IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

IJARSCT
Impact Factor: 6.252

Volume 2, Issue 2, July 2022

Secure File Storage on Cloud Using Hybrid Cryptography

Mr. Shrikanta Jogar[1] and Mr. Darshan S Handral[2]
Assistant Professor[1], Students[2]
Smt Kamala and Shri Venkappa M. Agadi College of Engineering and Technology, Laxmeshwar, India
shree.ahd@gmail.com, darshanhandral@gmail.com

Abstract: *Cloud is used in various fields like industry, military, college, etc. for various services and storage of huge amount of data. Data stored in this cloud can be accessed or retrieved on the users request without direct access to the server computer. The rapidly increased use of cloud computing within the many organization and IT industries provides new software with low cost. Cloud computing is useful in terms of low cost and accessibility of knowledge. Cloud computing gives lot of advantages with low cost and of knowledge accessibility through Internet. Ensuring the safety of cloud computing may be a major think about the cloud computing environment, as users often store sensitive information with cloud storage providers, but these providers could be untrusted. So, sharing data in a secure manner while preserving data from an untrusted cloud remains a challenging issue. Our approach ensures the safety and privacy of client sensitive information by storing data across single cloud, using AES, triple DES and Blowfish algorithm.*

Keywords: Cloud Computing

I. INTRODUCTION

In the proposed system, a method for securely storing files in the cloud using a hybrid cryptography algorithm is presented. In this system, the user can store the file safely in online cloud storage as these files will be stored in encrypted form in the cloud and only the authorized user has access to their files. As in the above figure, the files that the user will upload on the cloud will be encrypted with a user- specific key and store safely on the cloud.

1.1 User Registration

For accessing the services the user must first register yourselves. During the registration process various data like Name , username, password, email id, the phone number will be requested to enter

1.2 Uploading a File on Cloud

- When the user uploads a file on the cloud first it will be uploaded in a temporary folder.
- Then user's file will be split into N parts.
- These all parts of file will be encrypted using cryptographic algorithms. Every part will use a different encryption algorithm.
- These all parts of file will be encrypted using different algorithms that are AES, 3DES, Blowfish.
- After the encryption, the file reassembled and stored in the user`s specific folder. The original file is removed from the temporary folder.
- Then Combining all Encrypted Parts of file.

1.3 Download a File from the Cloud

- When the user requests a file to be downloaded first the file is split into N parts.
- Then these parts of file will be decrypted using the same algorithms with which they were encrypted
- Then these parts will be re-combined to form a fully decrypted file.
- Then file will be sent to the user for download.

DOI: 10.48175/IJARSCT-5861

II. OBJECTIVES OF THE PROJECT

- To achieve a secure platform for storing of files on cloud using Hybrid Cryptography.
- Data Confidentiality: completely protected from unprivileged data users
- To protect data from crypto attacks using hybrid cryptography.
- The Cryptography technique converts original data into ciphertext.
- To illustrate an encryption and decryption method to have key for the stored file.

III. METHODLOGY

3.1 Algorithm Used

A. Advanced Encryption Standard (AES)

The AES algorithm is related to Rijndael`s encryption. Rijndael is a family of encryption algorithms with different keys and block sizes. It consists of a continue serial operations, some of them involve the input of certain outputs (substitutions) and others the mixing of bits (permutations). All AES calculations algorithm is executed in bytes instead of bits. Therefore, for Advanced Encryption Standard, 128 bits of plain data is considered as a block of 16 bytes These 16 bytes are arranged in a 4x4 matrix for the processing. AES algorithm is of three types namely AES-128bit, AES- 192bit, and AES- 256bit. Each iteration encrypts and decrypts data in blocks using keys of either 128-bits or 192-bits or 256- bits, respectively. Rijndael method was enhanced to accept extra block sizes and also extra key lengths, but for AES, those functions were not inherited.

B. Triple Data Encryption Standard (3DES)

In cryptography, 3DES is an inherited enhanced version of DES (Data Encryption Standard). In the Triple DES algorithm, DES is used trice to increase the security level. Triple DES is also referred to as TDES or Triple Data Encryption Algorithm (TDEA).

TDES has following key:

- All keys being different
- Key 1 and key 2 being different & key 1 and key 3 is thesame.
- All keys Being Identical.

TDES is slowly invisible from use, it is maximally replaced by the AES (Advanced Encryption Standard). A far-reaching anomaly is in the digital payments industry, which still uses 2TDES and scatters standards on that basis (e.g. EMV, the standard for inter- operation of "Chip cards", and IC capable POS terminals and ATM's). This guarantees that TDES will remain as an agile cryptographic standard in the future.

3.2 Blowfish

Blowfish is a symmetric block cipher which uses a Fiestal network, 16 rounds of iterative encryption and decryption functional design. The block size used is of 64-bits and key size can vary from any length to 448.Blowfish cipher uses 18 sub arrays each of 32-bit commonly known as P- boxes and four Substitution boxes each of 32-bit, each having 256 entries.

The algorithm design is shown in figure. It consists of two phases: one is Key Expansion phase another is Data Encryption phase. In Key expansion phase, key is converted into several sub-keys and in Data Encryption phase, encryption occurs via 16-round networks. Each round consists of a key dependent permutation and a key and data dependent substitution.

3.3 Flow Diagram

- The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system.
- A data flow diagram is a way of representing a flow of data through a process or a system. The DFD also provides information about the outputs and inputs of each entity and the process itself. Is has no control flow, there are no decision rules and no loops.
- The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system

DOI: 10.48175/IJARSCT-5861

components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.

- DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output.

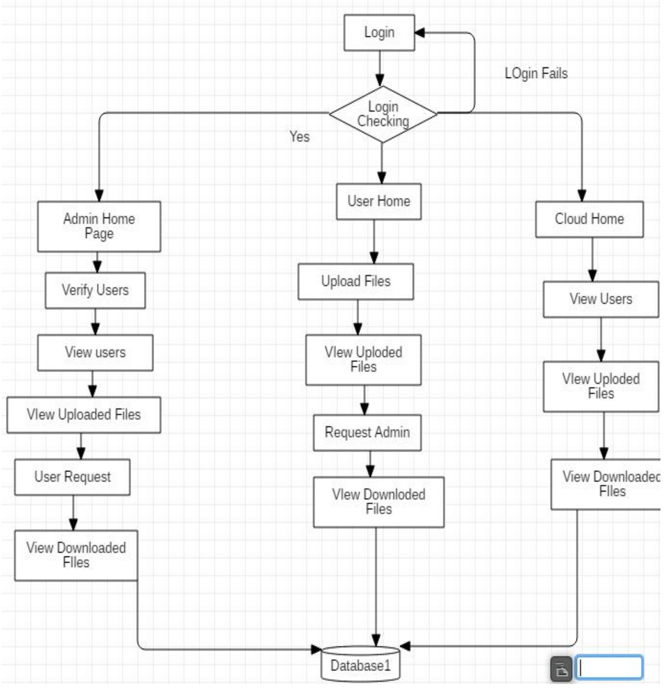


Fig 1: Data Flow diagram

3.4 Sequence Diagram

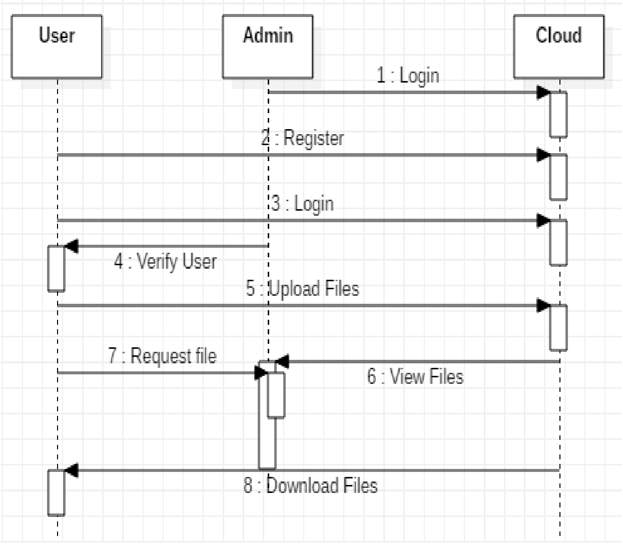


Fig 2 : Sequence diagram

A sequence diagram in Unified Modeling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order. It is a construct of a Message Sequence Chart. Sequence diagrams are sometimes called event diagrams, event scenarios, and timing diagrams.

3.5 Activity Diagram

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modeling Language, activity diagrams can be used to describe the business and operational step-by-step workflows of components in a system. An activity diagram shows the overall flow control.

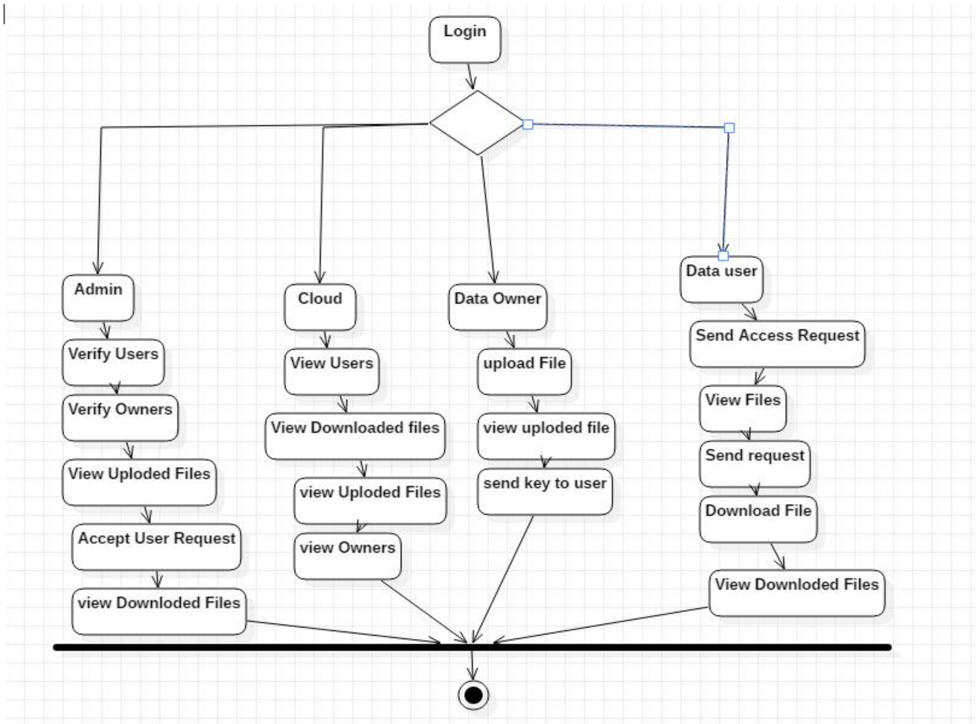


Fig 3: Activity Diagram

IV. REQUIREMENT SPECIFICATIONS

4.1 Hardware Requirement

Hardware is a set of physical components, which performs the functions of applying appropriate, predefined instructions. In other words, one can say that electronic and mechanical parts of computer constitute hardware

- System : Pentium IV 2.4 GHz.
- Hard Disk : 30 GB.
- Floppy Drive : 1.44 Mb.
- Monitor : 15 VGA Colour.
- Mouse : Logitech.
- Ram : 512 Mb.

4.2 Software Requirements

The software is a set of procedures of coded information or a program which when fed into the computer hardware enables the computer to perform the various tasks. Software is like a current inside wire, which cannot be seen but its effect can be felt.

- Operating system : Windows XP/7 and Above
- Coding Language : Python
- Data Base : MYSQL
- IDE : PYCHARM

DOI: 10.48175/IJARSCT-5861

A. Python

Python is a powerful and globally used programming language. Python is often used in as a scripting language. JavaScript embedded in a webpage can be used to control how a web browser such as Firefox displays web content, so JavaScript is a good example of a scripting language.

Python can be used as a scripting language for various applications, and is ranked in the top 5-10 worldwide in terms of popularity. Python is fun to use. In fact, the origin of the name comes from the television comedy series Monty Python's Flying Circus.

B. MYSQL

MYSQL is an open-source relational database management system (RDBMS). Its name is a combination of "My", the name of co-founder Wideness's daughter, and "SQL", the abbreviation for Structured Query Language. A relational database organizes data into one or more data tables in which data types may be related to each other; these relations help structure the data. SQL is a language programmer use to create, modify and extract data from the relational database, as well as control user access to the database. In addition to relational databases and SQL, an RDBMS like MySQL works with an operating system to implement a relational database in a computer's storage system, manages users, allows for network access and facilitates testing database integrity and creation of backups.

C. FLASK

Flask is a micro web framework written in Python. It is classified as a micro framework because it does not require particular tools or libraries. It has no database abstraction layer, form validation, or any other components where pre-existing third-party libraries provide common functions.

V. IMPLEMENTATION

Cloud proprietor transfer the information on cloud worker. Record is part into octet. All aspects of document is encoded all the while utilizing multithreading strategy. Encoded record is put away on cloud worker. Keys utilized for encryption are put away into cover picture. Distributed computing is the multi-client climate .In this beyond what one client can get to record from cloud worker. Cloud client demand for file. On solicitation of record client additionally get steno picture utilizing email which comprise of key data. Switch measure is utilized for translate the document.

5.1 Modules

- Data Owner
- Data User
- Admin
- Cloud

5.2 Modules Description

Data Owner (DO): Owner uploads the data on a cloud server. File is split into octet every part of the file is encoded simultaneously using multithreading technique. Encoded file is stored on cloud server. Keys used for encryption are stored into the cover image. Cloud computing is the multi user environment.

Data User (DU): Cloud user request for file. On request of the file user also gets a key using email which consists of key information. Reverse process is used to decode the file.

Admin: Admin login with username and password, the entered username and password is correct then only admin enter into the home page, if entered details are incorrect admin can't login to home page, after entered into the home page admin act like owner of this application and admin activate and deactivate the user and owner and admin can view all uploaded file details and request details

Cloud: Cloud module can operate by the admin in cloud module having all the registered users and owners details and owner uploaded file details and user downloaded details.

DOI: 10.48175/IJARSCT-5861

VI. RESULTS

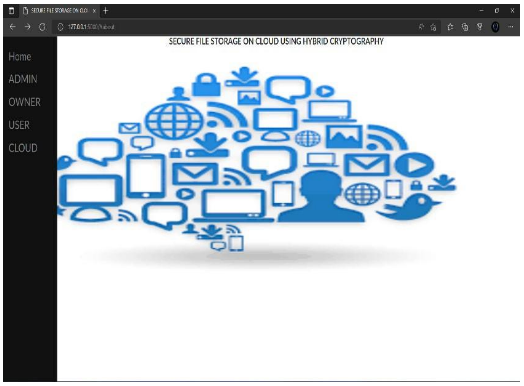


Fig 4 : Homepage

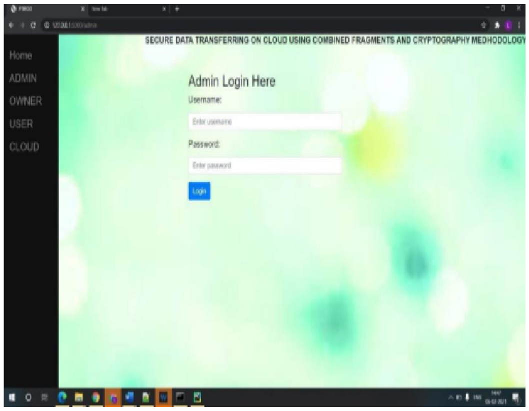


Fig 5: Admin Login Page

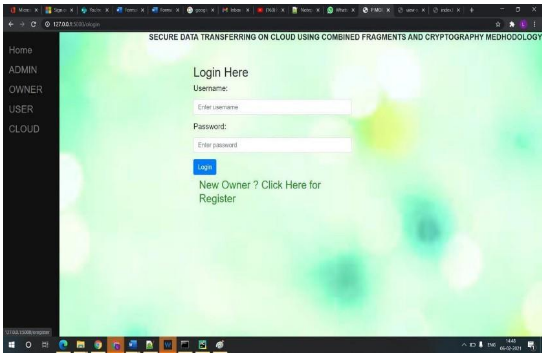

SECURE DATA TRANSFERRING ON CLOUD USING COMBINED FRAGMENTS AND CRYPTOGRAPHY MEDHODOLOGY
Home
ADMIN
OWNER
USER
CLOUD
Login Here
Username:
Enter username
Password:
Enter password
Login
New Owner ? Click Here for Register

Fig 6 : Owner Login Page

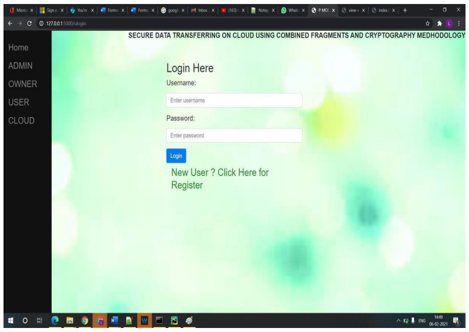
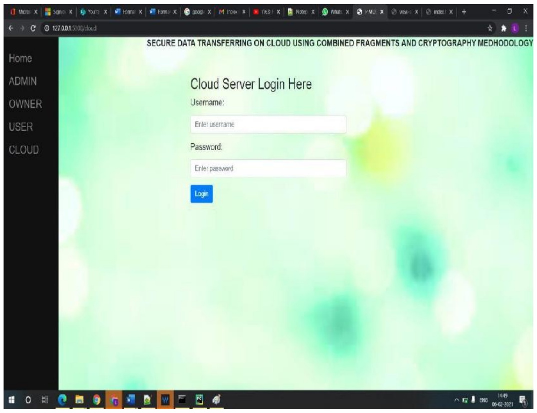

SECURE DATA TRANSFERRING ON CLOUD USING COMBINED FRAGMENTS AND CRYPTOGRAPHY MEDHODOLOGY
Home
ADMIN
OWNER
USER
CLOUD
Login Here
Username:
Enter username
Password:
Enter password
Login
New User ? Click Here for Register

Fig 7 : User Login Page



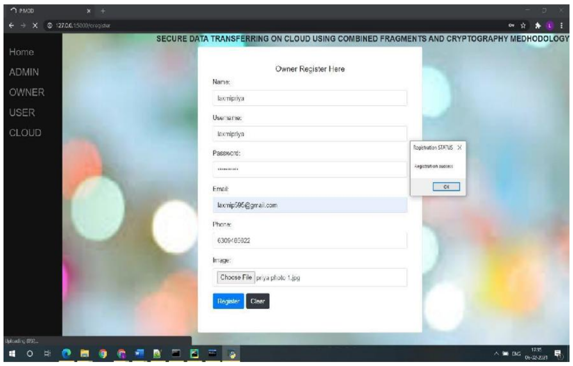
SECURE DATA TRANSFERRING ON CLOUD USING COMBINED FRAGMENTS AND CRYPTOGRAPHY MEDHODOLOGY

Cloud Server Login Here

Username: Enter username

Password: Enter password

Fig 8 : Cloud Login Page



SECURE DATA TRANSFERRING ON CLOUD USING COMBINED FRAGMENTS AND CRYPTOGRAPHY MEDHODOLOGY

Owner Register Here

Name: laxmipriya

Username: laxmipriya

Password: **********

Email: laxmip595@gmail.com

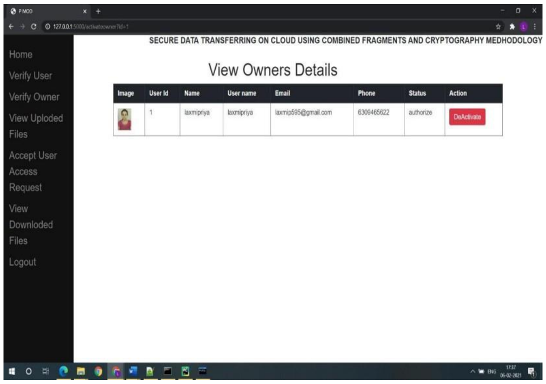
Phone: 6309465622

Image: priya photo 1.jpg

Registration STATUS

Registration success

Fig 9 : Owner Registration Form

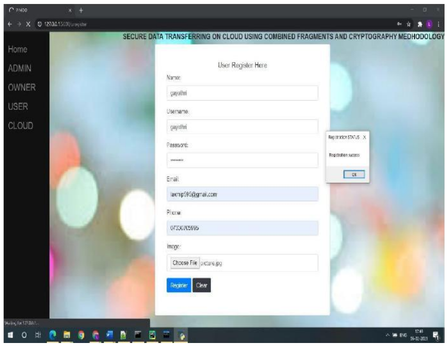


SECURE DATA TRANSFERRING ON CLOUD USING COMBINED FRAGMENTS AND CRYPTOGRAPHY MEDHODOLOGY

View Owners Details

Image	User Id	Name	User name	Email	Phone	Status	Action
	1	laxmipriya	laxmipriya	laxmip595@gmail.com	6309465622	authorize	DeActivate

Fig 10 : Admin Verifying Owner



SECURE DATA TRANSFERRING ON CLOUD USING COMBINED FRAGMENTS AND CRYPTOGRAPHY MEDHODOLOGY

User Register Here

Name: gayathri

Username: gayathri

Password: ********

Email: laxmip595@gmail.com

Phone: 07330705695

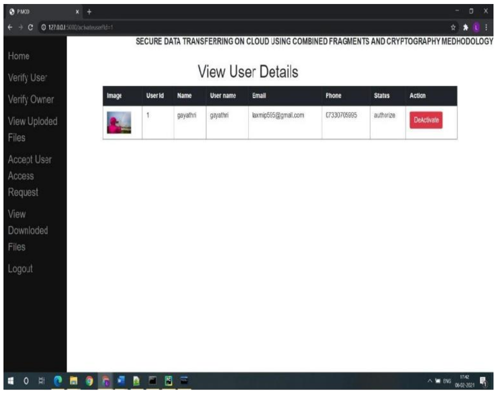
Image: picture.jpg

Registration STATUS

Registration success

Fig 11 : User Registration Form

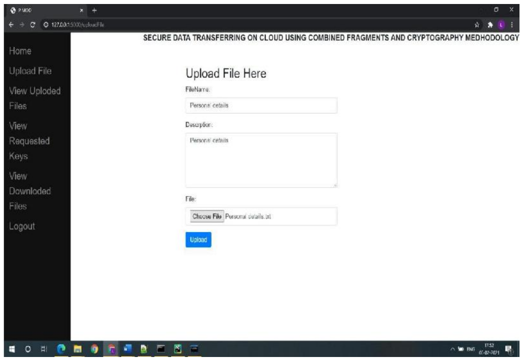
DOI: 10.48175/IJARSCT-5861


P MOD
127.0.0.1:5000/activateuser?id=1
SECURE DATA TRANSFERRING ON CLOUD USING COMBINED FRAGMENTS AND CRYPTOGRAPHY MEDHODOLOGY
Home
Verify User
Verify Owner
View Uploded Files
Accept User Access Request
View Downloded Files
Logout

View User Details

Image	User Id	Name	User name	Email	Phone	Status	Action
	1	gayathri	gayathri	laxmip555@gmail.com	07330705995	authorize	DeActivate

Fig 12 : Owner Uploading File


P MOD
127.0.0.1:5000/uploadFile
SECURE DATA TRANSFERRING ON CLOUD USING COMBINED FRAGMENTS AND CRYPTOGRAPHY MEDHODOLOGY
Home
Upload File
View Uploded Files
View Requested Keys
View Downloded Files
Logout

Upload File Here

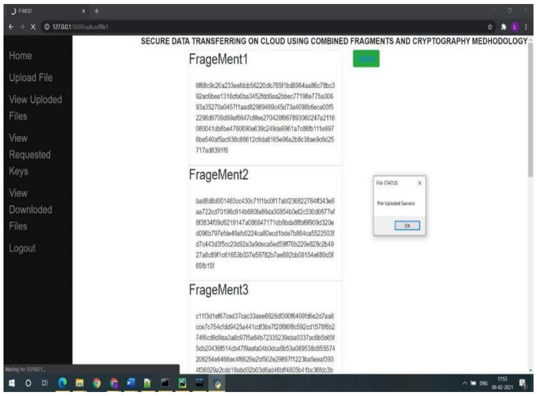
FileName: Personal details

Description: Personal details

File: Choose File Personal details.txt

Upload

Fig 13 : File Uploaded in Fragments


P MOD
127.0.0.1:5000/uploadfile1
SECURE DATA TRANSFERRING ON CLOUD USING COMBINED FRAGMENTS AND CRYPTOGRAPHY MEDHODOLOGY
Home
Upload File
View Uploded Files
View Requested Keys
View Downloded Files
Logout
Upload
OK

FrageMent1

```
6f68c9c20a233eefdcb56220cfc765f1bd8964aa86c78bc3
92ac6bea1316cfa0ba3452fdd6aa2bbec77198e775a306
93a35270a0457f1aad82989469c45d73a4098b6eca03f5
2298d9709d99af6647c8fee270428f967893060247a2116
080041db6be4760690e639c249de9961a7c86fb111e997
6be540af5ac938c86612c9da8165e96a2b8c38ae9c6d25
717ad8391f6
```

FrageMent2

```
bad8d8d001463cc430c71f1bd0f17abf236822784ff343e6
aa722cd70196c914b680fa86da30854b0ef2c330d0877ef
8f3834f09d6219147a086647171db9bda8ffbf6f909d320e
d096b797efde49afc0224ca80ecd1bde7b864ca5522503f
d7c443d3f5cc20d92a3a9deca5ed59ff70b220e828c2b49
27a8c89f1c61653b037e59782b7ae892bb08154e680d5f
65fb15f
```

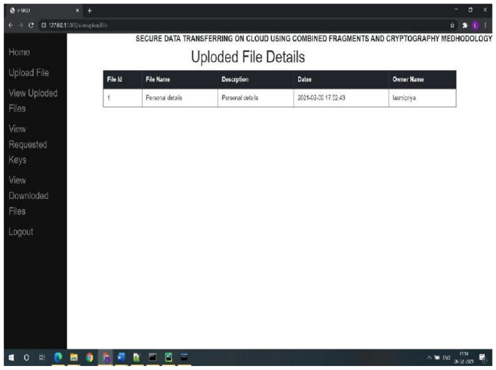
FrageMent3

```
c11f3d1ef67ced37cac33aee8626df390f6409fd6e2d7aa8
cce7c754cfdd9425a441cdf3be7f20f86f8c592cd1578f6b2
74f6cd9d9aa3a8c97f5a64b72335239eba0337ac6b5b65f
5db20436f514db47f9aefa04b0dca6b53a089538d855574
206254e6466ec4f6629e2bf502e29867f1223ba5eeaf393
4f36029a2cdd18ebd02b03d6ad46bff4805b41bc36fdc3b
```

File STATUS

File Uploded Success

Fig 14 : File Uploaded in Fragments

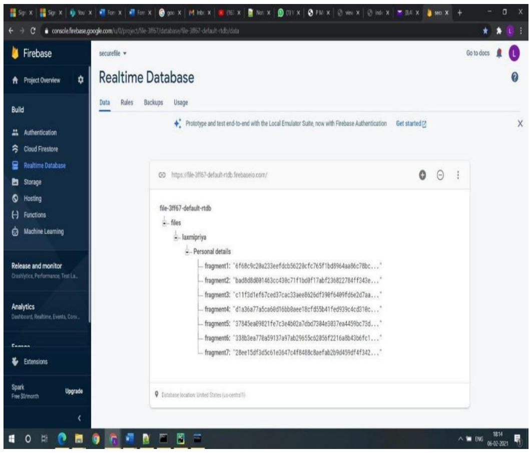

P MOD
127.0.0.1:5000/viewuploadFile
SECURE DATA TRANSFERRING ON CLOUD USING COMBINED FRAGMENTS AND CRYPTOGRAPHY MEDHODOLOGY
Home
Upload File
View Uploded Files
View Requested Keys
View Downloded Files
Logout

Uploded File Details

File Id	File Name	Description	Datee	Owner Name
1	Personal details	Personal details	2021-02-06 17:52:43	laxmipriya

Fig 15: Uploaded File

DOI: 10.48175/IJARSCT-5861



Realtime Database

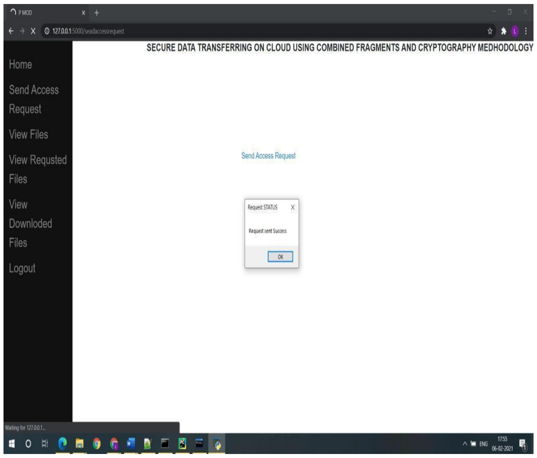
Prototype and test end-to-end with the Local Emulator Suite, now with Firebase Authentication

https://file-3ff67-default-rtdb.firebaseio.com/

```
file-3ff67-default-rtdb
 - files
    - laxmipriya
       - Personal details
          fragment1: "6f68c9c20a233eefdcb56220cfc765f1bd8964aa86c78bc..."
          fragment2: "bad8d8d001463cc430c71f1bd0f17abf236822784ff343e..."
          fragment3: "c11f3d1ef67ced37cac33aee8626df390f6409fd6e2d7aa..."
          fragment4: "d1a36a77a5ca60d16bb8aee18cfd55b41fed939c4cd310c..."
          fragment5: "37845ea09821fe7c3e4b02a7dbd7304e3037ea4459bc73d..."
          fragment6: "338b3ea770a59137a97ab29655c62056f2216a8b43b6fc1..."
          fragment7: "28ee15df3d5c61e3647c4f8488c8aefab2b9d459df4f342..."
```

Database location: United States (us-central1)

Fig 16: File Uploaded in Cloud

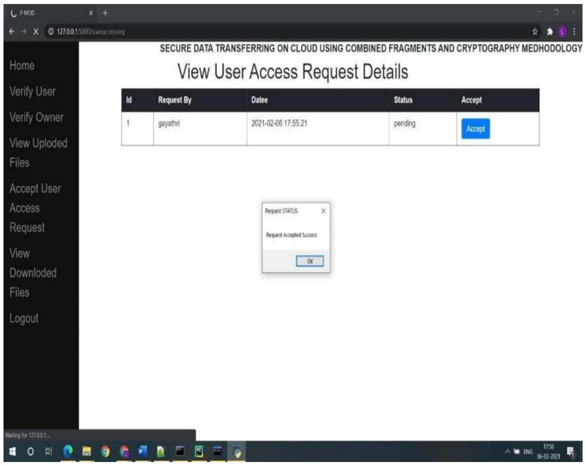


SECURE DATA TRANSFERRING ON CLOUD USING COMBINED FRAGMENTS AND CRYPTOGRAPHY MEDHODOLOGY

Request STATUS

Request sent Success

Fig 17: User Sending Access Request to view Files



SECURE DATA TRANSFERRING ON CLOUD USING COMBINED FRAGMENTS AND CRYPTOGRAPHY MEDHODOLOGY

View User Access Request Details

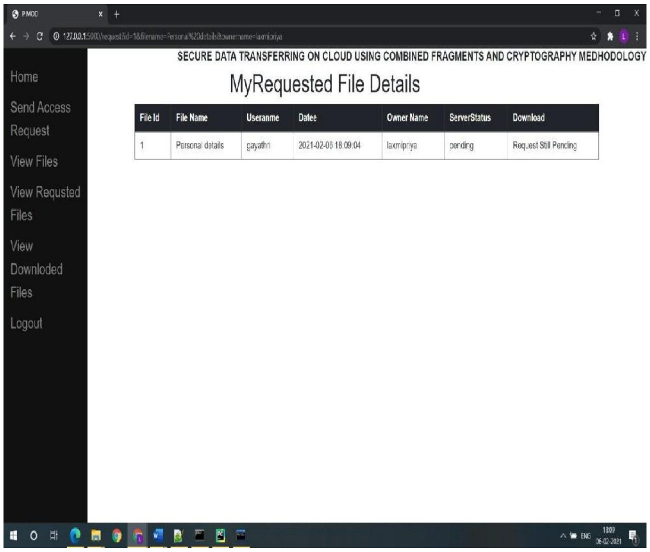
Id	Request By	Datee	Status	Accept
1	gayathri	2021-02-06 17:55:21	pending	Accept

Request STATUS

Request Accepted Success

Fig 18: Admin Accepting Request

DOI: 10.48175/IJARSCT-5861

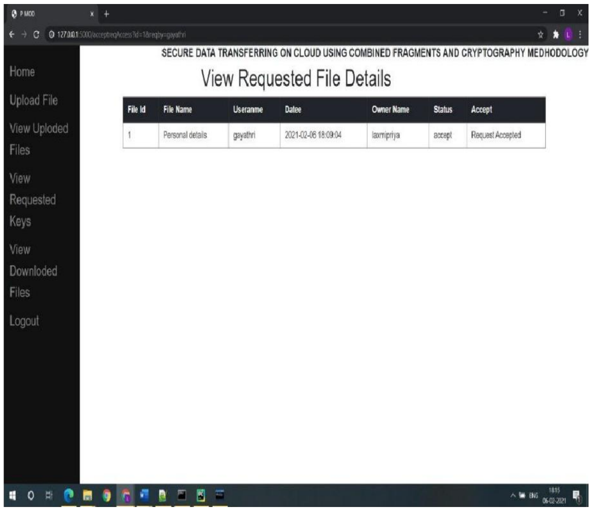


SECURE DATA TRANSFERRING ON CLOUD USING COMBINED FRAGMENTS AND CRYPTOGRAPHY MEDHODOLOGY

MyRequested File Details

File Id	File Name	Useranme	Datee	Owner Name	ServerStatus	Download
1	Personal details	gayathri	2021-02-06 18:09:04	laxmipriya	pending	Request Still Pending

Fig 19: User Sending Request to Owner for Downloading

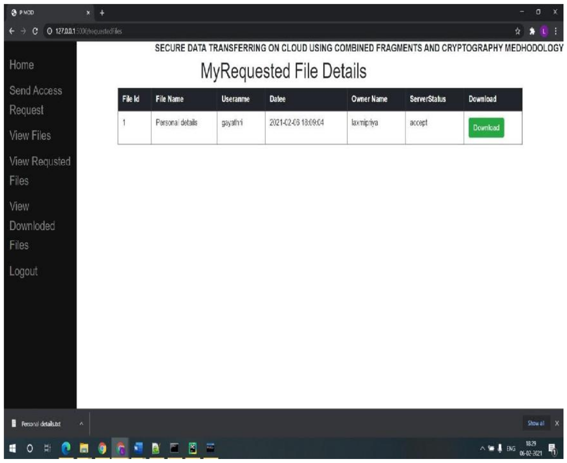


SECURE DATA TRANSFERRING ON CLOUD USING COMBINED FRAGMENTS AND CRYPTOGRAPHY MEDHODOLOGY

View Requested File Details

File Id	File Name	Useranme	Datee	Owner Name	Status	Accept
1	Personal details	gayathri	2021-02-06 18:09:04	laxmipriya	accept	Request Accepted

Fig 20 : Owner Accepting Request of User.



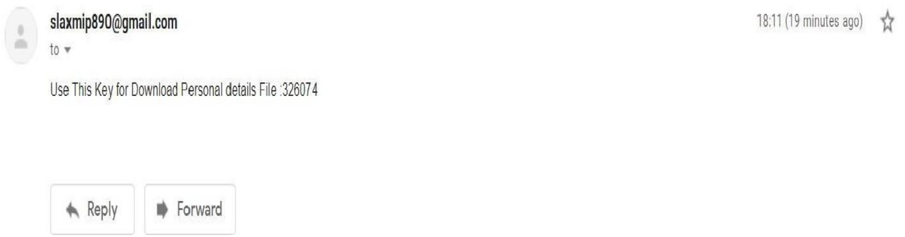
SECURE DATA TRANSFERRING ON CLOUD USING COMBINED FRAGMENTS AND CRYPTOGRAPHY MEDHODOLOGY

MyRequested File Details

File Id	File Name	Useranme	Datee	Owner Name	ServerStatus	Download
1	Personal details	gayathri	2021-02-06 18:09:04	laxmipriya	accept	Download

Fig 21 : File Download Page for User

DOI: 10.48175/IJARSCT-5861



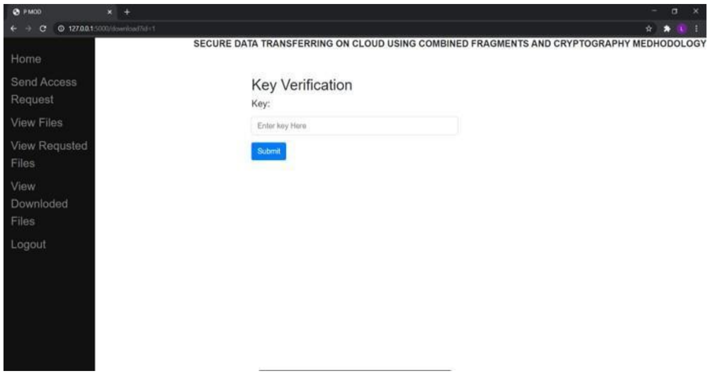
slaxmip890@gmail.com

to ▾

18:11 (19 minutes ago)

Use This Key for Download Personal details File :326074

Fig 22 : File Download Key Received by User.



SECURE DATA TRANSFERRING ON CLOUD USING COMBINED FRAGMENTS AND CRYPTOGRAPHY MEDHODOLOGY

Key Verification

Key:

Fig 23 : Key Verification Page for User.

VII. CONCLUSION

The various benefits gave by the cloud have driven numerous huge staggered associations to store and share their information on it. This project starts by calling attention to significant security concerns information proprietors have when sharing their information on the cloud. Next, the most generally executed and explored information sharing plans are briefly examined uncovering purposes of shortcoming in each. To address the worries, this paper proposes a Privilege-based Multilevel Organizational Data sharing plan that permits information to be shared efficiently and safely on the cloud. Parcels an information file into numerous sections dependent on client advantages and information affectability. Each section of the information file is then common relying upon information client advantages. We officially demonstrate that is secure against adaptively picked plaintext assault accepting that the DBDH presumption holds. The main aim of this system is to securely store and retrieve data on the cloud that is only controlled by the owner of the data. Cloud storage issues of data security are solved using cryptography and steganography techniques. Data security is achieved using BLOWFISH, 3DES and AES algorithm. Key information is safely stored using LSB technique (Steganography). Less time is used for the encryption and decryption process using multithreading technique. With the help of the proposed security mechanism, we have accomplished better data integrity, high security, low delay, authentication, and confidentiality.

REFERENCES

[1]. Uttam Kumar, Mr. Jay Prakash,"Secure File Storage On Cloud Using Hybrid Cryptography Algorithm", 2020 International Journal Of Creative Research Thoughts (IJCRT). ISSN:- 2320-2882 [Base Paper].

[2]. M. Malarvizhi, J. Angela Jennifa Sujana, T.Revathi, "Secure File Sharing Using Cryptographic Techniques In Cloud", 2014 International Conference On Green Computing Communication And Electrical Engineering (ICGCCEE).

[3]. Punam V. Maitri, Aruna Verma, "Secure File Storage In Cloud Computing Using Hybrid Cryptography Algorithm", IEEE Wispnet 2016.

[4]. Rashidhagat, Purvi Joshi, "Secure File Storage Using Hybrid Cryptography", International Journal Of Innovative Research In Technology(IJIRT) 2016.

[5]. Bilal Habib, Bertrand Cambou, Duane Booher, Christopher Philabaum, Public Key Exchange Scheme That Is Addressable (PKA), IEEE CNS 2017.

[6]. Tulip Dutta, Amarjyoti Pathak 2016 “Secure Data Sharing In Cloud Storage Using Key Aggregation Cryptography”.

[7]. Bhale Pradeep Kumar Gajendra, Vinay Kumar Singh, More Sujeet, “Achieving Cloud Security Using Third Party Auditor, MD5 And Identity Based Encryption”, ICCCA2016.

[8]. Shakeeba S. Khan, Prof.R.R. Tuteja, “Security In Cloud Computing Using Cryptographic Algorithms”, 2015

DOI: 10.48175/IJARSCT-5861