

DAYANANDA SAGAR UNIVERSITY

KUDLU GATE, BANGALORE – 560068



**Bachelor of Technology
in
COMPUTER SCIENCE AND ENGINEERING**

Major Project Phase-II Report

SECURE FILE STORAGE ON CLOUD USING CRYPTOGRAPHY

By

Faisal S	ENG18CS0099
Pavan B	ENG18CS0206
Shailendra B	ENG18CS0252
Shree Vallabha S	ENG18CS0270

**Under the supervision of
Prof. Nandini.K
Assistant Professor, Department of Computer Science**

**DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING,
SCHOOL OF ENGINEERING
DAYANANDA SAGAR UNIVERSITY,
BANGALORE**

(2021-2022)



DAYANANDA SAGAR UNIVERSITY

**School of Engineering
Department of Computer Science & Engineering**

Kudlu Gate, Bangalore – 560068
Karnataka, India

CERTIFICATE

This is to certify that the Phase-II project work titled “**SECURE FILE STORAGE ON CLOUD USING CRYPTOGRAPHY**” is carried out by **Faisal S(ENG18CS0099), Pavan B(ENG18CS0206), Shailendra B(ENG18CS0252), Shree Vallabha S(ENG18CS0270)**, bonafide students of Bachelor of Technology in Computer Science and Engineering at the School of Engineering, Dayananda Sagar University, Bangalore in partial fulfilment for the award of degree in Bachelor of Technology in Computer Science and Engineering, during the year **2021-2022**.

Prof.Nandini K

Assistant Professor
Dept. of CS&E,
School of Engineering
Dayananda Sagar University

Date:

Dr. Girisha G S

Associate Professor
Chairman CSE
School of Engineering
Dayananda Sagar University

Date:

Dr. A Srinivas

Dean
School of Engineering
Dayananda Sagar
University

Date:

Name of the Examiner

Signature of Examiner

1.

2.

DECLARATION

We, **Faisal S (ENG18CS0099), Pavan B(ENG18CS0206), Shailendra B (ENG18CS0252), Shree Vallabha S (ENG18CS0270)**, are students of the Eighth Semester B.Tech in **Computer Science and Engineering**, at School of Engineering, **Dayananda Sagar University**, hereby declare that the phase-II project titled “**SECURE FILE STORAGE ON CLOUD USING CRYPTOGRAPHY**” has been carried out by us and submitted in partial fulfilment for the award of degree in **Bachelor of Technology in Computer Science and Engineering** during the academic year **2021-2022**.

Student

Signature

Faisal S:

ENG18CS0099 :

Pavan B:

ENG18CS0206 :

Shailendra B:

ENG18CS0252 :

Shree Vallabha S:

ENG18CS0270:

Place: Bangalore

Date :

ACKNOWLEDGEMENT

It is a great pleasure for us to acknowledge the assistance and support of many individuals who have been responsible for the successful completion of this project work.

First, we take this opportunity to express our sincere gratitude to School of Engineering & Technology, Dayananda Sagar University for providing us with a great opportunity to pursue our Bachelor's degree in this institution.

*We would like to thank **Dr. A Srinivas. Dean, School of Engineering & Technology, Dayananda Sagar University** for his constant encouragement and expert advice.*

*It is a matter of immense pleasure to express our sincere thanks to **Dr. Girisha GS , Chairman, Department of Computer Science and Engineering, Dayananda Sagar University**, for providing right academic guidance that made our task possible.*

*We would like to thank our guide **Prof.Nandini K** , Assistant Professor, Dept. of Computer Science and Engineering, Dayananda Sagar University, for sparing his/her valuable time to extend help in every step of our project work, which paved the way for smooth progress and fruitful culmination of the project.*

*We would like to thank our **Project Coordinators Dr. Meenakshi Malhotra and Dr. Bharanidharan N**, and all the staff members of Computer Science and Engineering for their support.*

We are also grateful to our family and friends who provided us with every requirement throughout the course.

We would like to thank one and all who directly or indirectly helped us in the Project work.

Signature of Students

USN: ENG18CS0099, ENG18CS0206, ENG18CS0252, ENG18CS0270

NAME: Faisal S, Pavan B, Shailendra B, Shree Vallabha S

TABLE OF CONTENTS

	Page
LIST OF ABBREVIATIONS	vi
LIST OF FIGURES	vii
ABSTRACT	viii
CHAPTER 1 INTRODUCTION.....	02
1.1 BACKGROUND KNOWLEDGE	02
1.2. EXISTING SYSTEM	02
CHAPTER 2 PROBLEM DEFINITION	03
CHAPTER 3 LITERATURE SURVEY.....	06
CHAPTER 4 PROJECT DESCRIPTION.....	09
4.1. PROPOSED DESIGN	09
4.2. UML DESIGN	10
4.3.USE CASE DIAGRAMS.....	14
CHAPTER 5 REQUIREMENTS	16
5.1. FUNCTIONAL REQUIREMENTS	17
5.2. HARDWARE REQUIREMENTS.	18
CHAPTER 6 METHODOLOGY.....	20
CHAPTER 7 TEST CASES	21
CHAPTER 8 RESULTS	24
CHAPTER 9 CONCLUSION	32
REFERENCES	33
APPENDIX A	34
Funding and Published Paper details	35

LIST OF ABBREVIATIONS

ACRONYM	ACRONYM EXPANSION
DO	Data Owner
DU	Data User
AES	Advanced Encryption Standard
DES	Data Encryption Standard
MySQL	My Structured Query Language

LIST OF FIGURES

Fig. No	Description of the figure	Page No.
4.1.1	Project Design	09
4.2.1	Data flow diagram	11
4.3.1	Data owner Use case diagram	12
4.3.2	Data User Use case diagram	12
4.3.3	Admin use case diagram	13
4.3.4	Cloud use case diagram	13
4.4.1	Activity diagram	14
7.7.1	Screen-Design	23
7.7.2	Admin Page	23
7.7.3	Owner Page	24
7.7.4	User Page	24
7.7.5	Cloud Page	25
7.7.6	Owner Registration Form	25
7.7.7	User Registration Form	26
7.7.8	Admin Verifying User	26
7.7.9	Owner Uploading File	27
7.8.0	File Upload Fragments	27
7.8.1	User Key Request Activation	28
7.8.2	User Key Verification Page to Download	28
7.8.3	User Requested File	29

ABSTRACT

In this project, we expect to safely store data in the cloud, by parting information into a few pieces and putting away pieces of it in the cloud in a way that jelly information privacy, respectability, and guarantees accessibility. They quickly expanded the utilization of distributed computing in numerous association and IT businesses furnishing new programming with minimal effort. Distributed computing gives part of advantages with ease and information openness through the Internet. Guaranteeing the security of distributed computing is a central point in the distributed computing climate, as clients regularly store delicate data with distributed storage suppliers, however, these suppliers might be untrusted. So securely sharing information while safeguarding information from an untrusted cloud is as yet a difficult issue. Our methodology guarantees the security and protection of customer touchy data by putting away information across a single cloud, utilizing AES, DES, and Blowfish calculation.

CHAPTER 1

INTRODUCTION

CHAPTER 1 INTRODUCTION

The project aims to create an encrypted and secured file storage system to transfer files among users in a remote location. This system will require an input that is successfully encrypted using any of the algorithm techniques and stored anywhere. The uploaded file can be downloaded by other users, but to read the data present in it, they have to decrypt the file using the decryption algorithm and the information provided about the file within the users by the owner.

1.1 BACKGROUND KNOWLEDGE

The system uses public-key cryptographic techniques like RSA and Symmetric key cryptography like AES. Hashing techniques like static hashing and dynamic hashing are used for performing integrity. Due to the encryption of data, confidentiality is also achieved in the process. The project is also open to new challenges and future changes to other advanced technologies in keeping the data secured.

1.2 EXISTING SYSTEM

The main purpose of cryptography is to maintain the security of the data from a third party. There are following two types of algorithms such as (i) symmetric key-based algorithm, sometimes known as a conventional key algorithm, and (ii) asymmetric key-based algorithm, also known as a public-key algorithm. The symmetric algorithm can be further divided into two types. In the cloud computing environment, security is deemed to be a crucial aspect due to the significance of information stored in the cloud

CHAPTER 2

PROBLEM DEFINITION

CHAPTER 2 PROBLEM DEFINITION

First is the single point of failure, which will affect the data available that could occur if a server at the cloud service provider failed or crashed, which makes it harder for the customer to retrieve his stored data from the server. Availability of data is also an important issue that could be affected if the cloud service provider (CSP) runs out of service. Our second threat is data integrity. Integrity is the degree of confidence that the data in the cloud is what is supposed to be there, and is protected against accidental or intentional alteration without authorization. Such worries are no more beneficial issues; therefore, a cloud service customer can not entirely rely upon a cloud service provider to ensure the storage of his vital data. Security is a necessary service for wired networks as well as wireless network communication to improve what was offered in the cloud. Simply storing the information in clouds solves the problem is not data availability, but security. The strong point of this method is that the secret key has to be combined by reconstructing.

CHAPTER 3

LITERATURE SURVEY

CHAPTER 3 LITERATURE SURVEY

The author talks about the Method to provide high data security while using cloud storage services by using the Double Encryption Technique to increase the security of the file using HTML as the Front End and Python as Back End to store the file they use the cloud[1].

Crypto-steganography, one can achieve two levels of security. There will be no third-party interruption by using this technique because no one can even know that data is embedded into the image as there will be noise created in the cover image. By using AES and LSB algorithms this technique was implemented. [2]

Using cryptography, encryption, merging, unscrambling, and recovery cycle to make sure about the enormous information put away in the multi-cloud. With the help of AES, the Feistel algorithm achieved high performance compared to other algorithms.[3]

SeGshare-an end to end encrypted, group file sharing solution supporting large and dynamic groups using trusted execution environments(TEE) and sending data in a group or duplication of file.[4]

The proposed framework gives a secure sharing of information by utilizing RSA and AES calculations to preserve security inside the cloud server and could calculate the preserved file size inside the cloud server.[5]

The proposed scheme is proved selective-structure chosen plaintext secure and master key secure without random oracles. Besides, we develop another kind of key delegating capability in our scheme and also discuss some related issues including a stronger security model and applications.[6]

In this paper, we propose data access control for multiauthority cloud storage (DAC-MACS), an effective and secure data access control scheme with efficient decryption and revocation. Specifically, we construct a new multiauthority CP-ABE scheme with efficient decryption, and also design an efficient attribute revocation method that can achieve both forward security and backward security. We further propose an extensive data access control scheme (EDAC-MACS), which is secure under weaker security assumptions.[7]

Table 3.1: State of the Art-work

Paper Title	Conference Name and year	Technology used	Results	What we Infer
1. Efficient and Secure File Transfer in Cloud Through Double Encryption Using AES and RSA Algorithm. (K.Jaspin)	(2021) International Conference on Emerging Smart Computing and Informatics (ESCI) AISSMS Institute of Information Technology, Pune, India. Mar 5-7, 2021	ALGORITHM-AES, DES, BLOWFISH FRONT-END(HTML) BACK-END(PYTHON) CLOUD	Method to provide high data security while using Cloud storage services. We make use of the Double Encryption Technique to increase the security of the file.	We could understand using a Double-encryption algorithm how we can increase the security of the file through the cloud.
2. Secure Data Transfer Through Internet Using Cryptography and Image Steganography. (Krishna Chaitanya Nunna)	(2020). Secure Data Transfer Through Internet Using Cryptography and Image Steganography. 2020 SoutheastCon. doi:10.1109/southeastcon44009.2020	ALGORITHM-AES, LSB FRONT-END-HTML BACK-END-JAVASCRIPT	Crypto-steganography, one can achieve two levels of security. There will be no third-party interruption by using this technique because no one can even know that data is embedded into the image as there will be no noise created in the cover image.	We could understand using this Technique where we encrypt the data using the key and using that key, we are embedding the data in the pixels of the cover image pseudo-randomly.
3. Secure Data Storage in Cloud using Encryption Algorithm. (S.S.Tyagi)	Proceedings of the Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV 2021). IEEE Xplore Part Number: CFP21ONG-ART; 978-0-7381-1183-4	ALGORITHM-AES,FEISTEL FRONT-END-HTML BACK-END-PYTHON	Using Cryptography, encryption, merging, unscrambling, and recovery cycle to make sure about the enormous information put away in the multi-cloud. With the help of AES, the Feistel algorithm achieved high performance compared to other algorithms.	We could understand that using AES and Feistel algorithm achieved high performance to other algorithms.
4. SeGShare: Secure Group File Sharing in the Cloud using Enclaves. (Lina Hirschhoff)	Proceedings of the Fifth International Conference on Computing Methodologies and Communication (ICCMC 2021) IEEE Xplore Part Number: CFP21K25-ART	ALGORITHM-AES, RC6, DES FRONT-END-HTML BACK-END-JAVASCRIPT	SeGShare — an end-to-end encrypted, group file sharing solution supporting large and dynamic groups using trusted execution environments (TEE).	We could understand Encrypted data using trusted execution environments we send data in a group or duplication of file.
5. Securing of Cloud Data with Duplex Data Encryption Algorithm (Dr. S.Nikkath Bushra)	Proceedings of the Fifth International Conference on Computing Methodologies and Communication (ICCMC 2021) IEEE Xplore Part Number: CFP21K25-ART	ALGORITHM-AES, RSA, DES FRONT-END-HTML BACK-END-JAVASCRIPT	The proposed framework gives a secure sharing of information by utilizing RSA and AES calculations to preserve security inside the cloud server.	Using RSA and AES we could calculate and preserve file size inside the cloud server.

CHAPTER 4

PROJECT DESCRIPTION

CHAPTER 4 PROJECT DESCRIPTION

4.1. PROPOSED DESIGN

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 algorithms.

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 stored safely on the cloud.

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, and the phone number will be requested to enter.
- Using this data the server will produce unique user-specific keys that will be used for encryption and decryption purposes.
- But this key will not be stored in the database instead it will be stored using the steganography algorithm in an image that will be used as the user's profile picture.

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 a file will be encrypted using cryptographic algorithms. Every part will use a different encryption algorithm.
- These all parts of the file will be encrypted using different algorithms which are AES, 3DES, and Blowfish. The key to these algorithms will be retrieved from the steganographic image created during the registration.

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 the file will be decrypted using the same algorithms with which they were encrypted. The key to the algorithms for the decryption process will be retrieved from the steganographic image created during the registration.
- Then these parts will be re-combined to form a fully decrypted file.
- Then the file will be sent to the user for download.

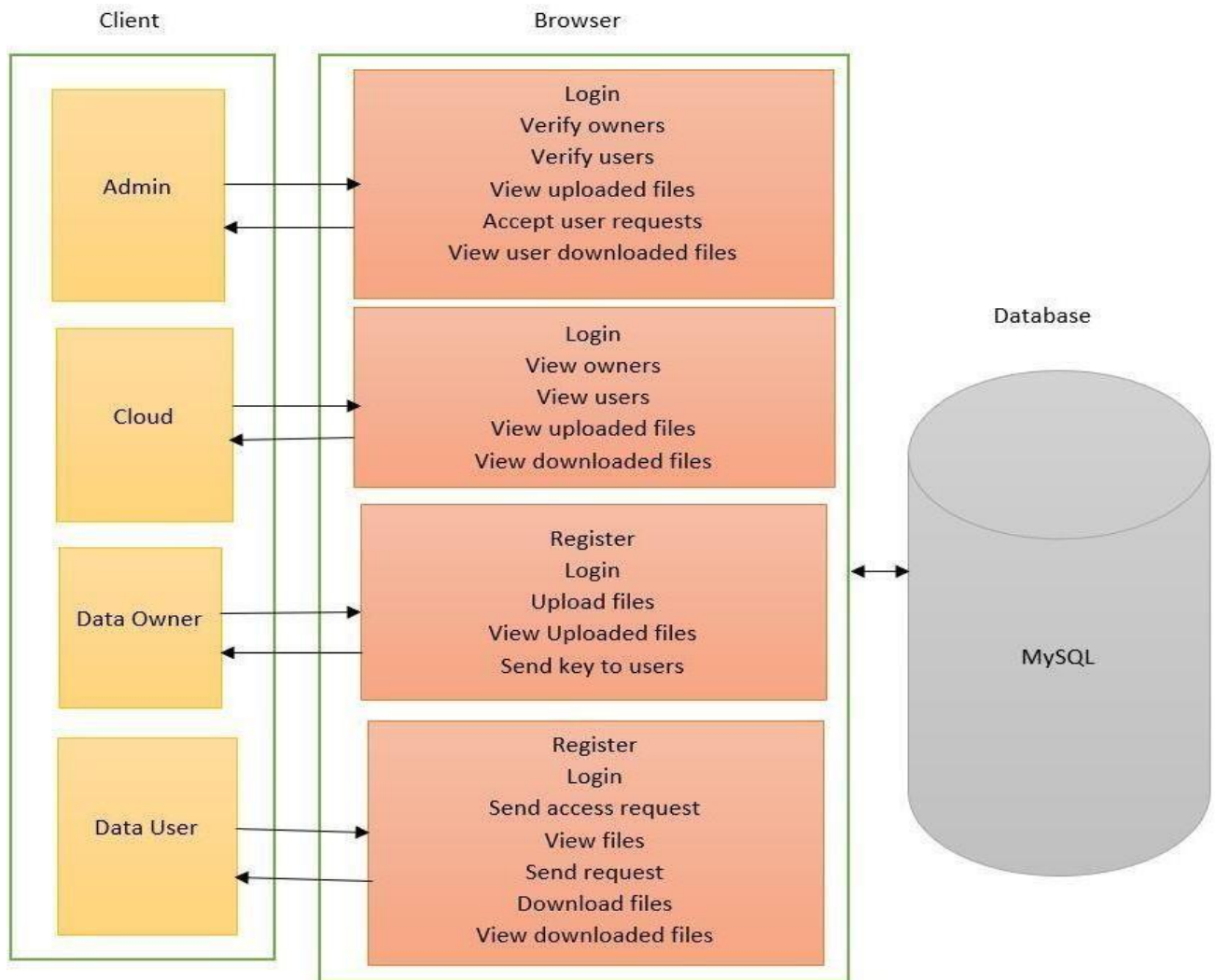


FIG 4.1.1 PROJECT DESIGN

4.2 UML DIAGRAMS

4.2.1 DATA FLOW DIAGRAM

- The DFD is also called a 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 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. It 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 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
- DFD is also known as a bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail. DFD consists of processes, flows, warehouses, and terminators.
- Process is part of the system that transforms inputs into outputs. The symbol is a circle, an oval, and a rectangle with rounded corners. The process name is named in one word or a short sentence.

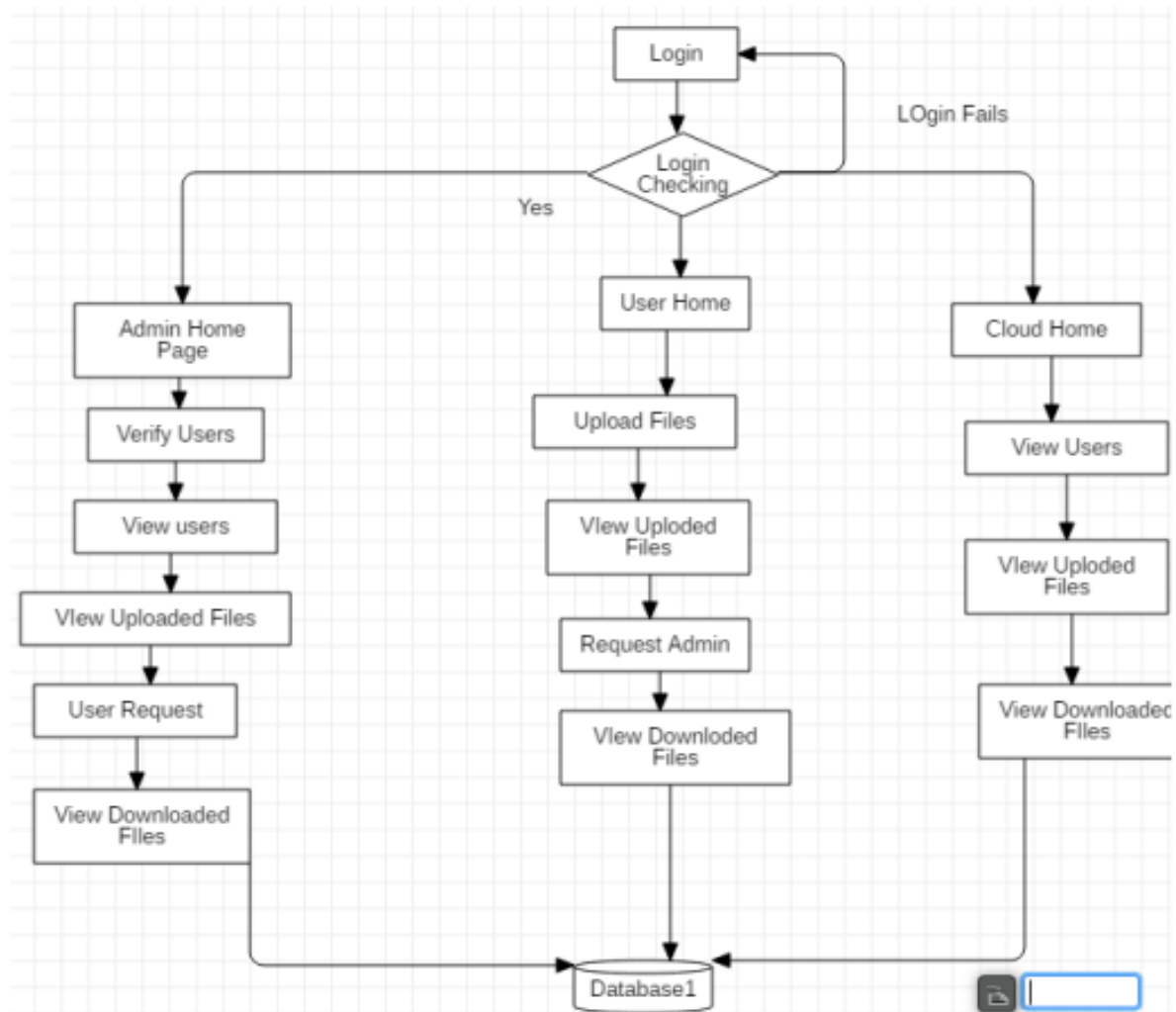


Fig 4.2.1: Data flow diagram

4.3 USE CASE DIAGRAMS

A use case diagram in the Unified Modeling Language (UML) is a type of behavioural diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. The roles of the actors in the system can be depicted.

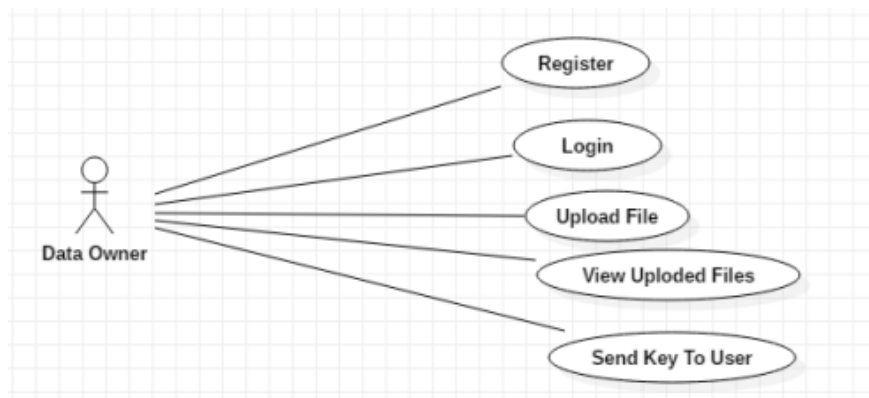


Fig 4.3.1: Data owner Use case diagram

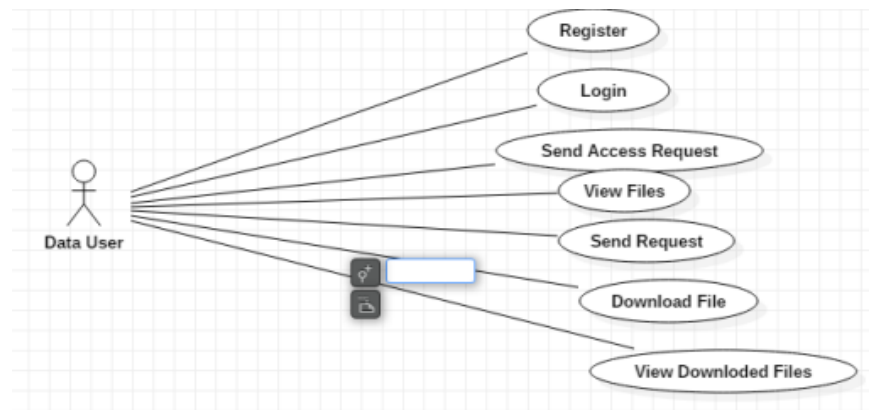


Fig 4.3.2: Data User Use case diagram

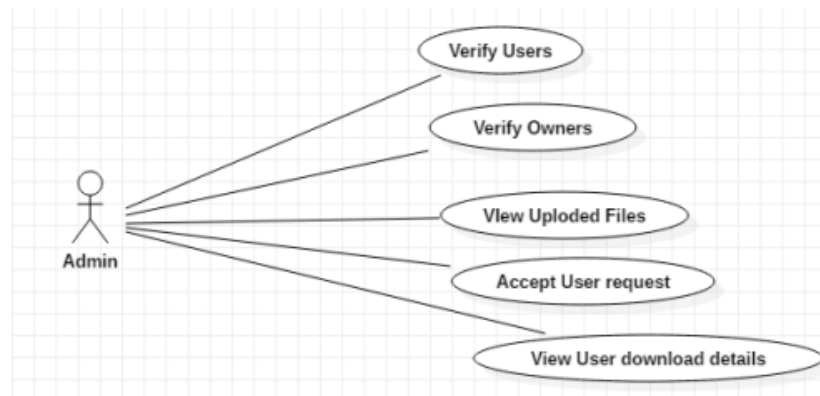


Fig 4.3.3: Admin use case diagram

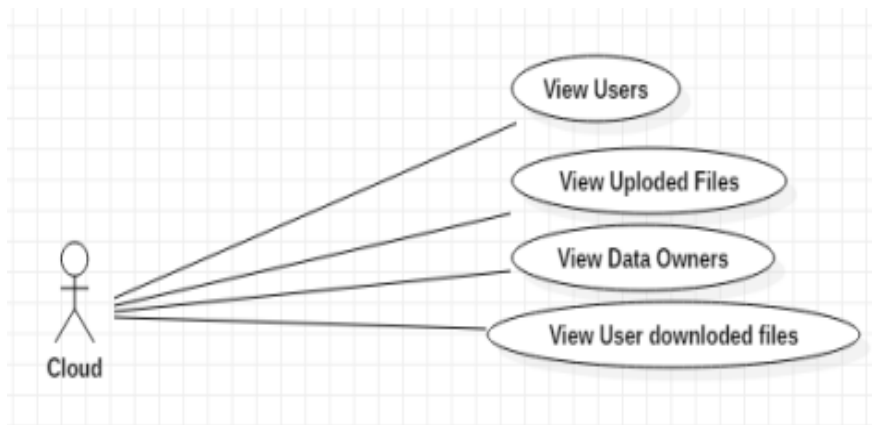


Fig 4.3.4: Cloud use case diagram

4.4. 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 of control.

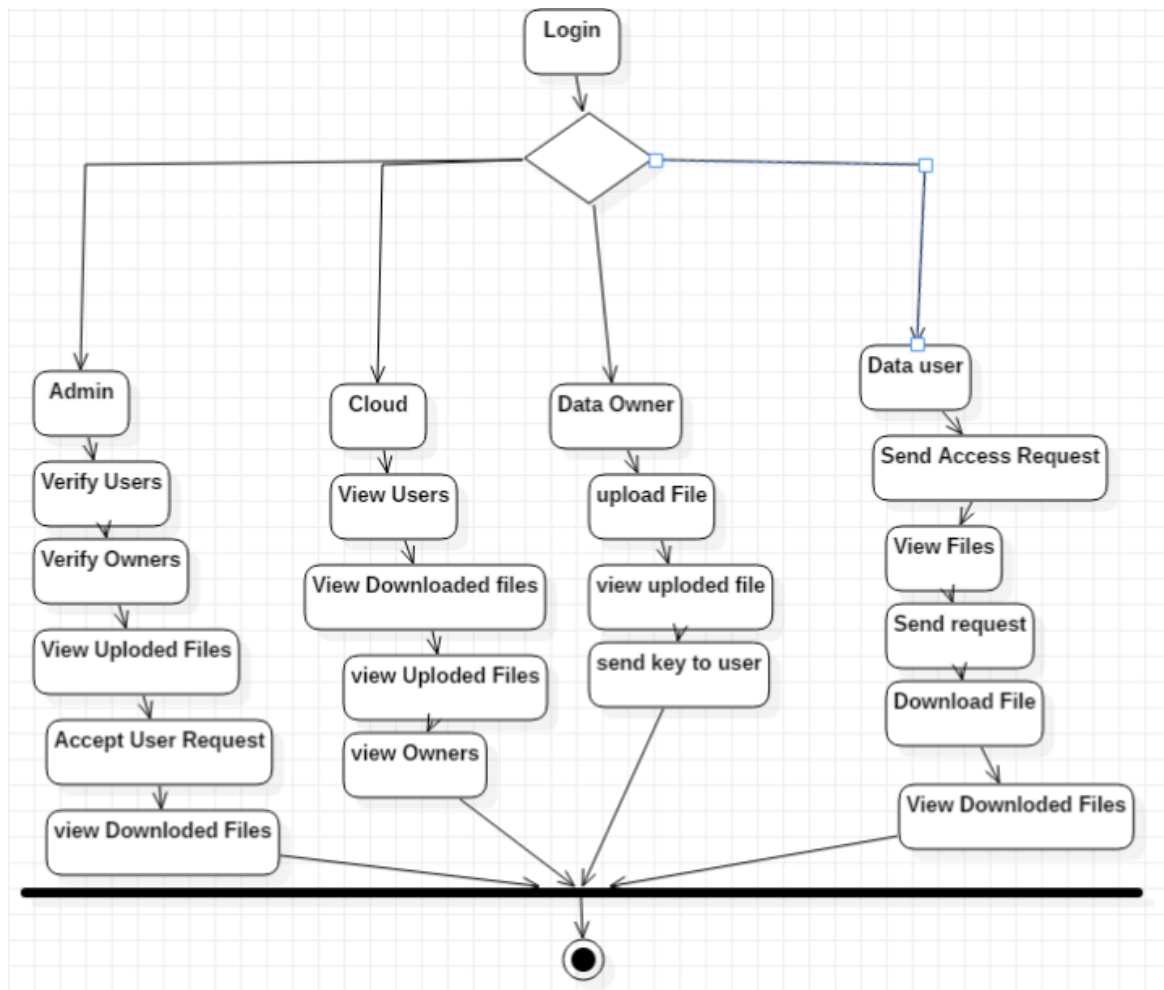


Fig 4.4.1: Activity diagram

CHAPTER 5

REQUIREMENTS

CHAPTER 5 REQUIREMENTS

5.1FUNCTIONAL REQUIREMENTS

5.1.1 DATA OWNER (DO)

The owner uploads the data to a cloud server. The file is split into an octet. Every part of the file is encoded simultaneously using the multithreading technique. The encoded file is stored on a cloud server. Keys used for encryption are stored in the cover image. Cloud computing is a multi-user environment.

5.1.2 DATA USER (DU)

Cloud user request for file. On request of file user also gets key using email which consists of key information. The reverse process is used to decode the file.

5.1.3 CLOUD

The Cloud module can operate by the admin in the cloud module having all the registered users, owner details and owner uploaded file details and user-uploaded file details.

5.1.4 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 log in to home page after entered into the home page admin act like the owner of this application and admin activate and deactivate the user and owner of this application and admin activate and deactivate the user, owner and admin can view all uploaded file details and request details

5.2 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 a computer constitute hardware.

- System: INTEL I31, I5, I7.
- Hard Disk: 30 GB.
- Ram: 512 Mb.
- Monitor: 15 VGA Colour.

5.3 SOFTWARE REQUIREMENTS

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

- Operating System: - Windows 7/Windows 10.
- Coding Language: Python
- Databases: MYSQL
- Server: Flask
- Cloud: Firebase

CHAPTER 6

METHODOLOGY

CHAPTER 6 METHODOLOGY

In this framework, AES, 3DES, and Blowfish calculations are utilized to dam savvy security info. The planned framework is the hybridizing of AES, 3DES, and Blowfish. All calculations are symmetric-key cryptography. These calculations utilize a solitary key for document secret writing and disentangling reason. All calculation's key size is 128 digits. to hide key information in the cover image utilizing the LSB technique. Usage of the planned framework is finished utilizing java language. Document secret writing and disentangling time are determined with the help of java programming. Record write and decipher time is determined for just content document with an examination of existing AES and Blowfish calculations. Document size is given in MB for AES calculation.

CHAPTER 7

TESTING CASES

CHAPTER 7 TESTING CASES

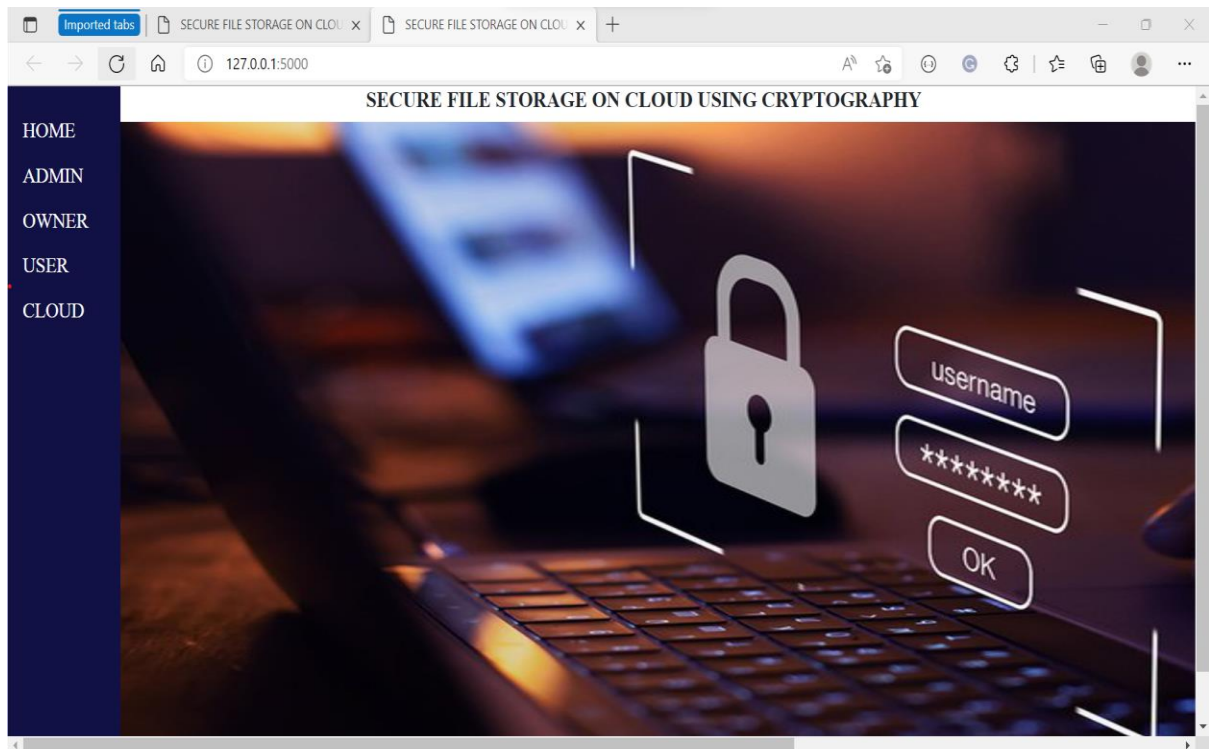
S.NO	TEST CASE DESCRIPTION	ACTUAL VALUE	EXPECTED VALUE	FAILED VALUE	RESULT
1.	Admin Login	Admin will Provide Login Credentials	Admin Home Page will Open	Invalid Login Details	Success
2.	Cloud Login	Cloud Person will Provide Credentials	Cloud Home Page will Open	Invalid Login Details	Success
3.	Owner Login	Owner will Provide Owner Credentials	Owner Home Page will Open	Invalid Owner Login Details	Success
4.	User Login	User will Provide Credentials	User Page will Open	Invalid Login Details	Success
5.	Owner Register	Owner will give Owner Details	Owner Registration Successful	Duplicate Owner Details	Success
6.	User Register	User will Give User Details	User Registration Successful	Duplicate User Details	Success

CHAPTER 8

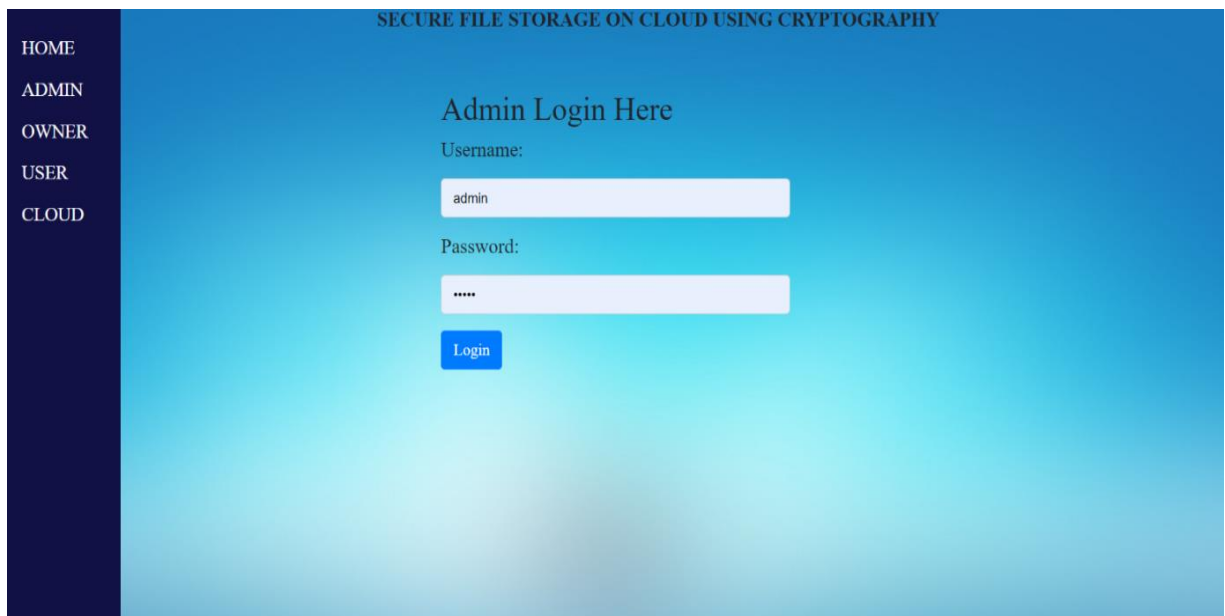
RESULTS

CHAPTER 8 RESULTS

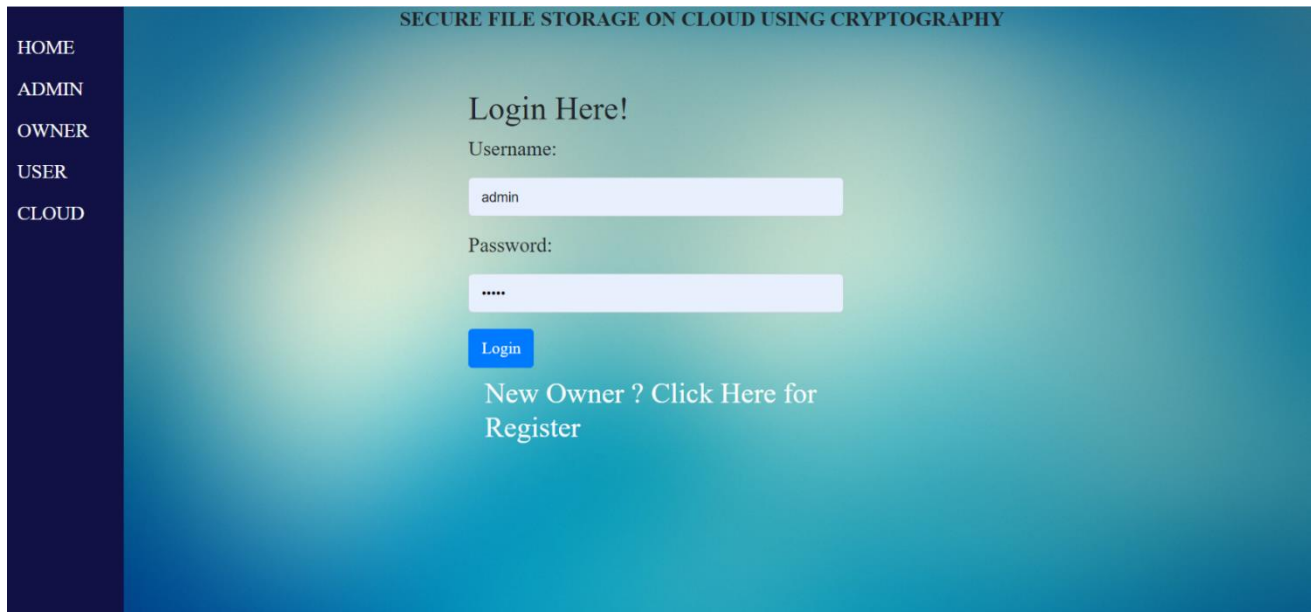
7.7.1 DESIGN- SCREEN DESIGN



7.7.2 ADMIN PAGE

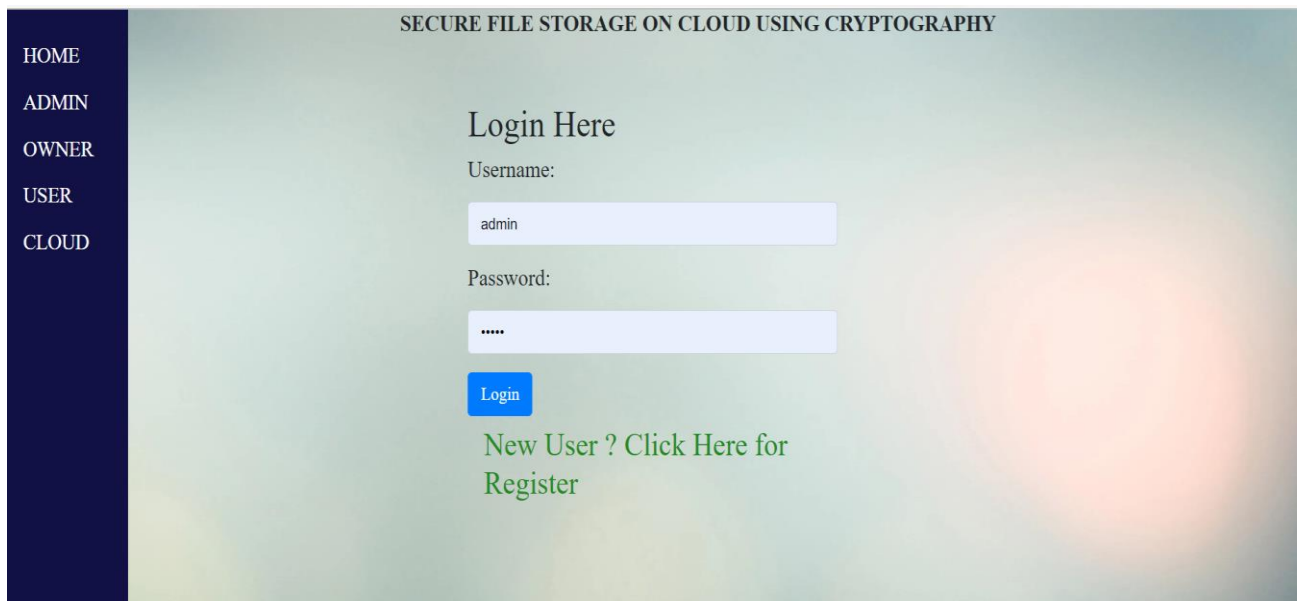


7.7.3 OWNER PAGE



The screenshot shows the 'OWNER PAGE' for the application. On the left is a dark blue sidebar with white text links: HOME, ADMIN, OWNER, USER, and CLOUD. The main content area has a blue gradient background. At the top, it says 'SECURE FILE STORAGE ON CLOUD USING CRYPTOGRAPHY'. Below this is the heading 'Login Here!'. There are two input fields: 'Username:' with the value 'admin' and 'Password:' with masked characters '*****'. A blue 'Login' button is positioned below the password field. At the bottom, there is a link that says 'New Owner ? Click Here for Register'.

7.7.4 USER PAGE



The screenshot shows the 'USER PAGE' for the application. It has the same dark blue sidebar with links: HOME, ADMIN, OWNER, USER, and CLOUD. The main content area has a light green gradient background. At the top, it says 'SECURE FILE STORAGE ON CLOUD USING CRYPTOGRAPHY'. Below this is the heading 'Login Here'. There are two input fields: 'Username:' with the value 'admin' and 'Password:' with masked characters '*****'. A blue 'Login' button is positioned below the password field. At the bottom, there is a link that says 'New User ? Click Here for Register' in green text.

7.7.5 CLOUD PAGE

SECURE FILE STORAGE ON CLOUD USING CRYPTOGRAPHY

Cloud Server Login Here

Username:

admin

Password:

.....

Login

7.7.6 OWNER REGISTRATION FORM

Owner Register Here!

Name:

ADMIN

Username:

admin

Password:

.....

Email:

faisalssheriff@gmail.com

Phone:

9742759134

Image:

Choose File TEST.jpeg

Register Clear

Registration STATUS X

Registration success

OK

7.7.7 USER REGISTRATION FORM

HOME
ADMIN
OWNER
USER
CLOUD

User Register Here

Name:

Username:

Password:

Email:

Phone:

Image:

wallpaperflare.com - wallpaper (1).jpg

Registration Status

Registration success

OK

7.7.8 ADMIN VERIFYING USER

SECURE FILE STORAGE ON CLOUD USING CRYPTOGRAPHY							
View User Details							
Image	User Id	Name	User name	Email	Phone	Status	Action
	3	Faisal S	admin123	faisalssheriff@gmail.com	9901898283	unauthorized	<button>Activate</button>

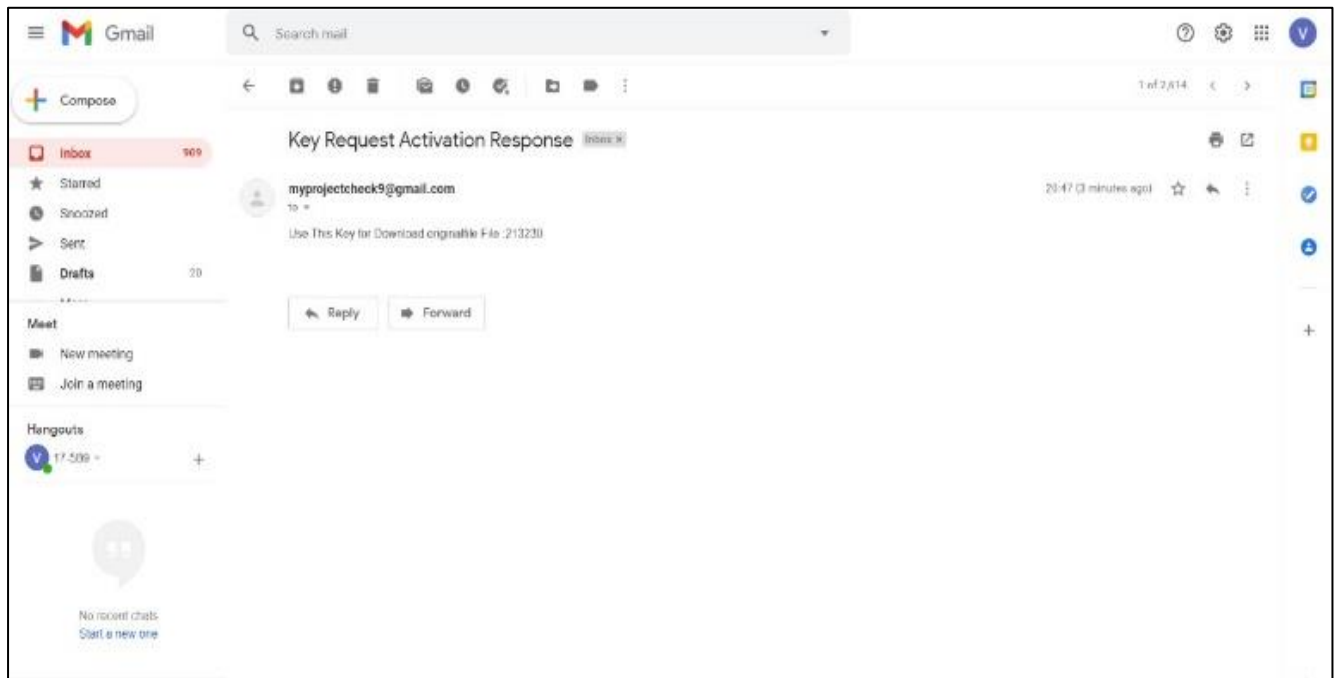
7.7.9 OWNER UPLOADING FILE

The screenshot shows the 'Upload File Here' page of the 'SECURE FILE STORAGE ON CLOUD USING CRYPTOGRAPHY' application. On the left is a dark blue sidebar with navigation links: Home, Upload File, View Uploaded Files, View Requested Keys, View Downloaded Files, and Logout. The main content area has a light blue header with the application name. Below the header, the title 'Upload File Here' is centered. The form includes three input fields: 'FileName:' with the text 'PERSONAL DETAILS', 'Description:' with the text 'PERSONAL DETAILS', and 'File:' with a 'Choose File' button and the text 'PERSONAL DETAILS (1).txt'. A blue 'Upload' button is at the bottom of the form.

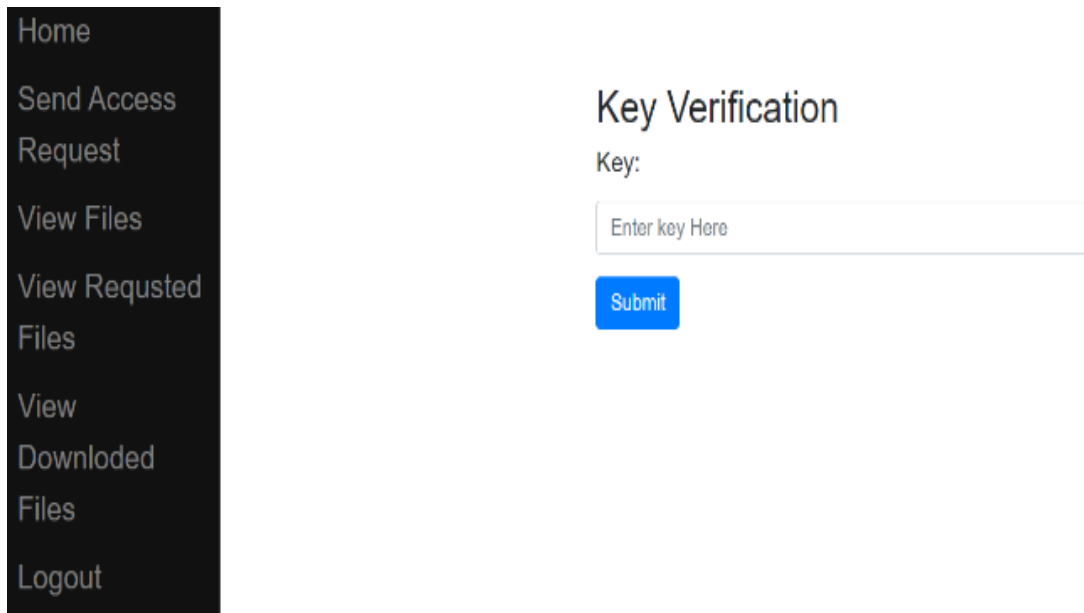
7.8.0 FILE UPLOADED IN FRAGMENTS

The screenshot shows the file upload progress interface. The sidebar is the same as in the previous screenshot. The main content area has a light blue header with the application name. Below the header, there is a table with five rows, each representing a file fragment. The first column of the table lists the fragments: 'FrageMent1', 'FrageMent2', 'FrageMent3', 'FrageMent4', and 'FrageMent5'. The second column shows the progress of each fragment, represented by a small bar and a percentage: 'b5f2', '7f99', '6d17', '873d', and '5689'. To the right of the table is a green 'Upload' button. A small dialog box titled 'File STATUS' is open, showing 'File Uploaded Success' and an 'OK' button.

7.8.1 USER KEY REQUEST ACTIVATION



7.8.2 USER KEY VERIFICATION PAGE TO DOWNLOAD



7.8.3 USER-REQUESTED FILE

- Home
- Send Access Request
- View Files
- View Requested Files
- View Downloaded Files
- Logout

MyRequested File Details

File Id	File Name	Useraname	Datee	Owner Name	ServerStatus	Download
10	originalfile	vyshnavi	2021-05-27 20:45:32	niharika	accept	Download

CHAPTER 9

CONCLUSION

CHAPTER 9 CONCLUSION

Here, we tend to propose a way to supply high information security whereas using Cloud storage services. We build use of the Double cryptography Technique to extend the protection of the file. From the results obtained, our technique provides high security with resistance against propagation errors. The runtime of our algorithmic rule is less compared to the present algorithms, thus it's quick. Therefore, we tend to propose a secure and price-effective information protection technique for cloud service end-users. Our system efficiency in terms of runtime with secure protection of text information over the cloud compared with existing cryptography and decryption methodologies like AES, Blowfish, 3-DES.

REFERENCES

- [1]Fuhry, B., Hirschhoff, L., Koesnadi, S., & Kerschbaum, F. (2020). SeGShare: Secure Group File Sharing in the Cloud using Enclaves. 2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). doi:10.1109/dsn48063.2020.00061
- [2] Inder Singh, M. Prateek,” “Data Encryption and Decryption Algorithms using Key Rotations N. Sharma, A. Hasan, “A New Method Towards Encryption Schemes, IEEE, International Conference on Reliability, Optimization and Information Technology, pages 310-313, Feb 2019.
- [3] Jasleen K., S.Garg, “Security in Cloud Computing using Hybrid of Algorithms”, IJERJS, Volume 3, Issue 5, ISSN 2091-2730, pages 300-305, September-October, 2015
- [4] Jaspin, K., Selvan, S., Sahana, S., & Thanmai, G. (2021). Efficient and Secure File Transfer in Cloud Through Double Encryption Using AES and RSA Algorithm. 2021 International Conference on Emerging Smart Computing and Informatics (ESCI). doi:10.1109/esci50559.2021.9397005
- [5] Pronika, & Tyagi, S. S. (2021). Secure Data Storage in Cloud using Encryption Algorithm. 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV). doi:10.1109/icicv50876.2021.9388388
- [6] Subasini, C. A., & Nikkath Bushra, S. (2021). Securing of Cloud Data with Duplex Data Encryption Algorithm. 2021 5th International Conference on Computing Methodologies and Communication.(ICCMC). doi:10.1109/iccmc51019.2021.9418
- [7] Kumar, S., Karnani, G., Gaur, M. S., & Mishra, A. (2021). Cloud Security using Hybrid Cryptography Algorithms. 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM). doi:10.1109/iciem51511.2021.94453
- [8] Kodumru, N. L., & Supriya, M. (2018). Secure Data Storage in Cloud Using Cryptographic Algorithms. 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA). doi:10.1109/iccubea.2018.8697550

APPENDIX A

APPENDIX A PUBLISHED PAPER DETAILS

International Journal for Research in Applied Science and Engineering Technology (IJRASET) is a UGC recognized, international peer-reviewed, open-access, multidisciplinary online journal with high impact factor published for the enhancement of research in various disciplines of Applied Science & Engineering Technologies.

Paper Submission Details:

- Paper Title: Secure file storage on cloud using cryptography
- Paper ID: IJRASET43535
- Authors: Faisal S, Shailendra B, Shree Vallabha S, Pavan B , Nandini K
- Publish Date:11-06-2022
- ISSN: 2321-9653
- Publisher Name: IJRASET, Volume 10 Issue VI June 2022
- DOI Link: <https://doi.org/10.22214/ijraset.2022.43535>



iJRASET

International Journal For Research in
Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 Issue: VI Month of publication: June 2022

DOI: <https://doi.org/10.22214/ijraset.2022.43535>

www.ijraset.com

Call:  08813907089

E-mail ID: ijraset@gmail.com

Secure File Storage on Cloud Using Cryptography

Nandini K¹, Faisal. S², Shailendra B³, Shree Vallabha S⁴, Pavan B⁵

^{1, 2, 3, 4, 5}Department of Computer Science, Dayananda Sagar University, Bangalore, Karnataka

Abstract: Hacking became a serious drawback lately. Transference of secure knowledge or communication through the web turns out to be difficult because of security considerations. To anticipate these security hurdles, we tend to use Cryptography, and Image Steganography. Day's cloud computing is currently employed in several areas like business, colleges, and Universities to store a great amount of knowledge. We will extract knowledge from the cloud for the asking of users. To store knowledge on the cloud we've to face several errors and issues. Cryptography and steganography techniques are well-liked currently a day's for knowledge security. Using one algorithmic rule isn't effective for prime-level security to knowledge in cloud computing. During this paper, we initiated a new security mechanism using symmetrical key cryptography algorithmic rules and steganography. During this projected system AES, Blowfish, RC6, and 3DES algorithms are used to supply block-wise security to knowledge. All algorithms have a key size of 128 bits. Key data contains that a part of the file is encrypted using that algorithmic rule and key. The file is split into eight components. Every part of the file is encrypted using different algorithmic rules. All components of the file are encrypted at the same time with the assistance of the multithreading technique. Encoding keys are inserted into a cover image using LSB technique. Steganography image is sent to a valid receiver using email. For file secret writing purposes reverse method of cryptography is applied.

Keywords-Hacking, Steganography, Cryptography, Cloud service provider (CSP), cloud server (CS), Encode, Decode, Delay, Integrity

I. INTRODUCTION

Internet isn't any longer safe to transfer sensitive info. The dependence of the individuals created the hackers to observe the network and attack for sensitive info. The info is firmly saved in our system and won't be safe after we transfer it over the web. Also, the system itself may be established with viruses, trojans, and malware in the same ways that. This results in intrusion into the system and once more loss of data. Therefore, security is the most important factor for individuals since the evolution of hacking. Cryptography is the technique of embedding information into an object wherever human sense cannot sense it. This means the communication is accomplished in such a way that the message's existence cannot be known. The word Cryptography in Greek may be shown as 'Krypto' suggests that it is hidden and 'graphene' suggests that writing. Security and protection keep a crucial obstruction on Distributed computing as an example safeguarding classification, uprightness, and accessibility of information. This methodology guarantees that the information is most certainly not noticeable to outer clients and cloud executives, however, has the impediment that plain content-based principally looking calculation does not appear to be relevant.

A. Cloud Computing

Cloud computing is the utilization of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). Cloud computing entrusts remote services with a user's information, code, and computation. Cloud computing consists of hardware and code resources created and accessible online as managed third-party services. These services generally offer access to advanced code applications and high-end networks of server computers.



The goal of cloud computing is to apply traditional supercomputing, or superior computing power, ordinarily utilized by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications like financial portfolios, to deliver customized info, to produce information storage or to power giant, immersive laptop games. Cloud computing uses networks of huge teams of servers usually running low-priced shopper computer technology with specialized connections to unfold data-processing chores across them. This shared IT infrastructure contains massive pools of systems that are joined along. Often, virtualization techniques are accustomed to maximizing the power of cloud computing.

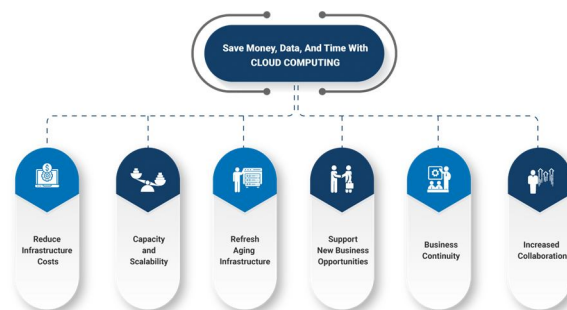
A. Benefits Of Cloud Computing

Achieve economies of scale – increase volume output or productivity with fewer individuals. Scale back payment on technology infrastructure. Maintain quick access to your info with nominal direct payment. Pay as you go (weekly, quarterly, or yearly), supported demand. widen your personnel on a budget. individuals worldwide will access the cloud, provided they need a web association. contour processes. Get additional work finished in less time with fewer individuals. scale back capital prices. There's no got to pay money on hardware, software, or licensing fees. Improve accessibility. you have got access anytime, anywhere, creating your life easier! The monitor comes additional effectively. keep among budget and sooner than completion cycle times. Less personnel coaching is required. It takes fewer people to try and do additional work on a cloud, with a nominal learning curve on hardware and software system problems. Minimize licensing new software systems. Stretch and grow while not the necessity to shop for overpriced computer code licenses or programs. Improve flexibility. you'll be able to modify direction while not serious "people" or "financial" problems at stake.



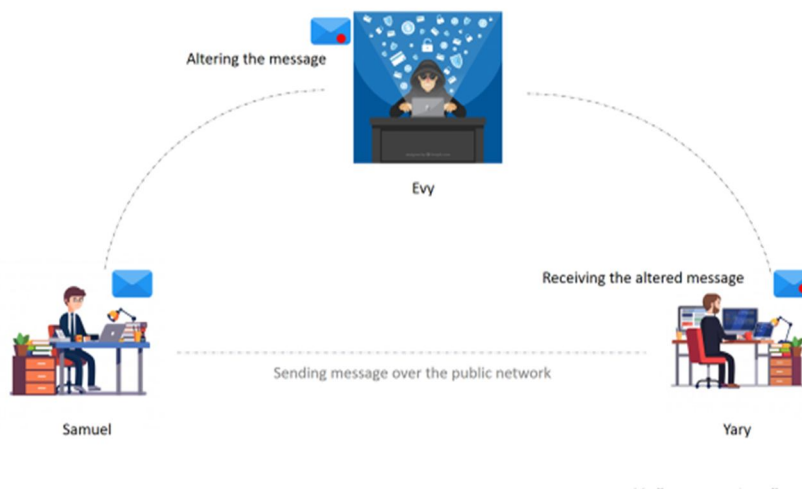
B. Advantages Of Cloud Computing

Pay for only the resources used. Cloud instances are isolated within the network from alternative instances for improved security. Instances are going to be value-added instantly for improved performance. Purchasers have access to the complete resources of the Cloud's core hardware. Auto-deploy cloud instances once required. Uses multiple servers for max redundancies. just in case of server failure, instances are going to be mechanically created on another server. able to log in from any location. Server snap and a package library allow you to deploy custom instances. Deals with a spike in traffic with fast preparation of further instances to handle the load.



II. CRYPTOGRAPHY

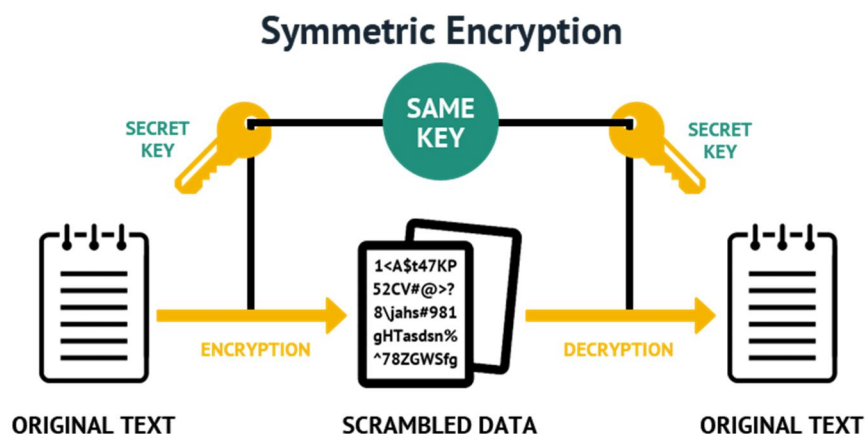
Cryptography could be a methodology of protective info and communications through the utilization of codes so only those for whom the data is meant will scan and the method it. In technology, cryptography refers to secure info and communication techniques derived from mathematical ideas and a group of rule-based calculations known as algorithms, to rework messages in ways that are exhausting to decipher. These settled algorithms are used for cryptological key generation, digital signing, and verification to guard information privacy, internet browsing on the web, and confidential communications like MasterCard transactions and email. Cryptography is closely associated with the disciplines of cryptography and cryptology. It includes techniques like microdots, merging words with pictures, and alternative ways to cover info in storage or transit. However, in today's computer-centric world, cryptography is most frequently related to scrambling plaintext (ordinary text, generally named cleartext) into ciphertext (a method known as encryption), then back once more (known as decryption). people who observe this field are referred to as cryptographers.



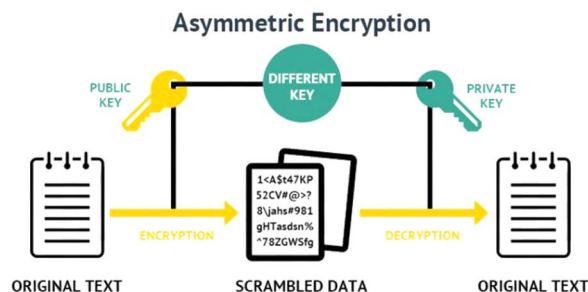
A. Types Of Cryptography

Cryptography is classed into two categories supported by the kinds of keys and cryptography algorithms:

- 1) *Symmetric Key Cryptography*: Also called Secret Key Cryptography, personal key encoding encrypts information providing a single key that only the sender and receiver understand. the secret key should be identified by each sender and therefore the receiver, however, shouldn't be sent across the channel; but, if the hacker obtains the key, deciphering the message is easier. once the sender and also the receiver meet on the telephone, the key should be addressed. though this can be not a perfect technique. as a result of the key remains constant, it's less complicated to deliver a message to a particular receiver. the info encoding framework (DES Algorithm) is the most generally used centrosymmetric key system.



- 2) **Asymmetric Key Cryptography:** Asymmetric key cryptography, additionally referred to as public-key cryptography, consists of two keys, a non-public key, that is used by the receiver, and a public key, that is declared to the general public. two completely different keys are utilized in this methodology to cipher and rewrite the information. These 2 distinct keys are mathematically connected. they're oversubscribed in pairs. the general public key's accessible to anyone, whereas the non-public key's only accessible to the one that generates these two keys.



III. OBJECTIVE

The proposed paper meets the desired security desires and implementation of the info center of the cloud server. The paper uses some regular key cryptography techniques in addition to stenography techniques. the concept of splitting and merging adds on to satisfy the principle of knowledge security. This hybrid approach once enforced during a cloud server makes the remote server safer and so, helps the cloud suppliers to do their work additional firmly. For knowledge security and privacy protection issues, the basic challenge of separation of sensitive data and access management is fulfilled. The Cryptography technique converts original information into ciphertext. The cryptography technique is split into symmetric-key cryptography and public-key cryptography. therefore only an authorized person will access data from the cloud server. Ciphertext data is visible to all people. but for that again the cryptography technique needs to be used to translate it back into the initial text.

IV. RELATED WORK

- 1) They focused on the information over-collection drawback. They tried to place all client details into a cloud the security of client details might be multiplied they have explored numerous experiments and also the output shows the effectiveness of their approach. Their most direct improvement was reducing the storage in client smartphone footage, videos and different storage info or information occupy a lot of space for storing therefore these are vacated that alter users to put in new applications. They showcased an active approach. Whenever an application needs client information it has to access requests within the cloud.
- 2) Attribute-based proxy re-encryption scheme (ABPRE) may be a new science primitive that extends the normal proxy re-encryption (public key or identity-based cryptosystem) to the attribute-based counterpart, and so empower users with delegation capability within the access management surroundings. Users, known by attributes, might freely designate a proxy that will re-encrypt a ciphertext connected with an exact access policy to another one with a different access policy. The planned scheme is proven selective-structure chosen plaintext secure and passkey secure without random oracles. Besides, we tend to develop another quite key authorization capability in our theme and additionally discuss some connected problems together with a stronger security model and applications.
- 3) In the security model symmetric algorithm uses chunk level encryption and decryption of data in cloud computing. The key size is 256 bit. The Key is rotated to achieve high-level security. For data integrity purposes hash value is generated. Hash values are garnetted after encryption and before decryption. If both hash values match then that data is in the correct form. In this security model, only valid users can access data from the cloud. The advantages of the security model are integrity, security, and confidentiality.
- 4) Three algorithms are used for the implementation of the hybrid algorithm. For user authentication purposes a digital signature is used. The blowfish algorithm is used to produce high data confidentiality. It is an asymmetric algorithm. It uses a single key. The blowfish algorithm needs the least amount of time to encode and decode. The subkey array concept is used in the blowfish algorithm. It is a block-level encryption algorithm. The main aim of this hybrid algorithm is to achieve high security for data for upload and download from the cloud. A hybrid algorithm solves the security, confidentiality, and authentication issues of the cloud.

V. SYSTEM DESIGN

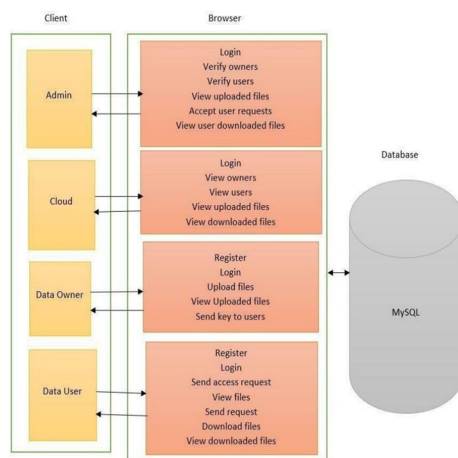


Fig 1. Project Design

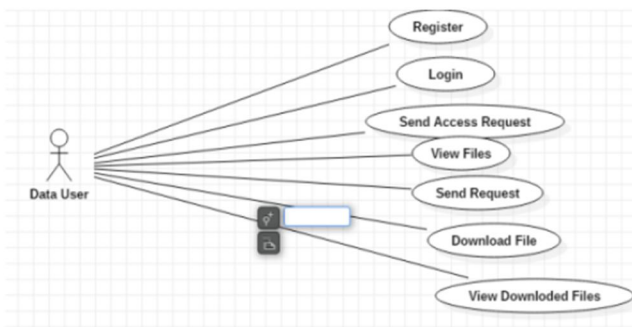
We propose a method that provides high security. The user uploads a file into the cloud which has public and private fragments. The private fragment is supposed to be securely protected. As said before we have proposed to use the Double Encryption Technique. For Double Encryption, the algorithms that we have used are AES, 3DES, and Blowfish. Here we first encrypt the private fragment containing the important information with AES128. After the first encryption is over the corresponding key is generated. This encrypted file is again subjected to encryption with another algorithm.

Fig1.1 Data owner Use case diagram.



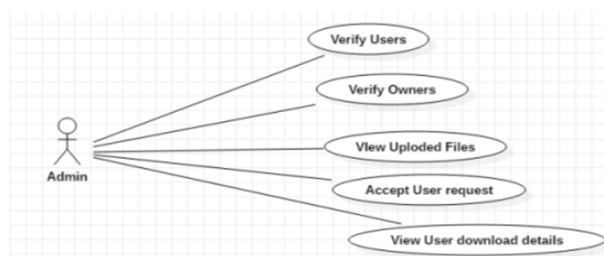
Data Owner needs to register first and through the login, the owner of the details needs to upload the file after uploading the file owner can send the key to the user.

Fig1.2 Data User Use case diagram



Data User will have to register and login through those given credentials and send an access request to the owner to view those files and then through the given key user can download the file.

Fig1.3 Admin use case diagram



Admin has to verify the user and owner after verifying admin can view uploaded files and has permission to accept user requests and can also view user download details.

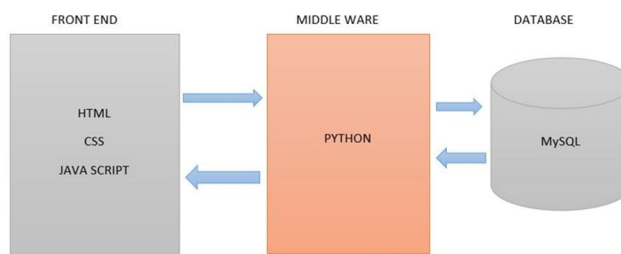


Fig 2. Technical Architecture

VI. PROPOSED SYSTEM

Algorithm

- 1) Start
- 2) Admin will be managing all the system operations.
- 3) Cloud Admin will just see the members, uploaded files, and downloaded files.
- 4) Data Owner will upload the file which is encrypted with double encryption using (AES, Blowfish & Triple DES) algorithms. The first encryption will be done by using AES the and second encryption will be done using Blowfish & triple DES based on the size of the file.
- 5) After that the file is divided into 7 fragments and will be saved in a real-time cloud (Firebase)
- 6) Data User will not able to see any files after he login then data user will request to see the files then the admin will request, when he accepts data user will see the files but not able to see the information in them.
- 7) Data User will keep request to file then the request is sent to data owner who is uploaded the file if the data owner accepts the request and send the keys to the data use.
- 8) The keys sent by the data owners are not original keys, the keys are like OTP(one-time-password) used by the particular user and a particular time.
- 9) Then data user can download the file by using that keys.
- 10) end

VII. IMPLEMENTATION

The system has been implemented using AES,3DES, and Blowfish algorithms. The algorithms are explained here.

A. Working on AES Algorithm

- 1) Obtain the key from the cipher key.
- 2) Assign the plain text to the state array.
- 3) Prefix state array with initial round key.
- 4) Perform manipulation nine times.
- 5) Carry out the tenth and last manipulation.
- 6) Copy ciphertext.

Figure 3 represents the working of the AES algorithm. AES is an iterative cipher. It is symmetrical block cipher algorithm. It is capable of encrypting 128 bits of plain text. The various keys used by this algorithm are 128,192,256 bits. It is considered the most secured algorithm

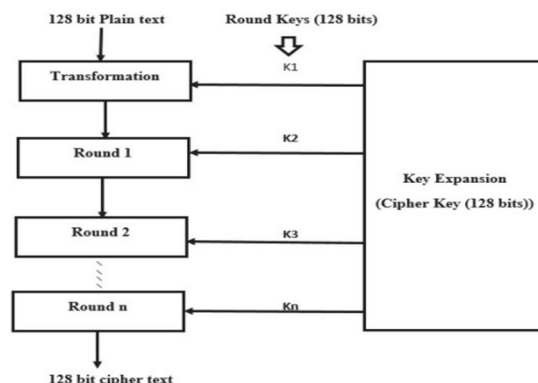


Fig. 3. Working of AES Algorithm

B. Working on 3DES Algorithm

- 1) Encrypt the plaintext blocks using a single DES with key K1.
- 2) Now decrypt the output of step 1 using a single DES with key K2.
- 3) Finally, encrypt the output of step 2 using a single DES with key K3.
- 4) The output of step 3 is the ciphertext.
- 5) Decryption of a ciphertext is a reverse process. The user first decrypts using K3, then encrypt with K2, and finally decrypts with K1.

Due to this style of Triple-DES as encrypt–decrypt–encrypt method, it's potential to use a 3TDES (hardware) implementation for one DES by setting K1, K2, and K3 to be identical to the same. This provides backward compatibility with DES. Triple DES systems are unit considerably safer than single DES, however, these are clearly a way slower method than encoding exploitation single DES.

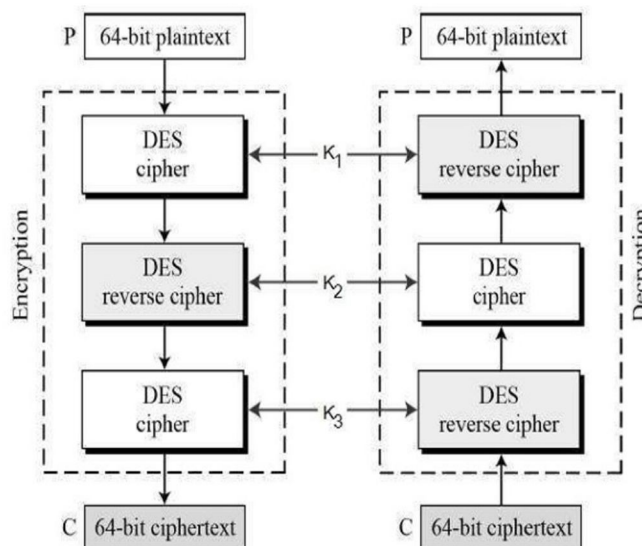


Fig.4 Working of 3DES Algorithm

C. Working on Blowfish Algorithm:

- 1) Generation of subkeys: 18 subkeys{P[0]...P[17]} are needed in both encryption as well as decryption process and the same subkeys are used for both the processes. These 18 subkeys are stored in a P-array with each array element being a 32-bit entry.
- 2) 4 Substitution boxes(S-boxes) are needed:{S[0]...S[4]} in both encryption as well as decryption process with each S-box having 256 entries{S[i][0]...S[i][255], 0≤i≤4} where each entry is 32-bit.

3) Encryption

The encryption function consists of two parts:

- Rounds:** The encryption consists of 16 rounds with each round (R_i) taking inputs from the plaintext (P.T.) from the previous round and the corresponding subkey (P_i).
- Post-processing:** The output after the 16 rounds is processed.

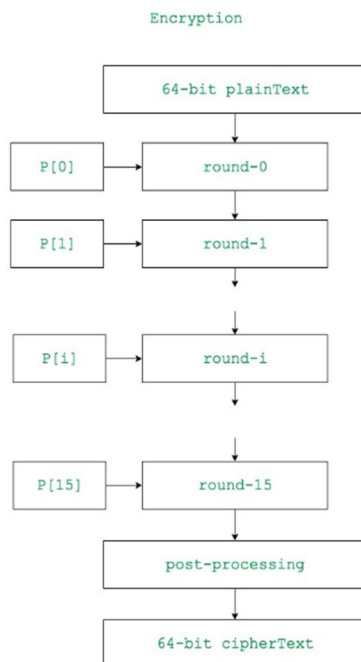


Fig 5. Working of Blowfish Algorithm

TABLE I. DATA TABLE FOR ENCRYPTION RUNTIME OF TEXT FILE

File(MB)	DES (in sec)	Blowfish (in sec)	RC5 (in sec)	3-DES (in sec)	AES+RS A (in sec)
0.1	2.5	1.2	1.5	2	1
0.5	3	1.6	1.8	2.5	1.5
0.75	4.5	4	4.2	4.5	3.5
1	5.5	4.5	4.8	5	4
Average time	15.5	11.3	13.8	14	10
Throughp ut(MB/sec)	1	1.8	1.6	1.25	2

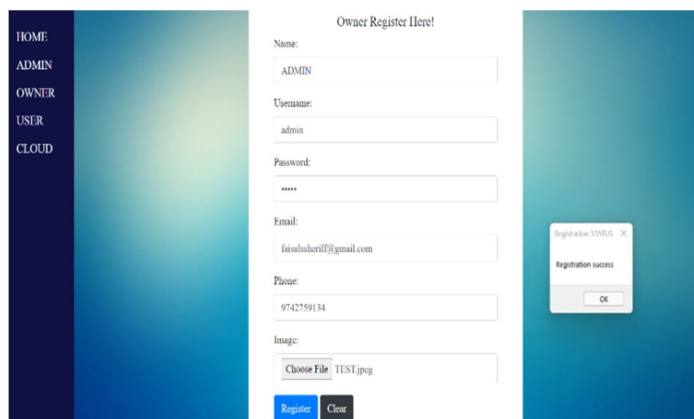
TABLE II. DATA TABLE FOR DECRYPTION RUNTIME OF TEXT FILE

File(MB)	DES (in sec)	Blowfish (in sec)	RC5 (in sec)	4-DES 5-(in sec)	AES+RSA (in sec)
0.1	2.0	1.2	1.5	1.8	1
0.5	2.5	1.8	2	2.3	1.5
0.75	3	2.3	2.5	2.7	2
1.0	4	3.5	3.5	3.8	3
Average time	11.5	8.8	9.5	10.6	7.5

VIII. IMPLEMENTATION AND RESULT

We have created a web-based application to give access to the authorized users of the application to communicate and transfer the data among themselves.

Fig.6 Owner Registration Form where the user needs to fill up the details of the form and then for verification, he needs to add an image as a captcha.



Owner Register Here!

Name:

Username:

Password:

Email:

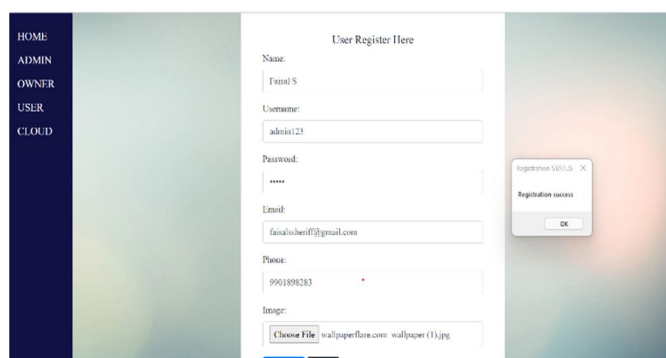
Phone:

Image:

Registration SUCCESS
Registration success
OK

Fig.6 Owner Registration Form

Fig 7. User Registration Form where the user needs to fill up the details of the form and then for verification, he needs to add an image as a captcha.



User Register Here

Name:

Username:

Password:

Email:

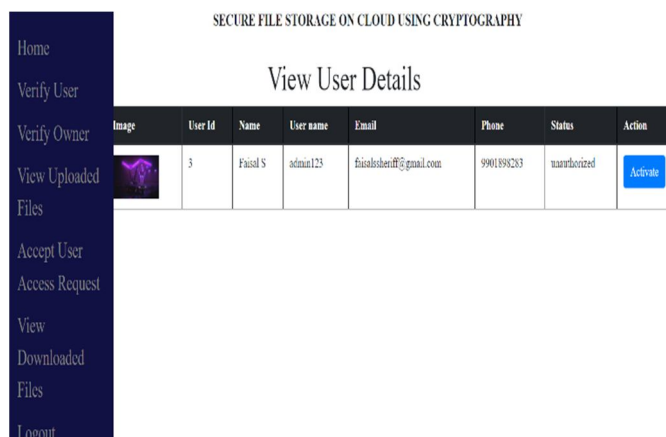
Phone:

Image:

Registration SUCCESS
Registration success
OK


Fig.7 User Registration Form

Fig.8 Admin Verifying User after the user registration process the id and status would be visible to the admin then can activate the credentials.



SECURE FILE STORAGE ON CLOUD USING CRYPTOGRAPHY

View User Details

Image	User Id	Name	User name	Email	Phone	Status	Action
	3	Faizal S	admin123	faizalsheriff@gmail.com	9901896283	Unauthorized	<input type="button" value="Activate"/>

Home
Verify User
Verify Owner
View Uploaded Files
Accept User
Access Request
View Downloaded Files
Logout

Fig.8 Admin Verifying User

Fig.9 Owner Uploading File where user can fill up filename and description then the owner needs to upload file in the cloud.

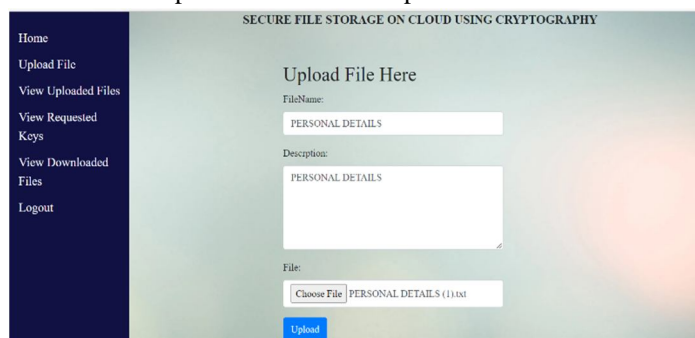


Fig.9 Owner Uploading File

Fig.10 File Uploaded in Fragments as the process of uploading text files then through the 3DES algorithm the text is split into fragments and uploaded to the cloud later can be retrieved by the user after the owner's acceptance.

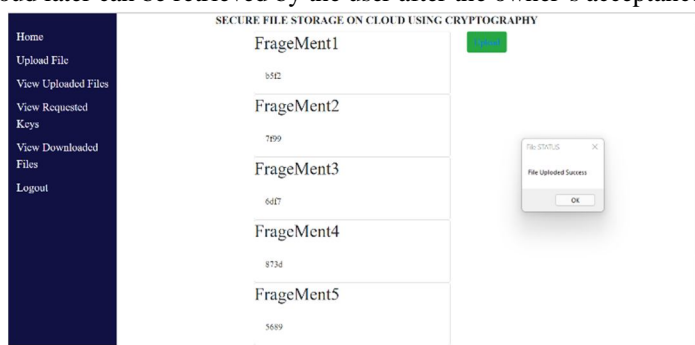


Fig.10 File Uploaded in Fragments

Fig.11 User-key request activation response page after the process of the fragments break down the user gets the key for downloading decrypted data into useful information.

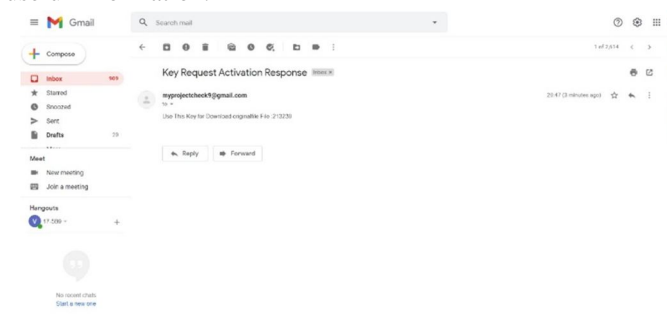


Fig.11 User-key request activation

Fig.12 User-key verification page to download the given data using the user-key which has been sent to mail id.

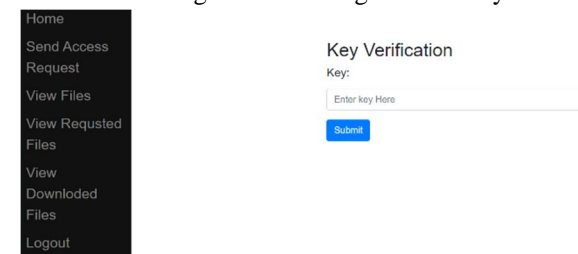


Fig.12 User-key verification page to download

Fig13. User-requested file details page through the activation key he can download the file using this link and then he download the data.

Home Send Access Request View Files View Requested Files View Downloaded Files Logout	MyRequested File Details					
	File Id	File Name	Username	Date	Owner Name	ServerStatus
	10	originalfile	vyshtmai	2021-05-27 20:45:32	niharika	accept
						Download

Fig13. User-requested file.

IX. CONCLUSION

In this paper, we tend to propose a way to supply high information security whereas using Cloud storage services. we build use of the Double cryptography Technique to extend the protection of the file. From the results obtained, our technique provides high security with resistance against propagation errors. The runtime of our algorithmic rule is less compared to the present algorithms, thus it's quick. Therefore, we tend to propose a secure and price-effective information protection technique for cloud service end-users. Our system efficiency in terms of runtime with secure protection of text information over the cloud compared with existing cryptography and decryption methodologies like AES, Blowfish, and 3DES. Our proposed conspire establishes a framework for future characteristic based, secure information for the executives and savvy contract improvement. As a future enhancement, we can accomplish high-level security using the hybridization of public-key cryptography algorithms.

REFERENCES

- [1] Fuhry, B., Hirschhoff, L., Koesnadi, S., & Kerschbaum, F. (2020). SeGShare: Secure Group File Sharing in the Cloud using Enclaves. 2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). doi:10.1109/dsn48063.2020.00061
- [2] Inder Singh, M. Prateek, "Data Encryption and Decryption Algorithms using Key Rotations N. Sharma, A. Hasan, "A New Method Towards Encryption Schemes, IEEE, International Conference on Reliability, Optimization and Information Technology, pages 310-313, Feb 2019.
- [3] Jasleen K., S.Garg, "Security in Cloud Computing using Hybrid of Algorithms", IJERJS, Volume 3, Issue 5, ISSN 2091-2730, pages 300-305, September-October, 2015
- [4] Jaspin, K., Selvan, S., Sahana, S., & Thanmai, G. (2021). Efficient and Secure File Transfer in Cloud Through Double Encryption Using AES and RSA Algorithm. 2021 International Conference on Emerging Smart Computing and Informatics (ESCI). doi:10.1109/esci50559.2021.9397005
- [5] Pronika, & Tyagi, S. S. (2021). Secure Data Storage in Cloud using Encryption Algorithm. 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV). doi:10.1109/icicv50876.2021.9388388
- [6] Subasini, C. A., & Nikkath Bushra, S. (2021). Securing of Cloud Data with Duplex Data Encryption Algorithm. 2021 5th International Conference on Computing Methodologies and Communication (ICCMC). doi:10.1109/iccmc51019.2021.9418
- [7] Kumar, S., Karnani, G., Gaur, M. S., & Mishra, A. (2021). Cloud Security using Hybrid Cryptography Algorithms. 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM). doi:10.1109/iciem51511.2021.94453
- [8] Kodumru, N. L., & Supriya, M. (2018). Secure Data Storage in Cloud Using Cryptographic Algorithms. 2018 Fourth International Conference on Computing Communication Control and Automation (ICCCUBEA). doi:10.1109/iccubea.2018.8697550



10.22214/IJRASET



45.98



IMPACT FACTOR:
7.129



IMPACT FACTOR:
7.429



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089  (24*7 Support on Whatsapp)