithm

Minutiae algorithm is minutiae-based matching algorithm in fingerprint recognition systems. Minutia matching is the most popular approach to fingerprint identification and verification. Fingerprint matching usually consist of two procedures: **minutia extraction** and **minutia matching**. The performance mostly depends on the accuracy of the **minutia extraction** procedure. **Minutiae matching** designate the time complexity of applied solution.

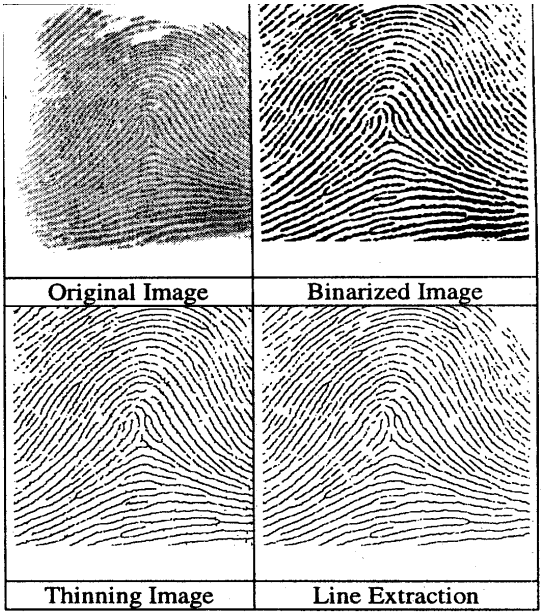

Fig.4 Fingerprint process

V. MODUEL DESCRIPTION

MODULE-1: User Registration:

This module involving the user registration to add the persnol deatils. User has been to including register designation entity(Assstent) beacuse user has been absent or busy time so access the system for designator entity. E.g Nama, DOB,Gender, Email ID, DesignatorEntity Name etc.

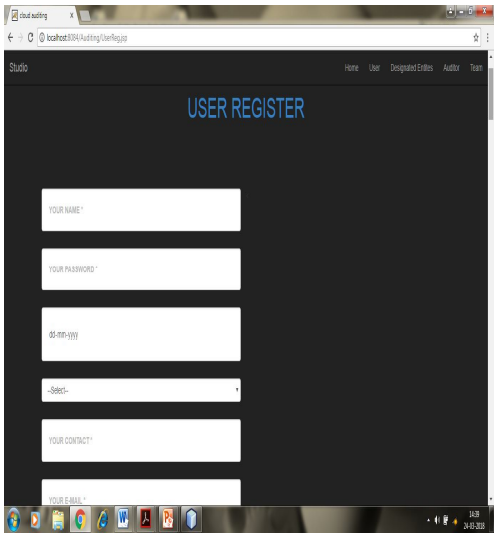

Fig.5 User Registration

MODULE 2- User Login

The module involving use login for webpage after register the details. To login the User account and permission are, File view,File download, File request.File view as list the upload file details. File upload as to store cloud storage. File request as admin to accept permission after download file for user or entity.

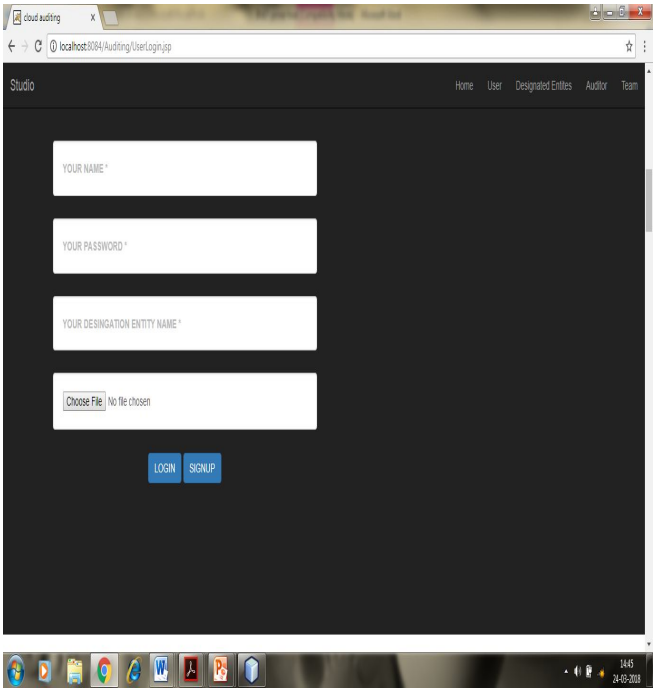

Fig. 6 user login

MODULE 3- User upload file:

User to send designation entity because somtime user not available to send file to admin for designation entity. File sending size as below 50kb.

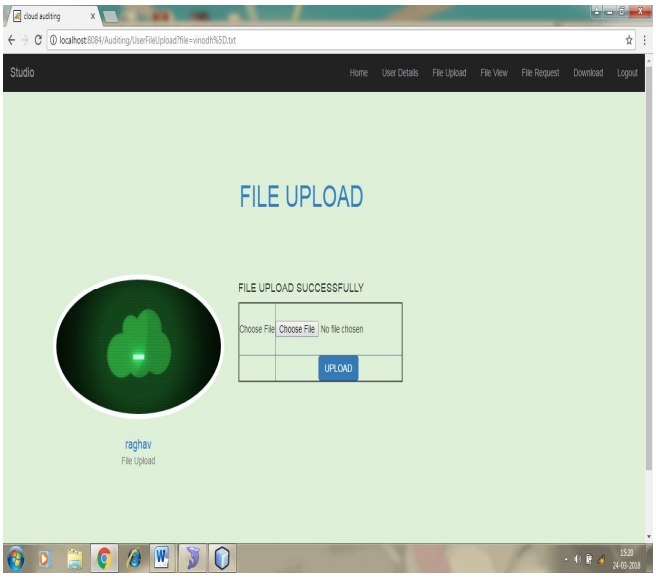

Fig. 7 UserFile Upload

MODULE 4- Entity Fileview:

The module involving entity file can be sent to admin. Entity to access the not only one system so validate MAC address and IP address.

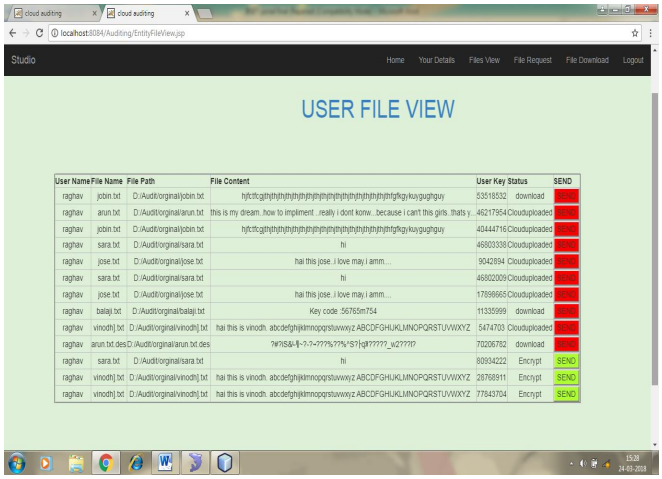

Fig.8 EntityFileview

MODULE 5- Admin File Upload:

The module involving after file send to admin store the in clouds. During upload to cloud split the file and convert to encrypt formats.

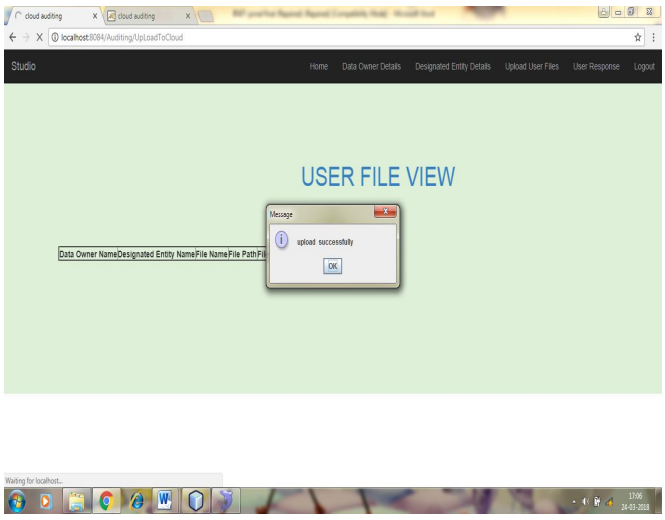

Fig.9 Admin File upload

MODULE-6 User/Entity Request:

The module involving entity/User to download the file first permit to the admin so Entity/User to send file request message. After admin see the MAC address and IP address and accept permission. MAC address and IP address wrong as admin to request permission will be canceled. During request to generate the key after send request permission.

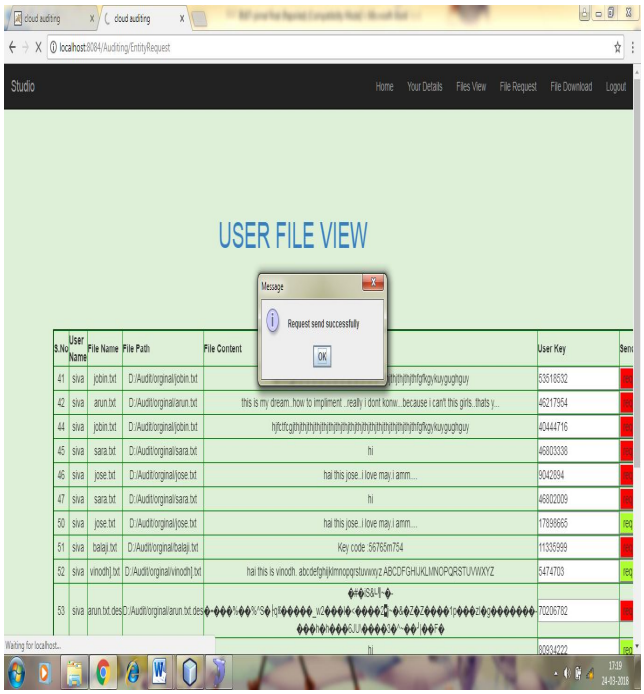

Fig.11 Entity/User request

MODULE-7 Admin Response

The method involving after request the permission entity/user to read details and check MAC address and IP address accept the permission.

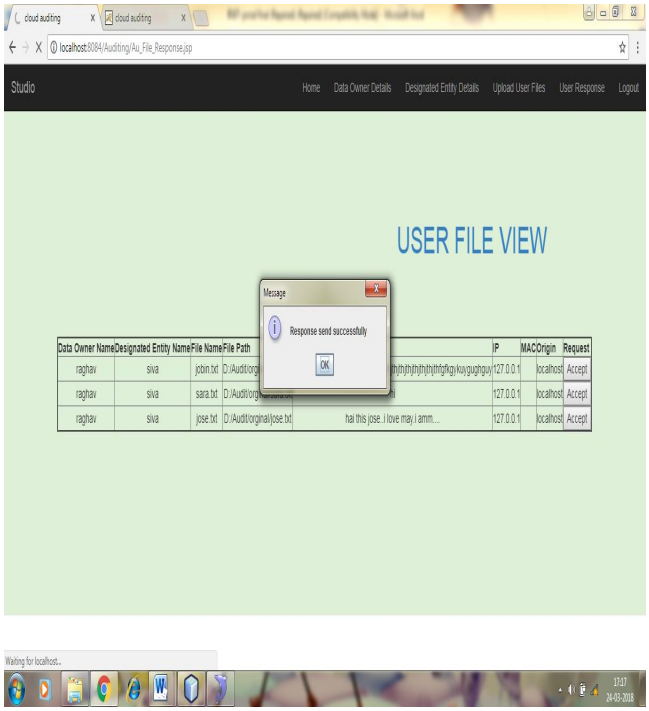

Fig 12 Admin response

MODULE 8- Entity/User download

Method involving after permit the admin to download entity/user doenload the file.During Download file to merge and decrypt formats.

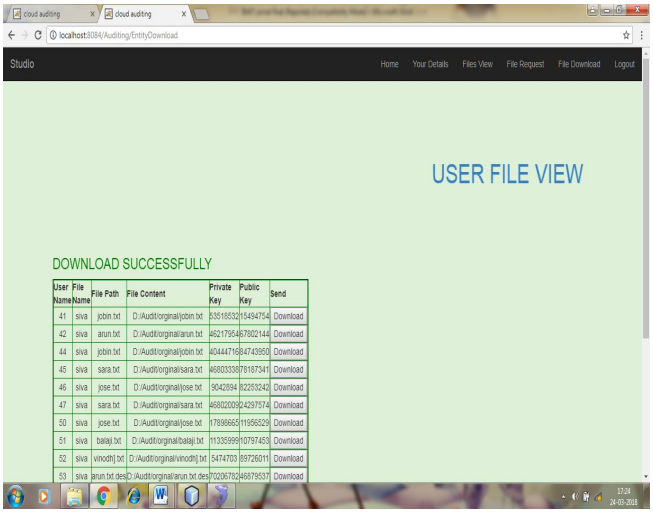

Fig.13 Entity/User download

VI. CONCLUSION AND FUTURE ENCHANCEMENT

we investigated proofs of storage in cloud in a multi-user setting. We introduced the notion of identity based data outsourcing and proposed a secure IBDO scheme. It allows the file-owner to delegate her outsourcing capability to proxies. Only the authorized proxy can process and outsource the file on behalf of the file-owner. Both the file origin and file integrity can be verified by a public auditor. The identity-based feature and the comprehensive auditing feature make our scheme advantageous over existing PDP/PoR schemes. Security analyses and experimental results show that the proposed scheme is secure and has comparable performance as the SW scheme. The use of the biometric as a password has made the ATM transaction system more reliable and secured. The OTP concept added to the system further enhances the security and avoids the need for us to remember passwords. Moreover the system is built on embedded technology which makes it user.

our future enhancement for a secure cloud service provider with biometric authentication and multiple cloud storage system are Dataowner upload PDF files and excel sheets. Future research will include advanced like uploading the pictures, videos in encrypted format for user convenience.

REFRENCES

[1] B. Wang, B. Li, and H. Li, “Panda: Public auditing for shared data with efficient user revocation in the cloud,” IEEE Transactions on Services Computing, vol. 8, no. 1, pp. 92–106, 2015.

[2] F. Chen, T. Xiang, Y. Yang, and S. S. M. Chow, “Secure cloud storage meets with secure network coding,” IEEE Transactions on Computers, vol. 65, no. 6, pp. 1936–1948, June 2016.

[3] Y. Wang, Q. Wu, B. Qin, X. Chen, X. Huang, and J. Lou,“Ownership-hidden group-oriented proofs of storage from prehomomorphic signatures,” Peer-to-Peer Networking and Applications, pp. 1–17, 2016.

[4] T. Jiang, X. Chen, and J. Ma, “Public integrity auditing for shared dynamic cloud data with group user revocation,” IEEE Transactions on Computers, vol. 65, no. 8, pp. 2363–2373, Aug 2016.

[5] X. Fan, G. Yang, Y. Mu, and Y. Yu, “On indistinguishability in remote data integrity checking,” The Computer Journal, vol. 58, no. 4, pp. 823–830, 2015.

[6] Y. Yu, M. H. Au, Y. Mu, S. Tang, J. Ren, W. Susilo, and L. Dong, “Enhanced privacy of a remote data integrity-checking protocol for secure cloud storage,” International Journal of Information Security, vol. 14, no. 4, pp. 307–318, 2015.

[7] Y. Yu, M. H. A. Au, G. Ateniese, X. Huang, W. Susilo, Y. Dai, and G. Min, “Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage,” IEEE Transactions on Information Forensics and Security, 2016.