International Journal of Future Generation Communication and Networking
Vol. 13, No. 3, (2020), pp. 351 - 364

Designing Security for Cloud Storage Using Key Aggregate Cryptosystem

Anjali Dubey, Sonali Markam, Prof. manjusha Talmale

Department of CSE, Guru Nanak Institute Of Technology, Nagpur

Abstract

Data sharing is an important functionality in cloud storage. Cloud computing is a recently developing technology which can be used to access and store data easily. Cloud storage will provide good reliability and lowest cost. Its functionality is sharing data with other users securely, efficiently and flexibly in cloud environment. We introduce a special type of public key encryption called as Key Aggregate cryptosystem (KAC). In KAC user encrypts message with public key and also with an identifier of cipher text. In KAC any set of secret keys can be aggregated and made them as single key. key cryptosystem produces constant size cipher texts and user can aggregate any set of secret keys and make them as compact as single and can decrypt any set of cipher texts by using that compact aggregate key but, files outside the set remain confidential. In this cryptosystem it is possible to efficiently assign decryption rights for the set of cipher texts to any users. The secret key holder can release a constant-size aggregate key for set of cipher texts and this compact aggregate key conveniently shared with others with very limited secure storage.

Keywords:*-- KAC(Key Aggregate cryptosystem), Encryption,Decryption,ECC (Elliptic curve cryptography), public-key cryptosystem, Data sharing..*

1. Introduction

The idea for designing the security system came from Cloud storage is gaining popularity recently. In enterprise settings, we see the rise in demand for data outsourcing, which assists in the strategic management of corporate data. It is also used as a core technology behind many online services for personal applications. Nowadays, it is easy to apply for free accounts for email, photo album, file sharing and/or remote access, with storage size more than 25GB (or a few dollars for more than 1TB). Together with the current wireless technology, users can access almost all of their files and emails by a mobile phone in any corner of the world.

The main purpose of the system is to develop a system that provides proper data security in Cloud storage using key aggregate cryptosystem. In the world of technical life cloud computing has become integral part and also understanding the way of business is changing and is likely to continue changing into the future. Using cloud storage services means that you and others can access and share files across a range of devices and position. Files such as photos and videos can sometimes be unmanageable to email if they are too big or you have a lot of data. You can upload your data to a cloud storage provider means you can speedily circulate your data with the help of cloud service and you can share your data files with anyone you choose. Since cloud computing shares distributed resources via network in the open environment thus it makes less secured. Data security has become a major issue in data sharing on cloud. The main motto behind our system is that it secures the data and generates the key for each transaction so every user can secure our shared data by the third party i.e. unethical hacker. Personal data stored in the Cloud may contain account numbers, passwords, notes, and other important information that could be used and misused by a miscreant, a competitor, or a court of law. These data are cached, copied, and archived by Cloud Service Providers, often without user's authorization and control. The system proposed consist of the key generation logic for cloud server which helps random key generation security. In addition, our system secures the data and generates the key for each transaction.

In this Report following are the important functions/features our project

1. Authentication

ISSN: 2233-7857 IJFGCN

2. Data Encryption and Compression
3. File Sharing in 1 to 1 and 1 to many manner.
4. All types File Upload/Download
5. Key Aggregation Services

Our System is a Web Based Application it provides a Single Platform where admin/user can Share and download the file in secured manner this will done by using ECC .

2. Literature Survey

Recently, lots of institutes outsource data storage to the cloud such that a member (owner) of an organization can easily share data with other members (users). Just due to presence of security concerns in the cloud, both owners and users are suggested to verify the integrity of cloud data with Provable Data Possession (PDP) before further utilization on data. However, previous methods either unnecessarily reveal the identity of a data owner to the untrusted cloud or any public verifiers, or introduce significant overheads on verification metadata to preserve anonymity. In this paper, we propose a simple and efficient publicly verifiable approach to ensure cloud data integrity without sacrificing the anonymity of data owners nor requiring significant verification metadata. Our purpose, decouples the anonymity protection mechanism from the PDP. So that institutes can employ its own anonymous authentication mechanism, and the cloud is oblivious to that since it only deals with typical PDP-metadata, consequently, there is no extra storage overhead when compared with existing non-anonymous PDP solutions. Security analyses prove our scheme is secure, and experiment results demonstrate our scheme is efficient [10].

Remotely store their own data by users and enjoy the ondemand high-quality services and applications from a shared pool of configurable computing resources, without the burden of local data storage and maintenance using cloud storage. Additional, users should be use the cloud storage as if it is local, without worrying about the need to verify its integrity. For cloud storage, enabling public audit ability is of critical importance so that users can resort to a third-party auditor (TPA) to check the integrity of outsourced data and be worry free. Safely presents an effective TPA, the auditing process should bring in no new vulnerabilities toward user data privacy, and introduce no additional online burden to user. Secure cloud storage system supporting privacy-preserving public auditing is proposed in this paper. Further enhance our result to enable the TPA to perform audits for multiple users efficiently and simultaneously. Performance and extensive security analysis show the proposed schemes are provably secure and highly efficient. Our preliminary experiment conducted on Amazon EC2 instance further demonstrates the fast performance of the design [15].

3. System Architecture

Basically whenever a user wants to use the system he/she is required to register onto the system if not registered. After registration the email is verified by sending the temporary password on mail itself. Ones the user has id and password he can login

ISSN: 2233-7857 IJFGCN

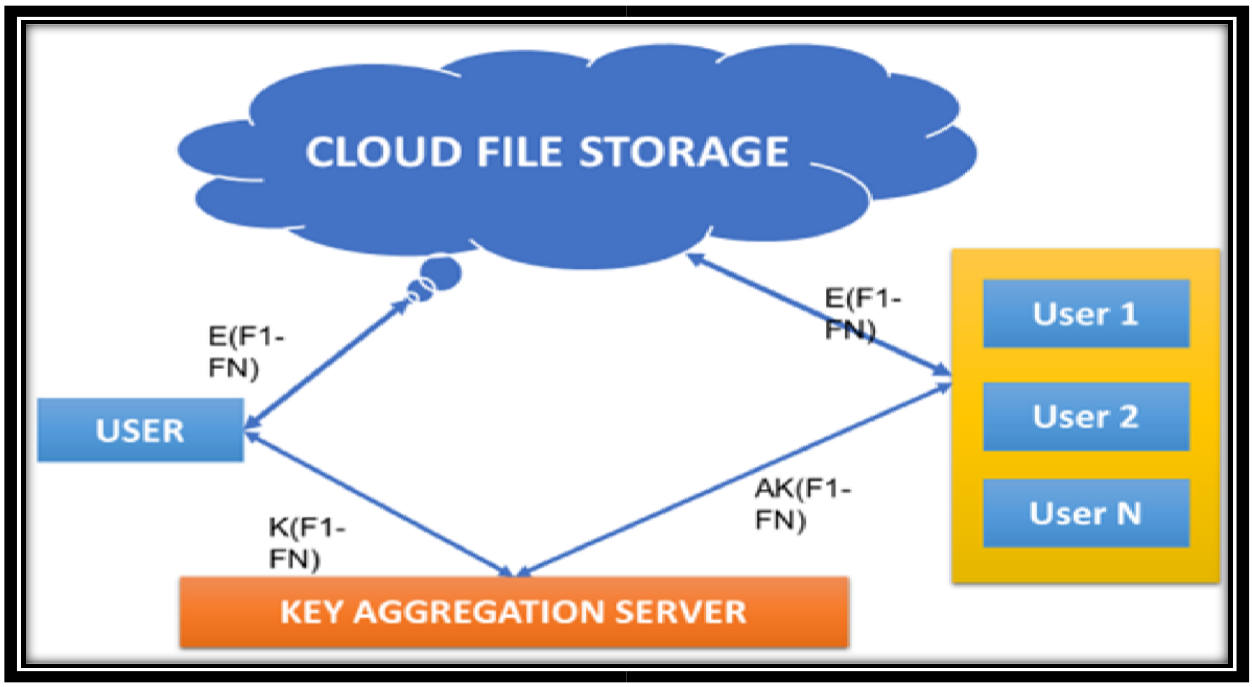


Fig -3.1 System A rchitecture

Key Aggregate Cryptosystem

A Key-Aggregate Cryptosystem consists of the following algorithms:

1. **Setup(1λ ,n):** It takes input the number of cipher text classes „n‟ and group order parameter „λ‟ and gives public and private parameters as a output. The data owner executes the setup phase.
2. **KeyGen ():** Outputs the public key „PK‟ and master secret key „msk‟ pair. This phase also gets executed by data owner.
3. **Encrypt(PK,i,m):** Takes input public key „PK‟, cipher text class „i‟ and the message „m‟ and gives output the cipher text „C‟. This phase is executed by any user who wants to store the encrypted data on cloud storage.
4. **Extract(msk,S):** Takes input the master secret key „msk‟ and a subset S⊆ {1,2,….n} and computes the aggregate key „Ks „ for the given subset of cipher text classes. This phase is executed by data owner for providing decryption rights for a particular set of ciphertexts classes to particular user.
5. **Decrypt(Ks ,S,i,C={c1,c2,c3,…}):** Takes input as the aggregate key „Ks ‟ corresponding to a subset S⊆ {1,2,..n}, the cipher text class „i‟ and the set of cipher texts „C‟ and gives output as a decrypted message „m‟ . This phase is executed by user who got aggregate key and decryption authority.

ISSN: 2233-7857 IJFGCN

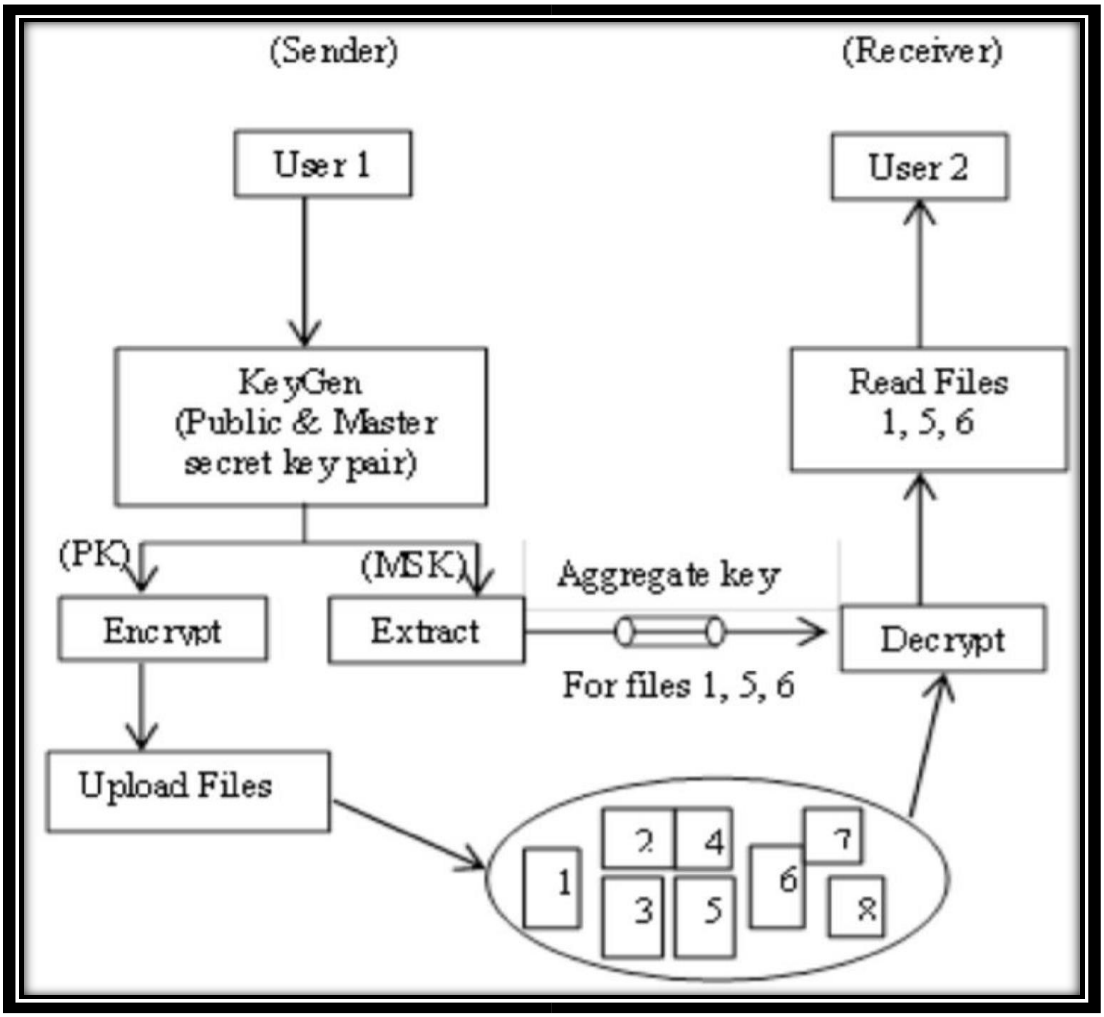


Fig 3.2 :-Key -Aggregate Cryptosystem Data Flow

4. System Flowchart

At first, we have to visit our website/system, after that if the user is already register then he can directly login otherwise user must have to register first then login.

After login user can perform following operations:

File Upload

File Download

File Share

File Delete

LOGOUT

ISSN: 2233-7857 IJFGCN

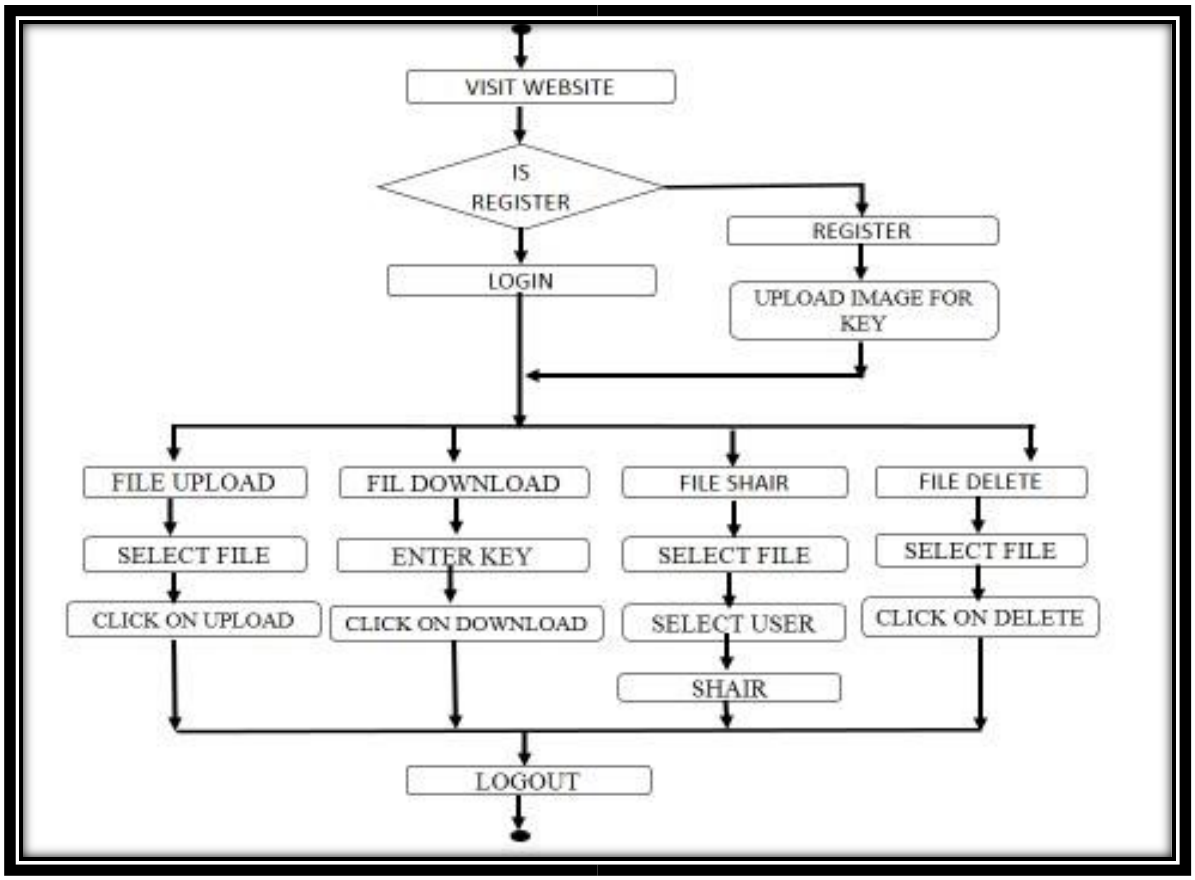


Fig 3.3: System Flow

In ABS, an underwriter, who have a set of qualities from the power, can sign a message with a predicate that is fulfilled by his attributes [1] specifically, the mark cover the ascribes used to fulfil the predicate and any distinguishing data about the endorser (that could connect different marks as being from the comparative underwriter). The cloud environment which contain number of data. To provide more security to these data also protect the user data privacy from the leakages should implement Attribute based signature using image as an attribute method in cloud. It can provide more security against the attacker through Hash algorithm with systems nano time, which generate a random key to the user to provide security to the user from unethical user.

- Key assignment schemes aim to minimize the expense in storing and managing secret keys for general cryptographic use.

- Utilizing a tree structure, a key for a given branch can be used to derive the keys of its descendant nodes (but not the other way round).

- Just granting the parent key implicitly grants all he keys of its descendant nodes. Sandhu proposed a method to generate a tree hierarchy of symmetric keys by using repeated evaluations of pseudorandom function/blockcipher on a fixed secret.

- The concept can be generalized from a tree to a graph. More advanced cryptographic key assignment schemes support access policy that can be modelled by an acyclic graph or a cyclic graph.

ISSN: 2233-7857 IJFGCN

The implementation of the data process includes two processes such as file uploading and downloading.

5. Mathematical Model

Set S = I, P, R, O

Where I = set of all inputs given to the system. (User name, password, encryption key)

P= Set of process to generate the output.

R= Set of rules.

O= Set of Output.

I= α, β, γ, δ α = login (id,password)

- Enter id and password
- Validate with database: Select * from user where userid='id' and password='password'
- if (userid==id and password==password) then
- login successful
- else login unsuccessful β =login result
- if (userid==id and password==password) then
- login successful
- else login unsuccessful γ = pk and mk δ = Pf Where pk=public key, mk= master key and Pf = file to be encrypted. P= p0, p1, p2, p3 P0= Login to system P1= Encrypt (Pf)
- Divide x into two 32-bit halves: xL, xR
- For i = 1to 16:
- x L = XL XOR Pi
- xR = F(XL) XOR xR
- Swap XL and xR

ISSN: 2233-7857 IJFGCN

- Swap XL and xR (Undo the last swap.)

- xR = xR XOR P17
- xL = xL XOR P18

Recombine xL and xR

P2= Generate aggregate key

P3=Decrypt (Ef)

R= R0, R1 R0= Verify (id,password).

R1= Activation Status.

O=O1, O2, O3

O1= Ef encrypted _le

O2= Ak aggregate key pair (pk,msk) where pk-public key and msk-master key O3= Df Decrypted file.

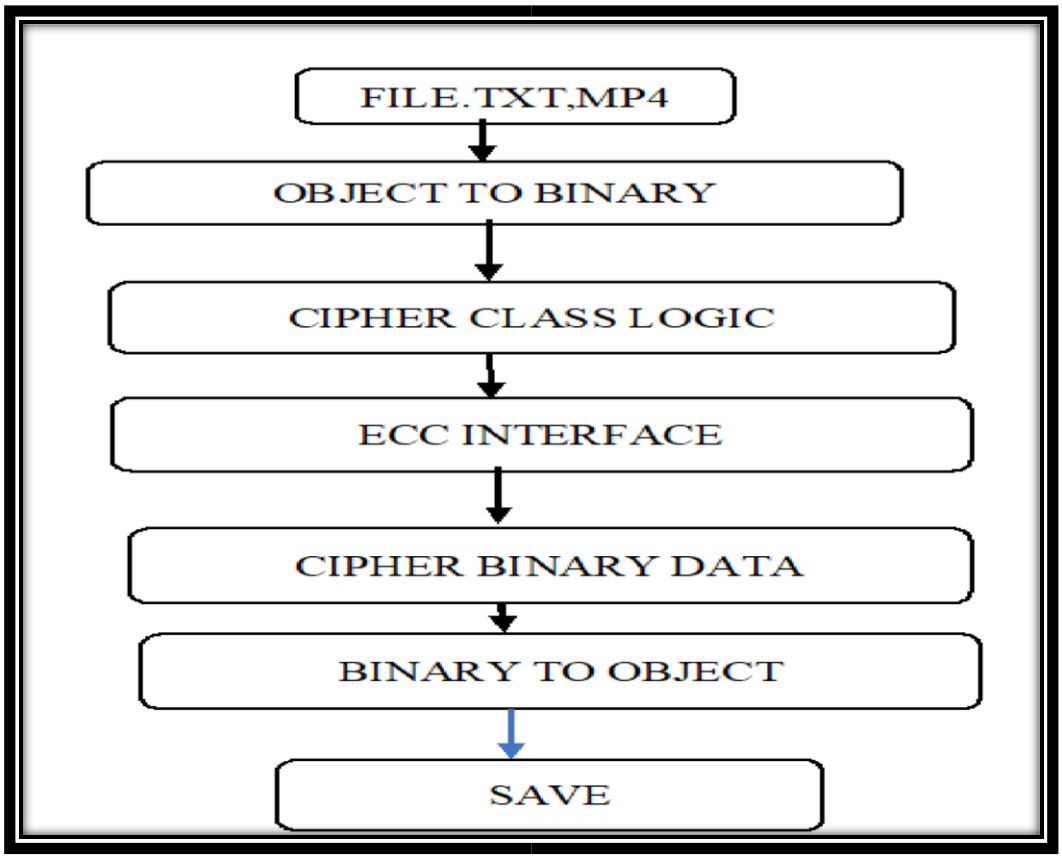
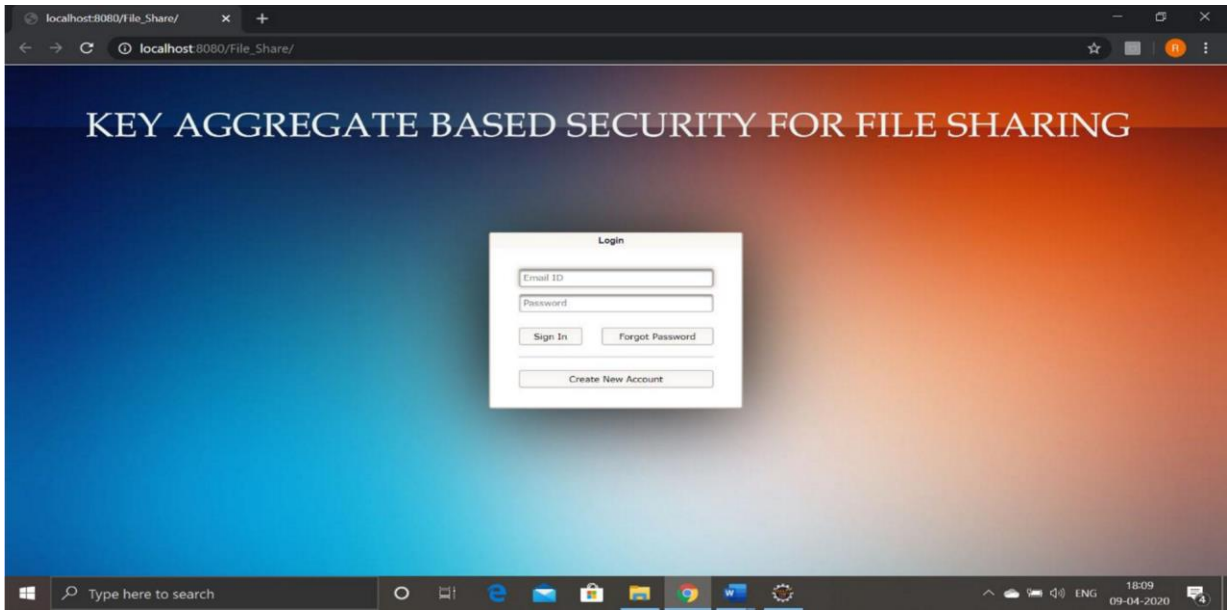


Fig 3.4:PROGRAM FLOW

ISSN: 2233-7857 IJFGCN

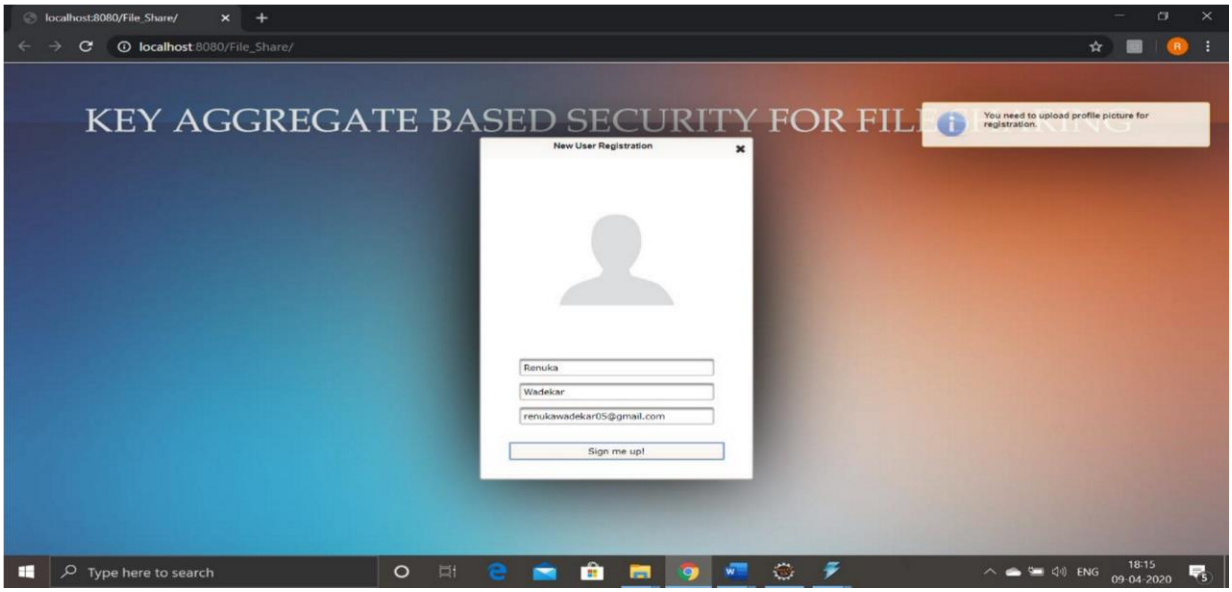
6. Result and Discussion

First have to visit our website/system, after that the following screen will be display.in that you have to log in.



Screenshort 4.1 Login Page

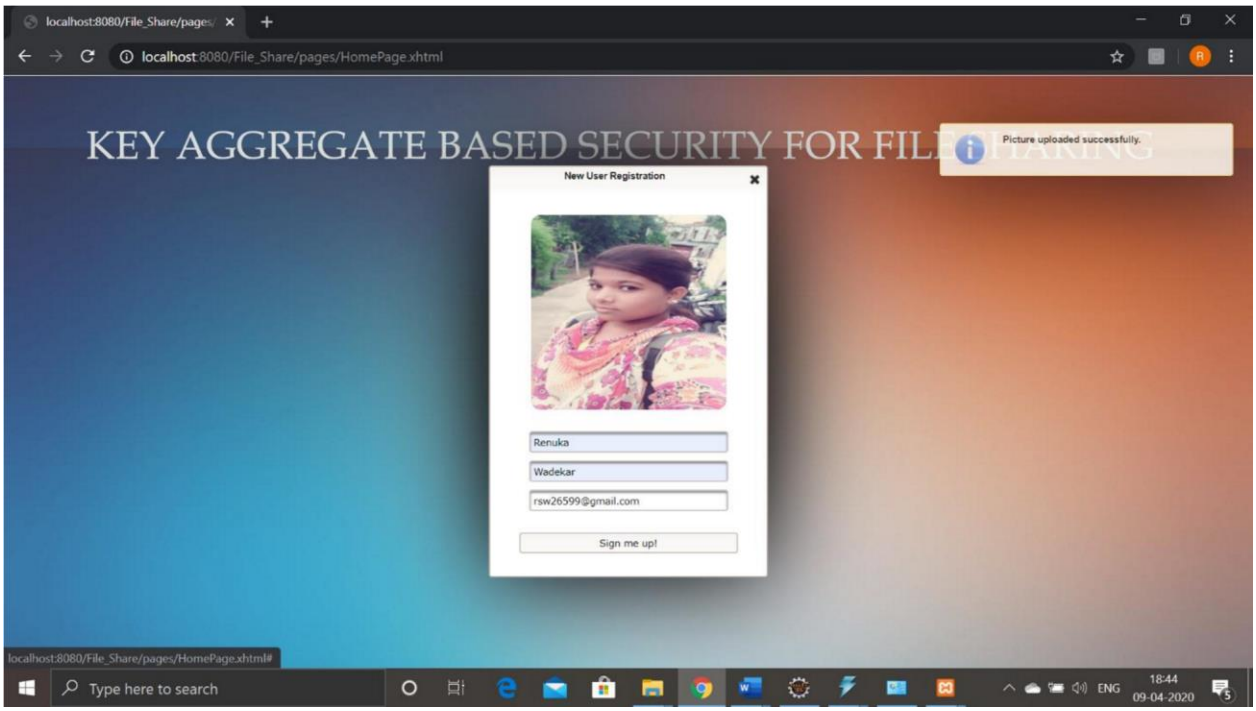
As shown in screen short ,If user is not register then have to register first,then and then user can login into the system.



Screenshort 4.2 User Registration

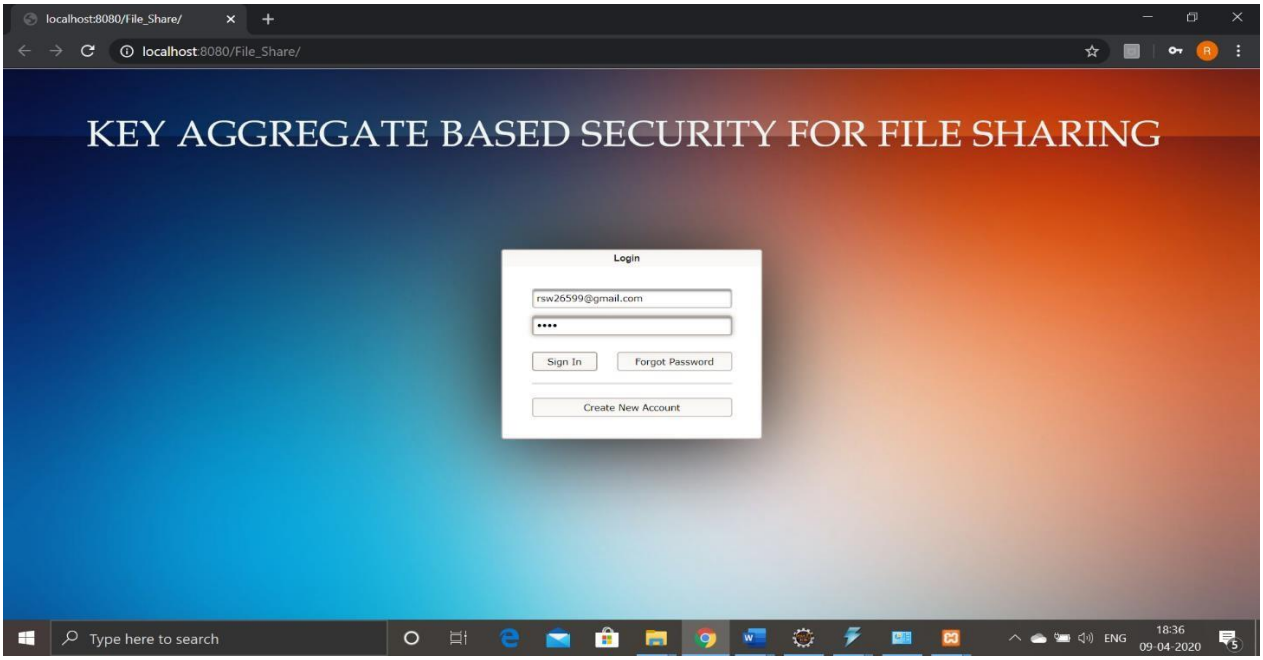
When you are going to register on our system then you must have to uplod profile picture for registration, without profile picture you can not register**.**

ISSN: 2233-7857 IJFGCN



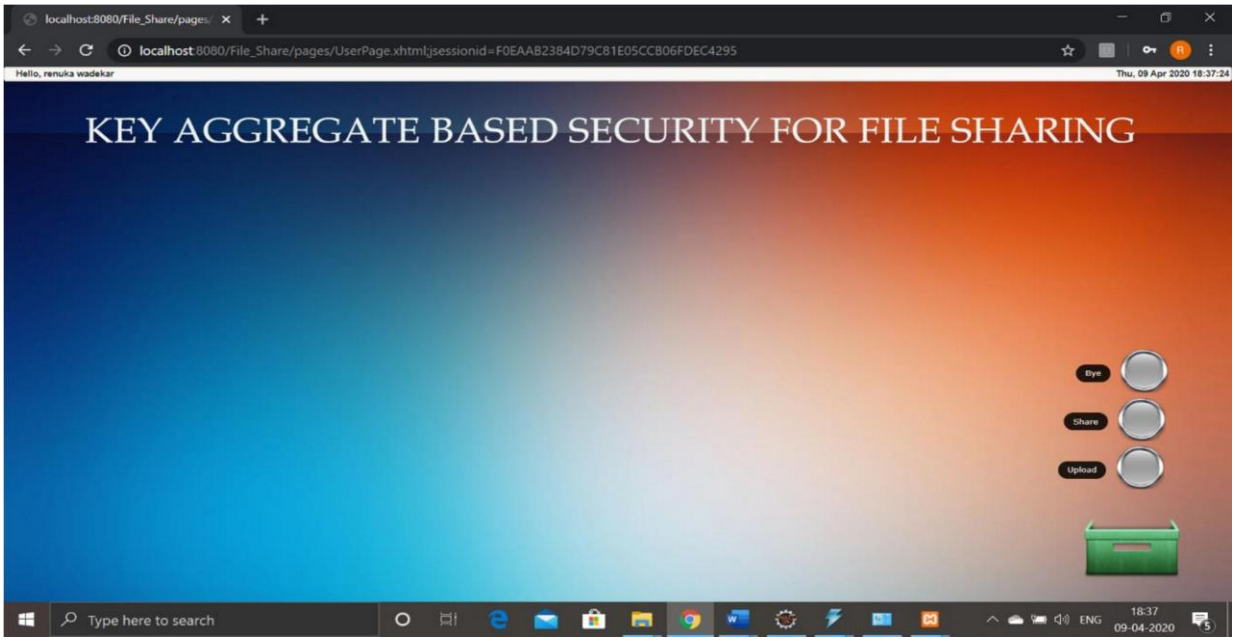
Screenshort 4.3 Signu Up

After successfully uploding picture your registration proccess get completed.then you have to click on sign up.



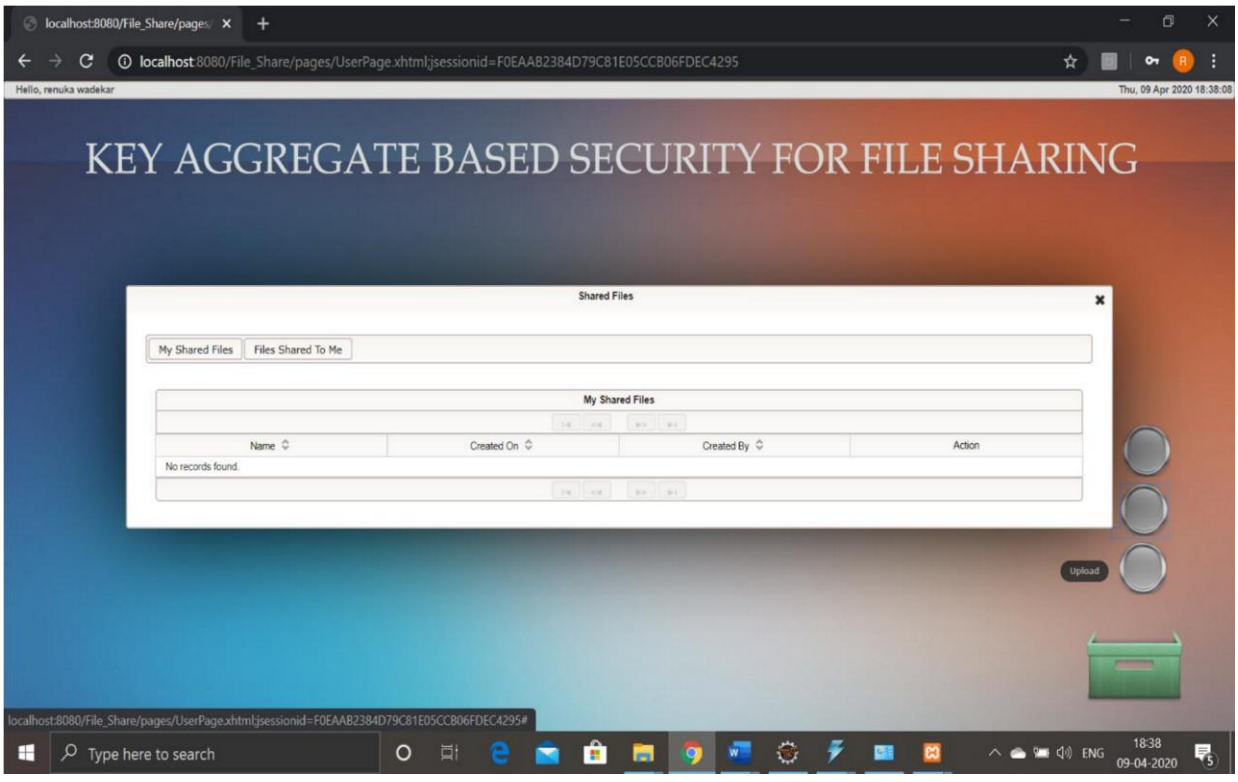
Screenshort 4.4 Sign In After Sign in you get the following page.

ISSN: 2233-7857 IJFGCN



Screenshort 4.5 User View after Sign in.

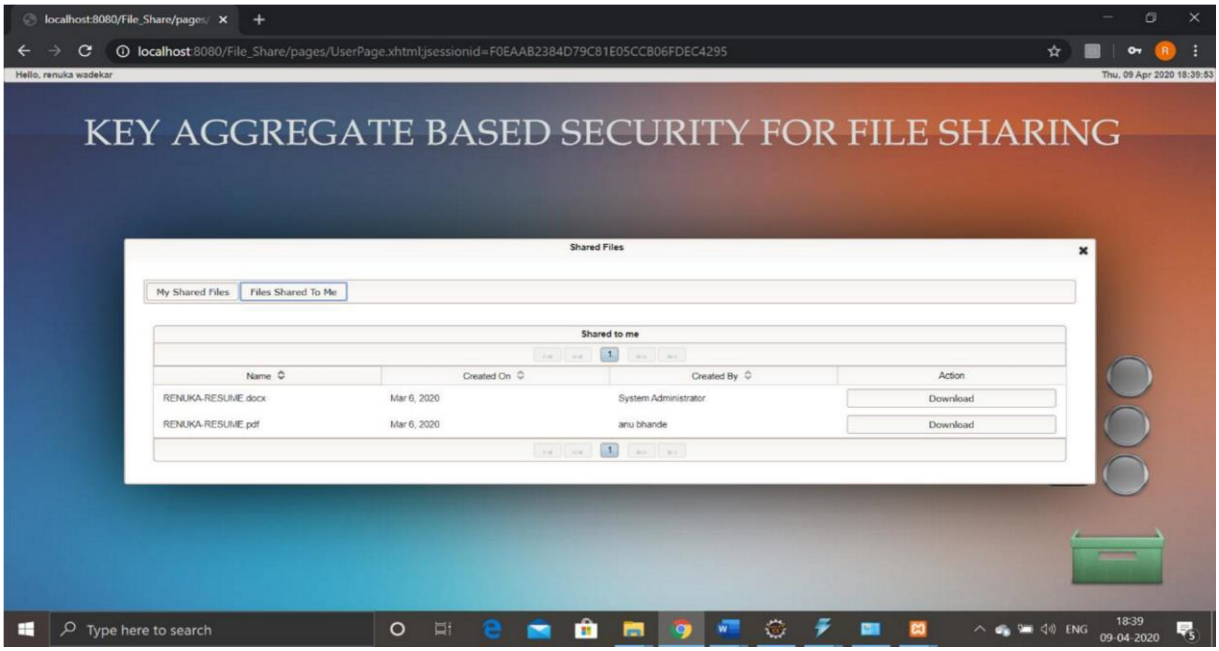
After sign in if user can perform task like uploading and sharing of file.



Screenshort 4.6 file sharing view

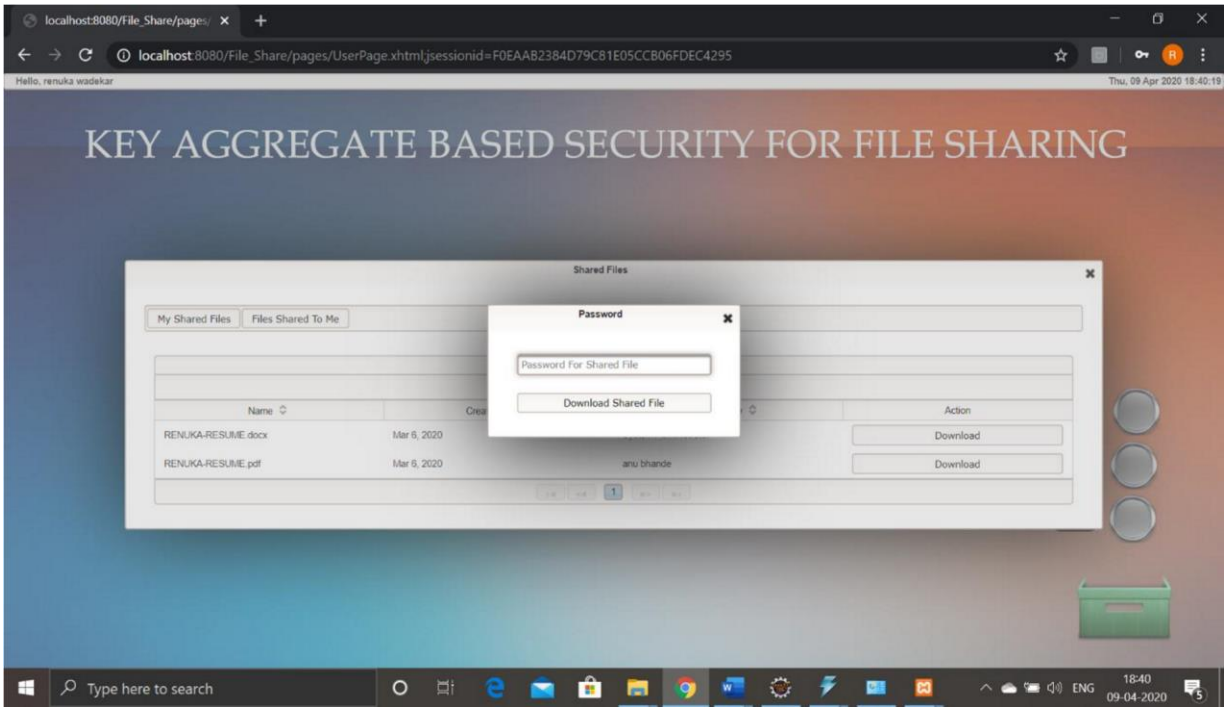
In file shared to me tab the file that shared with me that will be displayed.

ISSN: 2233-7857 IJFGCN



Screenshort 4.7 file shared with me tab

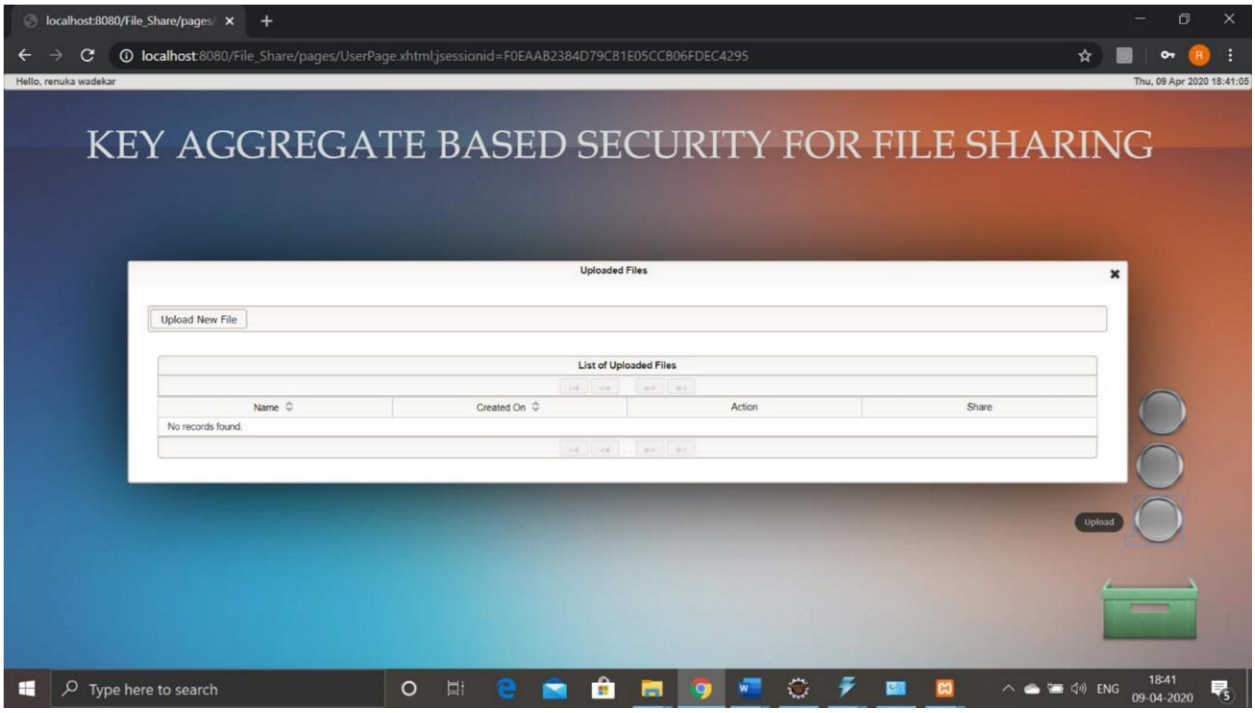
In that view you can download the files by entering the password i.e sent on register email.



Screenshort 4.8 - download the file

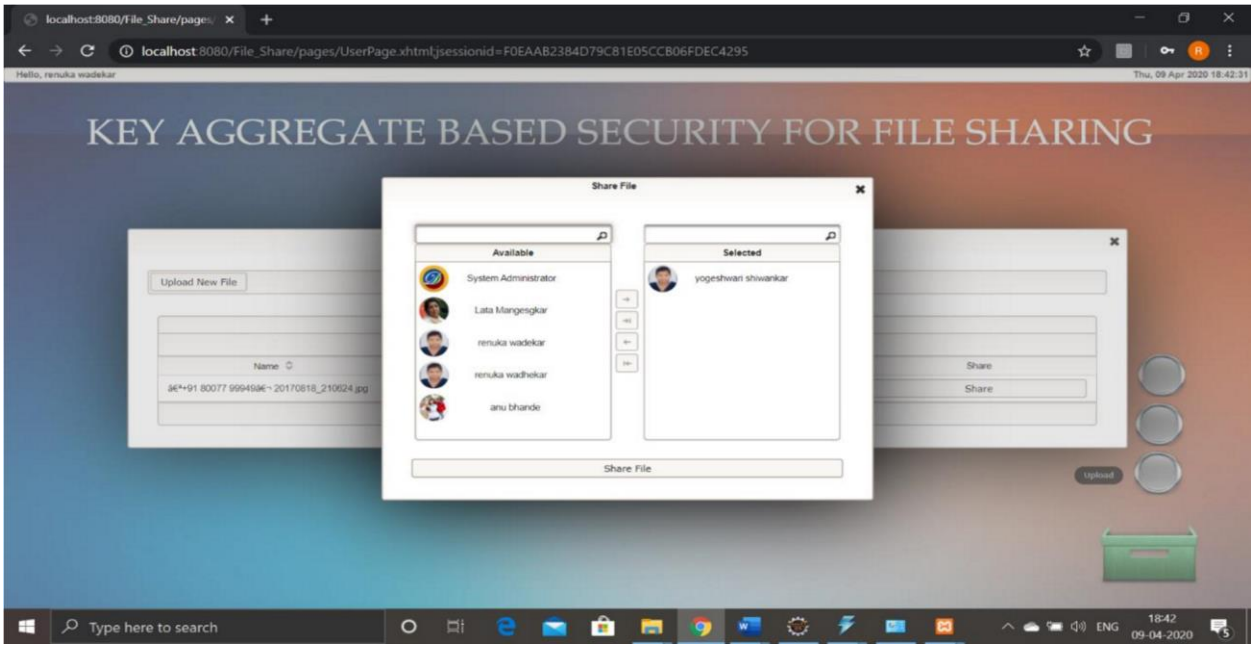
By clicking upload tab user can upload file.

ISSN: 2233-7857 IJFGCN



Screenshort 4.9- user upload view

User can share uploaded file to different user.



Screenshort -4.10 file sharing view

ISSN: 2233-7857 IJFGCN

Following is the user database,each registerd user data will be displayed in database.

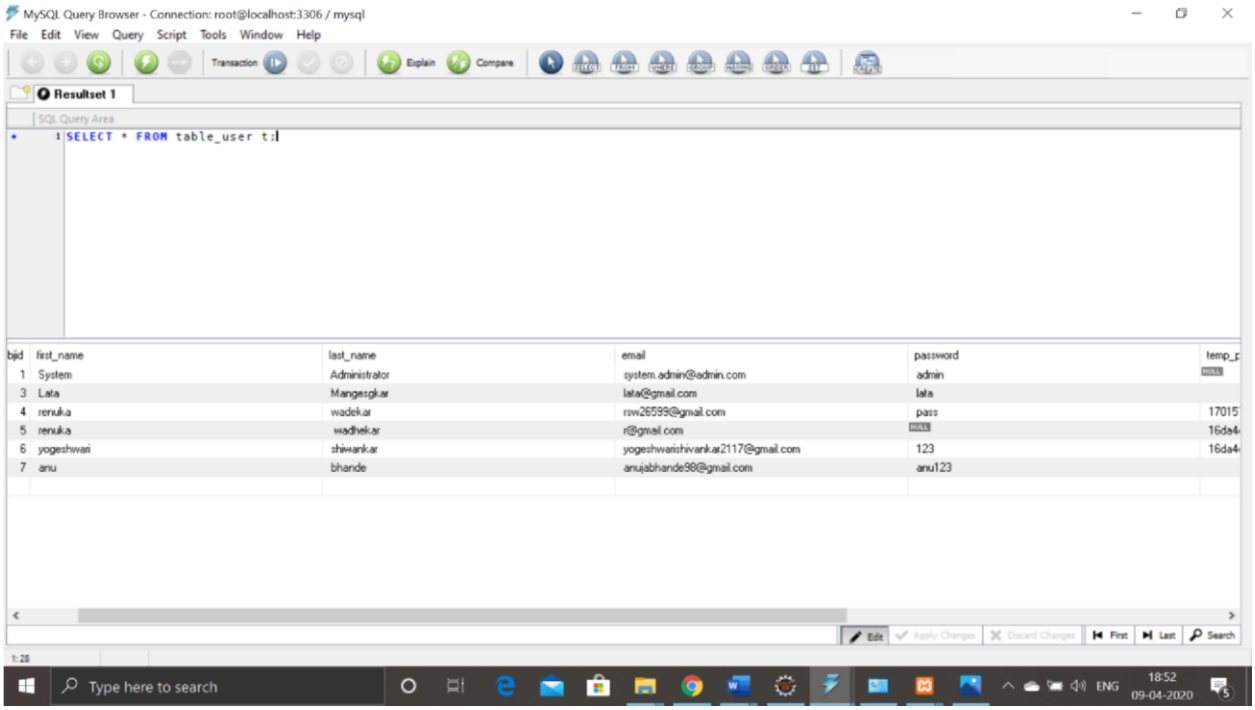


Fig 4.11 User Database

7. Conclusion

The proposed system provides security using Key Aggregation and ECC encryption algorithm. This project servers an alternative to key management systems. The security provided is improvise using a random key generator which uses a key aggregation function. The proposed system can be used in any application which includes data sharing between users (either one to one or many to many) approach.
The main concept of key aggregation will be done for all types of filesw can be shared through cloud storage.

Key sharing is made secured using key aggregation and file sharing is extended to 1 to many manners.
This Key-Aggregate Cryptosystem ensures that the cipher text and aggregate key are of constant size. Use of Elliptic Curve Cryptography (ECC) in addition provides advantage of shorter key length providing faster computations. ECC can provide a level of security with a 164-bit key where other systems require 1024-bit key for same level of security. As ECC provides more security with lower computing power and low resource usage, it is widely used for mobile applications.

References

1. Cheng-Kang Chu, Sherman S.M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng, Senior Member, " Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage" , *IEEE IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS*, VOL. 25, NO. 2, FEBRUARY 2014.
2. Shweta M. Kulkarni, Shubhada S. Kulkarni, " Generation of Shorter Length Keys for Broadcast and Multicast Services Using 2-way Hash

ISSN: 2233-7857 IJFGCN

3. Chain Schemes" *International Journal of Inventive Engineering and Sciences* (IJIES) ISSN: 2319–9598, Volume-1, Issue-10, September 2013.
4. "Hierarchical Identity-based Key Management in Cloud Computing" Wenjun Luo, Min Xu *Journal of Convergence Information Technology(JCIT)* Volume 7, Number 20, Nov 2012.
5. J.Lakshmanaperumal, K.Thanushkodi, N.M.Saravana kumarK.Saravanan, D.Vigneshwaran, T.Purusothaman , "Efficient Key Management Scheme for Secure Multicast in MANET" *IJCSNS International Journal of Computer Science and Network Security*, VOL.10 No.11, November 2010
6. Roy D'Souza1, David Jao,_, Ilya Mironov, and Omkant PandeyD.J.Bernstein and S. Chatterjee,"Publicly Verifiable Secret Sharing for Cloud-Based Key Management" (Eds.): INDOCRYPT 2011, LNCS 7107, pp. 290–309, 2011. Springer-Verlag Berlin Heidelberg 2011
7. "Hierarchical Attribute-Based Secure Outsourcing for Malleable Access in Cloud Computing", S. Usha, Dr. A. Tamilarasi, K. Mahalakshmi *International Journal of Engineering Trends and Technology (IJETT*) – Volume 4 Issue 6- June 2013.
8. "Improving Security and Efficiency in Attribute-Based Data Sharing" JunbeomHur IEEE Transactions on *Knowledge and Data Engineering* Vol: 25 o: 10 2013.
9. "Dynamic Credentials and Cipher text Delegation for Attribute-Based Encryption", AmitSahai UCLAHakanSeyalioglu†, UCLA Brent Watersffi, University of Texas at AustinAugust 1, 2012. D. Chaum and E. van Heyst. Group signatures. *In EUROCRYPT*, pages 257–265, 1991.
10. B. Wang, S. S. M. Chow, M. Li, and H. Li, "Storing Shared Data on the Cloud via Security-Mediator," in International Conference on Distributed Computing Systems - ICDCS 2013. IEEE, 2013
11. S. S. M. Chow, C.-K. Chu, X. Huang, J. Zhou, and R. H. Deng, "Dynamic Secure Cloud Storage with Provenance," in Cryptography and Security: From Theory to Applications - Essays Dedicated to JeanJacques Quisquater on the Occasion of His 65th Birthday, ser. LNCS, vol. 6805. Springer, 2012, pp. 442-464.
12. S. S. M. Chow, Y. J. He, L. C. K. Hui, and S.-M. Yiu, "SPICE - Simple Privacy- Preserving IdentityManagement for Cloud Environment," in Applied Cryptography and Network Security - ACNS 2012, ser. LNCS, vol. 7341. Springer, 2012, pp. 526-543.
13. S. Kamara, C. Papamanthou, T. Roeder. "Dynamic searchable symmetric encryption", Proceedings of the 2012 ACM conference on Computer and communications security (CCS), ACM, pp. 965-976, 2012.
14. Y. Hwang, P. Lee. "Public Key Encryption with Conjunctive Keyword Search and Its Extension to a Multi-user System", In:Pairing-Based Cryptography C Pairing 2007, LNCS, pp. 2-22, 2007.
15. L. Hardesty, "Secure computers aren't so secure," *MIT press*, 2009, http://www.physorg.com/news176107396.html.
16. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted data," in Proceedings of the13th ACM Conference on Computer and Communications Security (CCS "06). ACM, 2006, pp. 89–98.
17. M. Chase and S. S. M. Chow, "Improving Privacy and Security in MultiAuthority Attribute-BasedEncryption," in ACM Conference on Computer and Communications Security, 2009, pp. 121–130.

ISSN: 2233-7857 IJFGCN