

VISVESVARAYA TECHNOLOGICAL UNIVERSITY

"JNANA SANGAMA" ,MACHHE, BELAGAVI-590018



**Phase-1 Project Report
on**

“SECURED DATA TRANSFER IN CLOUD USING CRYPTOGRAPHY”

Submitted in partial fulfillment of the requirements for the VII semester

Bachelor of Engineering

in

Computer Science and Engineering

of

Visvesvaraya Technological University, Belagavi.

by

Bindu S (1CD19CS033)

Anushree K (1CD19CS022)

Balaji Reddy D (1CD19CS030)

Aman Mani G (1CD19CS057)

Under the Guidance of

Ms. Shilpa V

Assistant Professor

Dept. of CSE



**Department of Computer Science and Engineering
CAMBRIDGE INSTITUTE OF TECHNOLOGY, BANGALORE - 560 036**

2022-2023

CAMBRIDGE INSTITUTE OF TECHNOLOGY

K.R. Puram, Bangalore-560 036

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING



CERTIFICATE

Certified that **Ms. Bindu S, Ms. Anushree K, Mr. Balaji Reddy D and Mr. Aman Mani G** bearing **USN 1CD19CS033, 1CD19CS022, 1CD19CS030 and 1CD19CS057** respectively, are bonafide students of **Cambridge Institute of Technology**, has successfully completed the project entitled **“Secured Data Transfer in Cloud using Cryptography”** in partial fulfillment of the requirements for VII semester **Bachelor of Engineering in Computer Science and Engineering** of **Visvesvaraya Technological University, Belagavi** during academic year 2022-2023. It is certified that all Corrections/Suggestions indicated for Internal Assessment have been incorporated in the report deposited in the departmental library. The project report has been approved as it satisfies the academic requirements in respect of project work prescribed for the Bachelor of Engineering degree.

Project Guide
Prof. Shilpa V
Dept. of CSE, CITech

Project Co-ordinator
Prof. Sandeep Kumar
Dept. of CSE. CITech

Head of the Dept.
Dr. Shashikumar D.R.
Dept. of CSE. CITech

DECLARATION

We, **Ms. Bindu S, Ms. Anushree K, Mr. Balaji Reddy D and Mr. Aman Mani G** bearing USN **1CD19CS033, 1CD19CS022, 1CD19CS030 and 1CD19CS057** respectively, are students of VII semester, Computer Science and Engineering, Cambridge Institute of Technology, hereby declare that the project entitled “**Secured Data Transfer in Cloud using Cryptography**” has been carried out by us and submitted in partial fulfillment of the course requirements of VII semester **Bachelor of Engineering in Computer Science and Engineering** as prescribed by **Visvesvaraya Technological University, Belagavi**, during the academic year 2022-2023.

We also declare that, to the best of our knowledge and belief, the work reported here does not form part of any other report on the basis of which a degree or award was conferred on an earlier occasion on this by any other student.

Date:

Name	USN	Signature
Bindu S	1CD19CS033	
Anushree K	1CD19CS022	
Balaji Reddy D	1CD19CS030	
Aman Mani G	1CD19CS057	

ACKNOWLEDGEMENT

We would like to place on record my deep sense of gratitude to **Shri. D. K. Mohan**, Chairman, Cambridge Group of Institutions, Bangalore, India for providing excellent Infrastructure and Academic Environment at CITech without which this work would not have been possible.

We are extremely thankful to **Dr. G. Indumathi**, Principal, CITech, Bangalore, for providing us the academic ambience and everlasting motivation to carryout this work and shaping our careers.

We express our sincere gratitude to **Dr. Shashikumar D.R.**, HOD, Dept. of Computer Science and Engineering, CITech, Bangalore, for his stimulating guidance, continuous encouragement and motivation throughout the course.

We also wish to extend our thanks to **Mr. Sandeep Kumar**, Project Coordinator, Dept. of CSE, CITech, Bangalore, for critical, insightful comments, guidance and constructive suggestions to improve the quality of this work.

We also wish to extend our thanks to **Ms. Shilpa V**, Assistant Professor, Dept. of CSE, CITech for her guidance and impressive technical suggestions to complete our project.

Finally, to all our friends, teachers who helped us in some technical aspects and last but not the least we wish to express deepest sense of gratitude to our parents who were a constant source of encouragement and stood by us as pillar of strength for completing this work successfully.

Bindu S	(1CD19CS033)
Anushree K	(1CD19CS022)
Balaji Reddy D	(1CD19CS030)
Aman Mani G	(1CD19CS057)

ABSTRACT

Cloud storage is an application of clouds that liberates organizations from establishing in-house data storage systems. However, cloud storage gives rise to security concerns. In case of group- shared data, the data face both cloud-specific and conventional insider threats. Secure data sharing among a group that counters insider threats of legitimate yet malicious users is an important research issue. In this paper, we propose the Secure Data Sharing in Clouds (SeDaSC) methodology that provides: 1) data confidentiality and integrity; 2) access control; 3) data sharing (forwarding) without using compute-intensive reencryption; 4) insider threat security; and 5) forward and backward access control. The SeDaSC methodology encrypts a file with a single encryption key. Two different key shares for each of the users are generated, with the user only getting one share. The possession of a single share of a key allows the SeDaSC methodology to counter the insider threats. The other key share is stored by a trusted third party, which is called the cryptographic server. The SeDaSC methodology is applicable to conventional and mobile cloud computing environments. We implement a working prototype of the SeDaSC methodology and evaluate its performance based on the time consumed during various operations. We formally verify the working of SeDaSC by using high-level Petri nets, the Satisfiability Modulo Theories Library, and a Z3 solver. The results proved to be encouraging and show that SeDaSC has the potential to be effectively used .

CHAPTER 1

INTRODUCTION

1.1 Background

Cloud computing is rapidly emerging due to the provisioning of elastic, flexible, and on-demand storage and computing services for customers. Organizations with a low budget can now utilize high computing and storage services without heavily investing in infrastructure and maintenance in the present scenario. However, the loss of control over data and computation raises many security concerns for organizations, thwarting the wide adaptability of the public cloud. The loss of control over data and the storage platform also motivates cloud customers to maintain the access control over data (individual data and the data shared among a group of users through the public cloud). Moreover, the privacy and confidentiality of the data is also recommended to be cared for by the customers. The confidentiality management by a customer ensures that the cloud does not learn any information about the customer data.

Cryptography is used as a typical tool to provide confidentiality and privacy services to the data. The data are usually encrypted before storing to the cloud. The access control, key management, encryption, and decryption processes are handled by the customers to ensure data security. However, when the data are to be shared among a group, the cryptographic services need to be flexible enough to handle different users, exercise the access control, and manage the keys in an effective manner to safeguard data confidentiality. The data handling among a group has certain additional characteristics as opposed to two-party communication or the data handling belonging to a single user. The existing, departing, and newly joining group members can prove to be an insider threat violating data confidentiality and privacy. Insider threats can prove to be more devastating due to the fact that they are generally launched by trusted entities. Due to the fact that people trust insider entities, the research community focuses more on outsider attackers. Nevertheless, multiple security issues can arise due to different users in a group. We discuss some of the issues in the following discussion.

1.2 Technology Used :

Cryptography is the process of hiding or coding information so that only the person a message was intended for can read it. The art of cryptography has been used to code message for thousands of years and continues to be used in bank cards, computer passwords, and e-commerce. Modern cryptography techniques include algorithms and ciphers that enable the encryption and decryption of information, such as 128-bit and 256-bit encryption.

1.3 Applications:

1.3.1 Secure communications:

The most obvious use of cryptography, and the one that all of us use frequently, is encrypting communications between us and another system. This is most commonly used for communicating between a client program and a server. Examples are a web browser and web server, or email client and email server. When the internet was developed it was a small academic and government community, and misuse was rare. Most systems communicated in the clear (without encryption), so anyone who intercepted network traffic could capture communications and passwords. Modern switched networks make interception harder, but some cases – for example, public wifi – still allow it. To make the internet more secure, most communication protocols have adopted encryption. Many older protocols have been dropped in favour of newer, encrypted replacements.

The best example is web encryption, since here you can choose between a clear or encrypted version of a website by switching between HTTP and HTTPS in the URL. Most large companies now use the encrypted form by default, and you'll see that any visit to Google, Facebook, Microsoft Office 365 or other sites will be to the HTTPS version of the site. This is accompanied in recent browsers by extra information, including a padlock to show that it is HTTPS. Something you can try is to click the padlock on an encrypted page, and your browser will tell you more about the page security. It will also tell you the especially relevant fact of the actual site name you're visiting.

Therefore, if you're entering a password in a page, please do check that it is HTTPS.

1.3.2 End-to-end Encryption:

Email is one area where encryption is not widely in use. When email moves from server to server, and from server to you, it is encrypted. On the mail server and on your system, however, an administrator can read it. There are options to implement "end-to-end" encryption for email (I use PGP) but email systems are complex and these options are complex. Truly secure messaging systems – where only the sender and receiver can read the message – are those where encryption has been built in from the start. Whatsapp is good; Signal is better.

1.3.3 Storing Data:

We all store a large amount of data, and any data is valuable to at least the person who generated it. Every operating system uses encryption in some of the core components to keep passwords secret, conceal some parts of the system, and make sure that updates and patches are really from the maker of the system.

A more notable use of encryption is to encrypt the entire drive, and require correct credentials to access it. UCL has recently implemented Microsoft's Bitlocker on Desktop@UCL machines, and this means that without the user logging into the data on the drive is completely opaque. If someone took the drive and tried to read it, they would not be able to access any data. This has the occasional side effect of locking the system, so some UCL readers may have had to request the recovery key. One notable point is that many encrypted system may have had to request administrators of the system access. Office 365, for example, uses encrypted nonetheless allow but many senior Microsoft staff, and a few UCL administrators, can access the data. A relatively recent development is software to create encrypted containers on a drive.

1.3.4 Storing passwords:

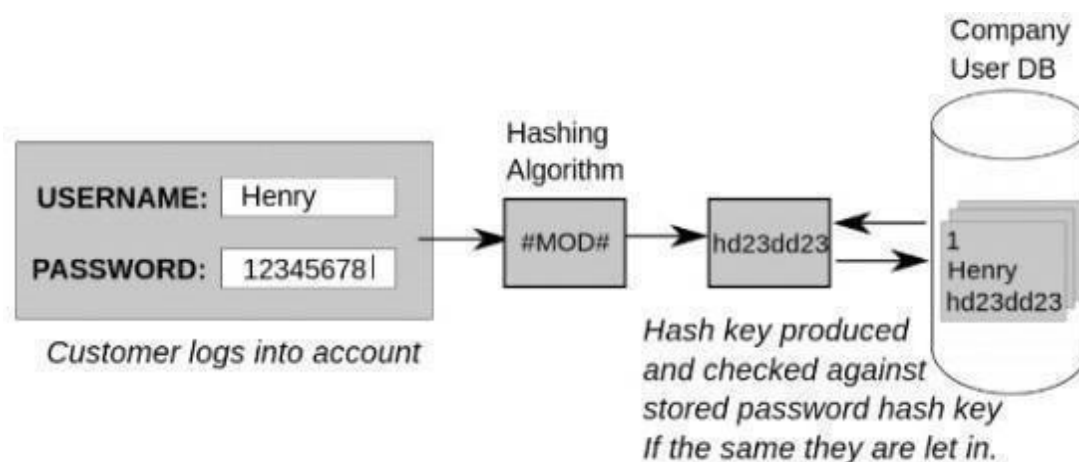


Fig 1.1: Login view

In the last blog post I briefly introduced cryptographic hashing, a one-way mapping of a string to a fixed-length value. One of the main uses of this is to store passwords. It is very risky to store passwords in an accessible way. If stored in plaintext on a system, anyone who has access to the system – legitimate or malicious – can read the password. Encryption is only a partial answer to storing passwords. If someone has access to the system storing the encrypted passwords, they will probably have access to the encryption key to decrypt the password. Hashing, on the other hand, produces a relatively useless value for the attacker. A system will take the password on login, hash it, and compare to the hashed value. At no point will the system – or an attacker – have access to the plaintext password.

1.4 Motivation:

Classically, cryptography used "security by obscurity" as way **to keep the transmitted information secure**. In those cases, the technique used was kept secret from all but a few, hence the term "obscurity." This made the communication secure, but it was not very easy to implement on a wide scale.

1.5 Problem Statement:

Cloud security is quickly establishing itself as a major difference and competitive advantage among cloud providers. Cloud security may soon be more secure than the level attained by IT departments using their own hardware and software, thanks to the application of more robust security approaches and policies. The lack of trust in the cloud provider is a major roadblock to shifting IT systems to the cloud. The cloud provider, in turn, must enforce stringent security measures, which necessitates increased client trust. A robust trust foundation must be in place to improve mutual trust between the user and the cloud provider. To various people, cloud computing might mean different things. A consumer utilizing a public cloud application and a medium-sized organization using a customized suite of business apps on a cloud platform will undoubtedly have distinct privacy and security concerns, and this will result in a different set of benefits and hazards.

The real value that the user tries to protect, however, remains constant. The value that is at danger for an individual can range from civil liberties to the contents of bank accounts. The worth of a business can range from crucial trade secrets to business continuity and public reputation. Much of this is difficult to assess and convert into common value metrics. The goal of this transition is to weigh the benefits of cloud adoption against the hazards of doing so. Why isn't everyone using cloud computing if it's so beneficial? Because the cloud functions as a large black box, nothing inside it is visible to the client, who leads to two major issues: Integrity It's a measure of how confident you are that your data in the cloud is safe from unintentional or malicious alteration. As a result, data should be stored on cloud servers honestly, and any violations can be identified. Privacy All sensitive data, such as credit card numbers, is hidden in this approach, and only authorized users has access to it. Google Docs had a major problem on the SAAS cloud in 2009. Google Docs allows users to edit documents online while also sharing them with others. However, once these documents were shared with anyone, they became available to everyone. As a result, in this era of personal privacy, personal data should be protected at all costs.

CHAPTER 2

LITERATURE SURVEY

2.1 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 style 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 how 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.

2.2 RELATED WORK

[1] Jasleen K., S.Garg, "Security in Cloud Computing using Hybrid of Algorithm", IJERJS, Volume 3, Issu 5, ISSN 2091-2730, pages 300-305, SeptemberOctober, 2015.

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] 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
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.

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] 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

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 generated 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] 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

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.

CHAPTER 3

SYSTEM ANALYSIS

Analysis is the process of breaking a complex topic or substance into smaller parts to gain a better understanding of it. Gathering requirements is the main attraction of the Analysis Phase. The process of gathering requirements is usually more than simply asking the users what they need and writing their answers down. Depending on the complexity of the application, the process for gathering requirements has a clearly defined process of its own.

3.1 Proposed System:

The aim of the project is to transfer data from sender to receiver using cloud computing. The main model of the project is mainly divided into two phases. The first phase the sender registers and uploads a file and sets a password. In second phase the receiver receives the file and access it by entering the password.

3.2 Hardware Requirements:

One machine is needed with following minimal requirement for this,

- System : Intel Core i3,i5,i7 and 2GHz Minimum
- Ram : 4 GB
- Hard Disk : 50 GB or above
- Input Device : Keyboard and Mouse
- Output Device : Monitor or PC

3.3 Software Requirements:

Operating System : Windows 7 and above

Language : Python

Database : Django framework MySQL database

3.4 User Requirements:

The requirements of the product is given as use cases below.

Table 3.1 User Requirement

SI.no	Requirements
Req.1	User can register and login
Req.2	User can upload any file
Req.3	The file should be detected
Req.4	The user should set password for the file
Req.5	The file should be sent to the user
Req.6	The receiver can access the file by entering password

CHAPTER 4

DESIGN

4.1 Purpose

The proposed paper meets the desired security desires and implementation of the info center of the cloudserver. 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 1 firmly. For knowledge security and privacy protection issues, the basic challenge of separation data and access management is fulfilled.

4.2 Different Types Of Cryptography

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

- **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
- **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.

4.3 Scope:

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.

4.4 System Architecture

We propose a method that provides high security. The user uploads a file into the cloud which has published 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 algorithm that we have used are AES, 3DES, 3DES and, 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.

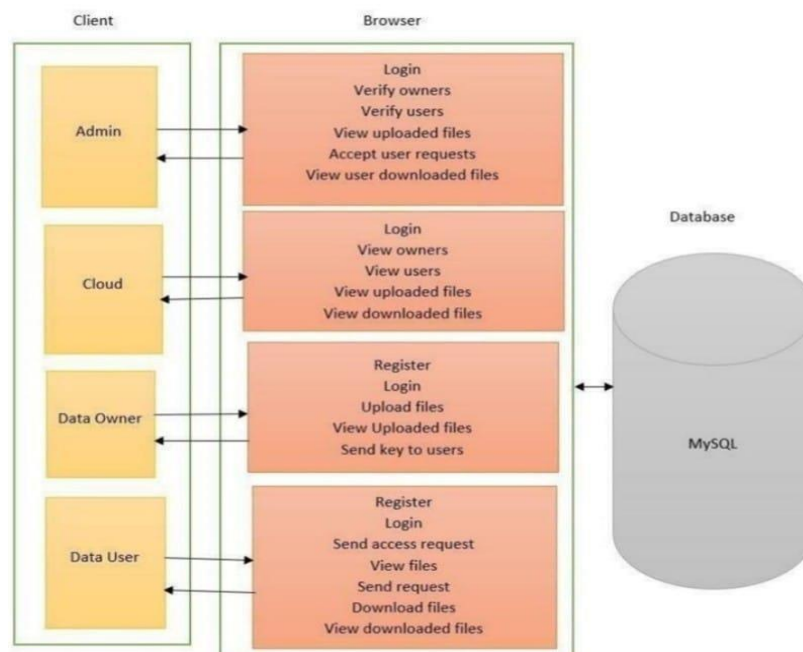


Fig. 4.1 System Architecture

4.5 Use Case Model

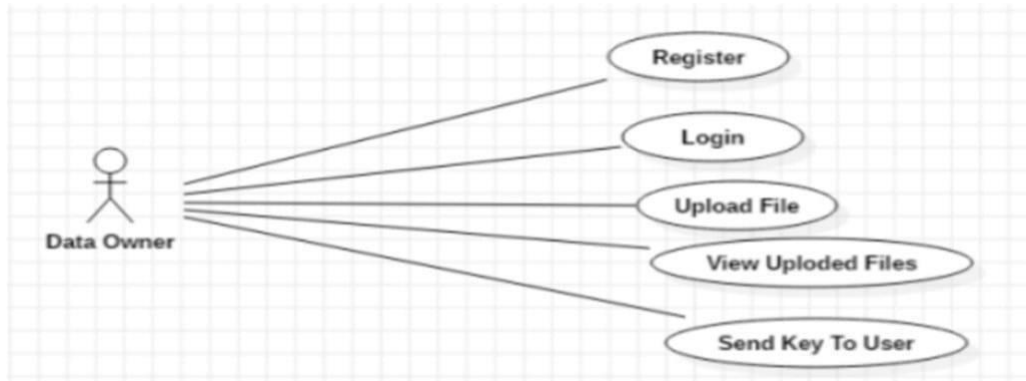


Fig 4.2 Data owner use case diagram

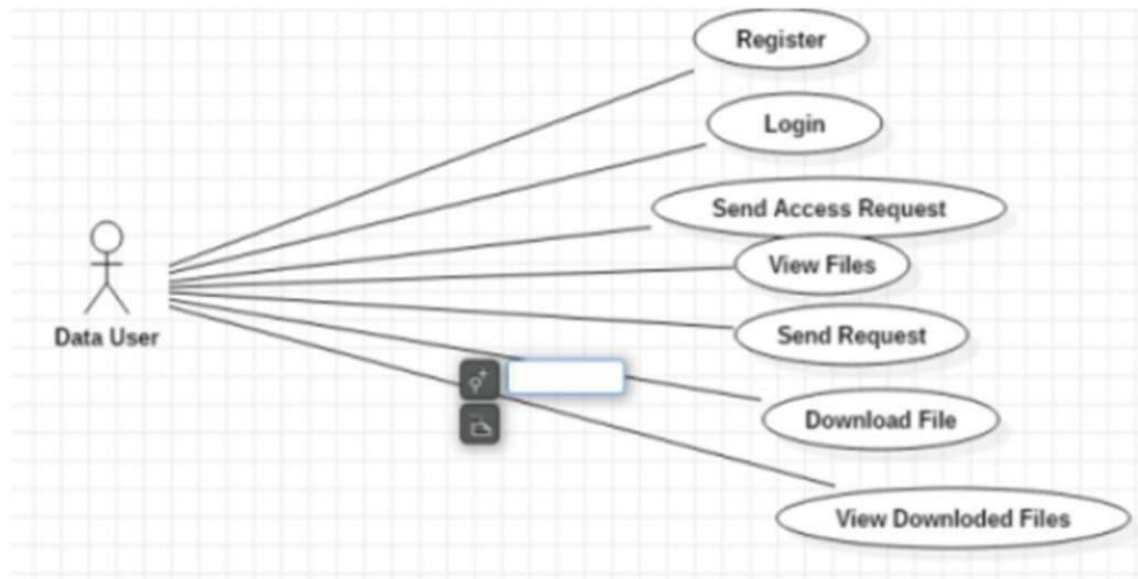


Fig. 4.3 Data user use case diagram

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

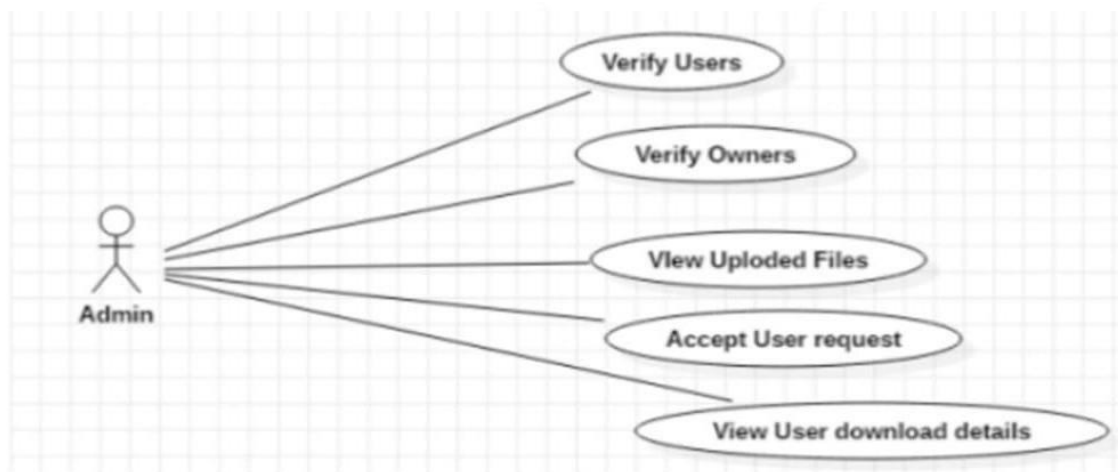


Fig. 4.4 Admin use case diagram

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.

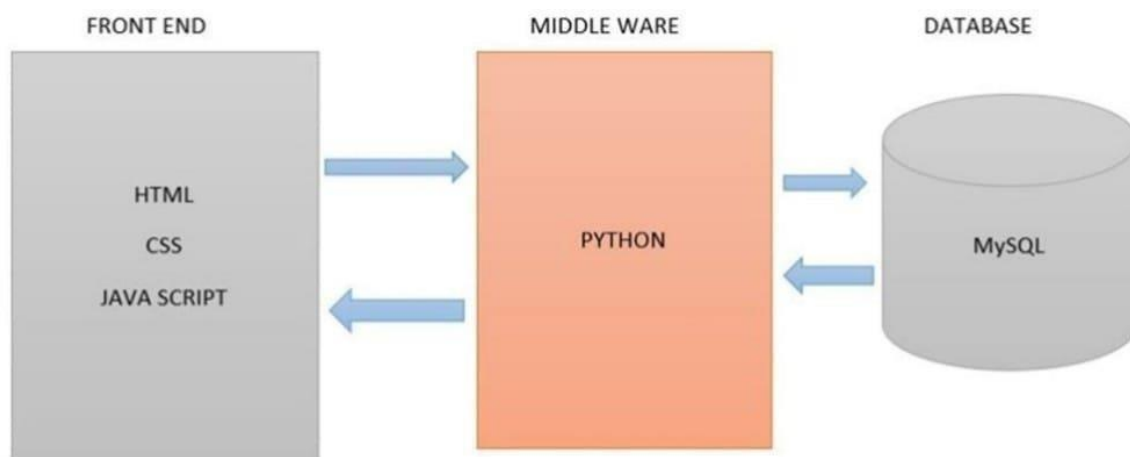


Fig. 4.5 Technical Architecture

4.6 Activity Diagram

An activity diagram shows business and software processes as a progression of actions. These actions can be carried out by people, software components or computers. Activity diagrams are used to describe business processes and use cases as well as to document the implementation of system processes. Even the most complex progression can be visualized by activity diagrams. Activity diagram represent activities that are made up by a flow of actions.

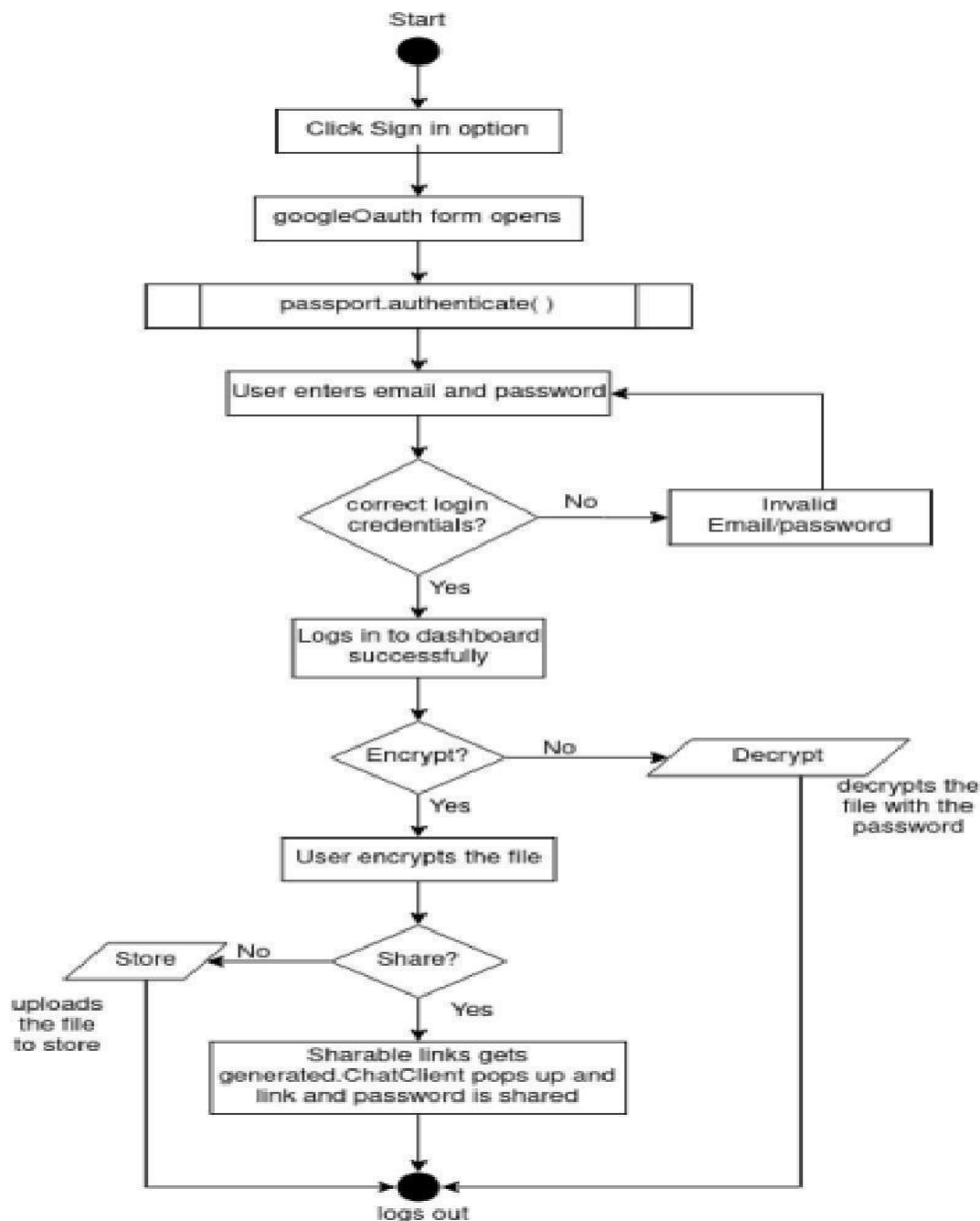


Fig 4.6 Activity Diagram

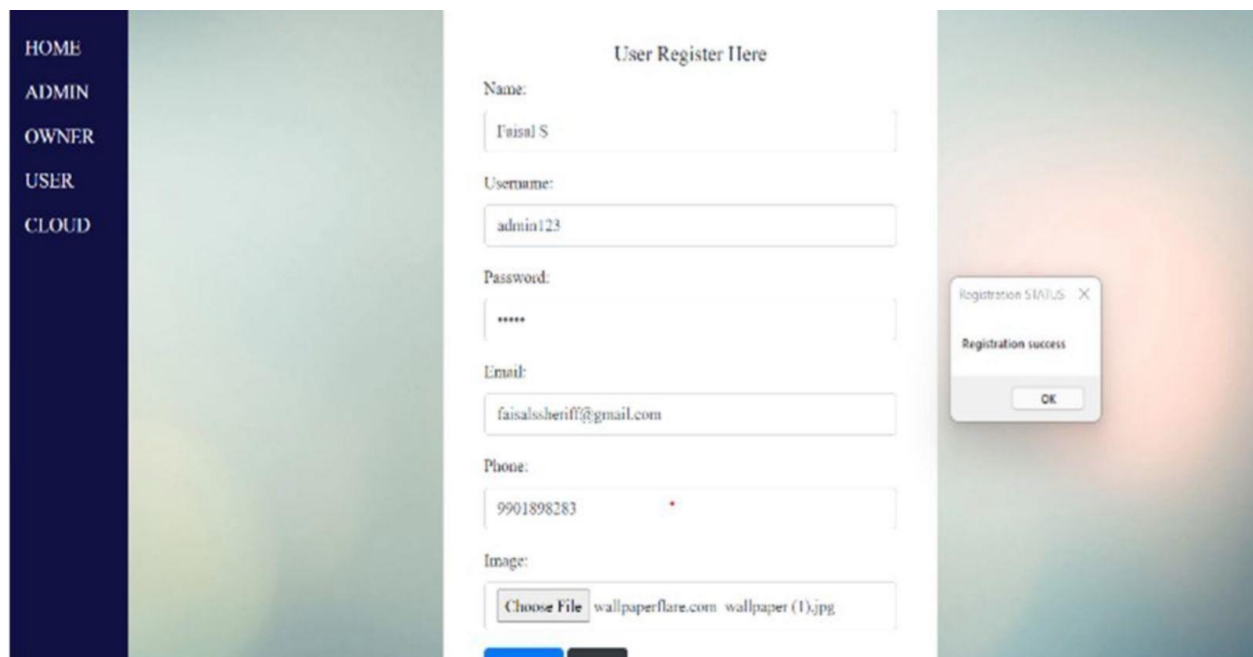
CHAPTER 5

EXPECTED OUTCOMES

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. In this study the proposed web application was built to provide an encryption/decryption tool and securely share and store the files using cryptographic modules and packages. From the practical implementation we got the following results:

The screenshot displays a web application interface for owner registration. On the left, a dark blue sidebar contains navigation links: HOME, ADMIN, OWNER, USER, and CLOUD. The main content area has a light blue background and is titled "Owner Register Here!". It contains a registration form with the following fields: Name (filled with "ADMIN"), Username (filled with "admin"), Password (masked with "*****"), Email (filled with "fnisulsherriff@gmail.com"), Phone (filled with "9742759134"), and Image (with a "Choose File" button and "TEST.jpeg" text). At the bottom of the form are "Register" and "Clear" buttons. To the right of the form, a small white modal box with a blue border displays the message "Registration success" and an "OK" button.

Fig 5.1: Owner Registration Form



The image shows a user registration form titled "User Register Here". The form includes fields for Name, Username, Password, Email, Phone, and Image. A "Choose File" button is next to the Image field. To the right of the form, a modal window titled "Registration STATUS" displays "Registration success" with an "OK" button.

User Register Here

Name: Faisal S

Username: admin123

Password: *****

Email: faisalssheriff@gmail.com

Phone: 9901898283

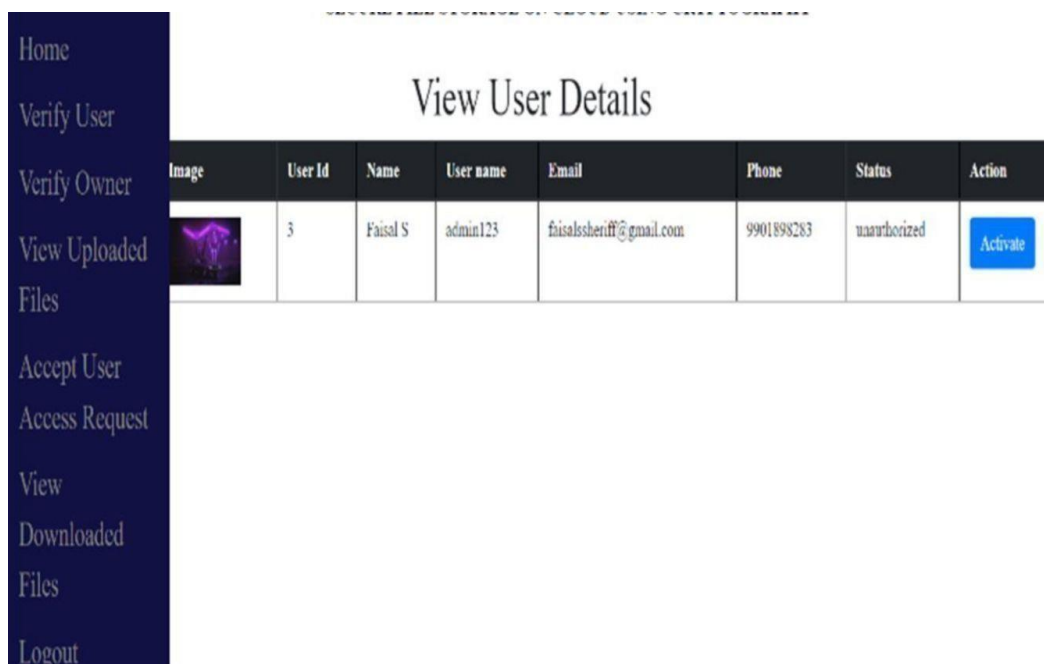
Image: Choose File wallpaperflare.com wallpaper (1).jpg

Registration STATUS X

Registration success

OK

Fig 5.2: User Registration Form



The image shows an admin interface titled "View User Details". On the left is a dark blue sidebar menu with options: Home, Verify User, Verify Owner, View Uploaded Files, Accept User, Access Request, View Downloaded Files, and Logout. The main content area displays a table with user details. The table has columns: Image, User Id, Name, User name, Email, Phone, Status, and Action. One user is listed with the status "unauthorized" and an "Activate" button in the Action column.


Image	User Id	Name	User name	Email	Phone	Status	Action
	3	Faisal S	admin123	faisalssheriff@gmail.com	9901898283	unauthorized	<button>Activate</button>

Fig 5.3: Admin Verifying User

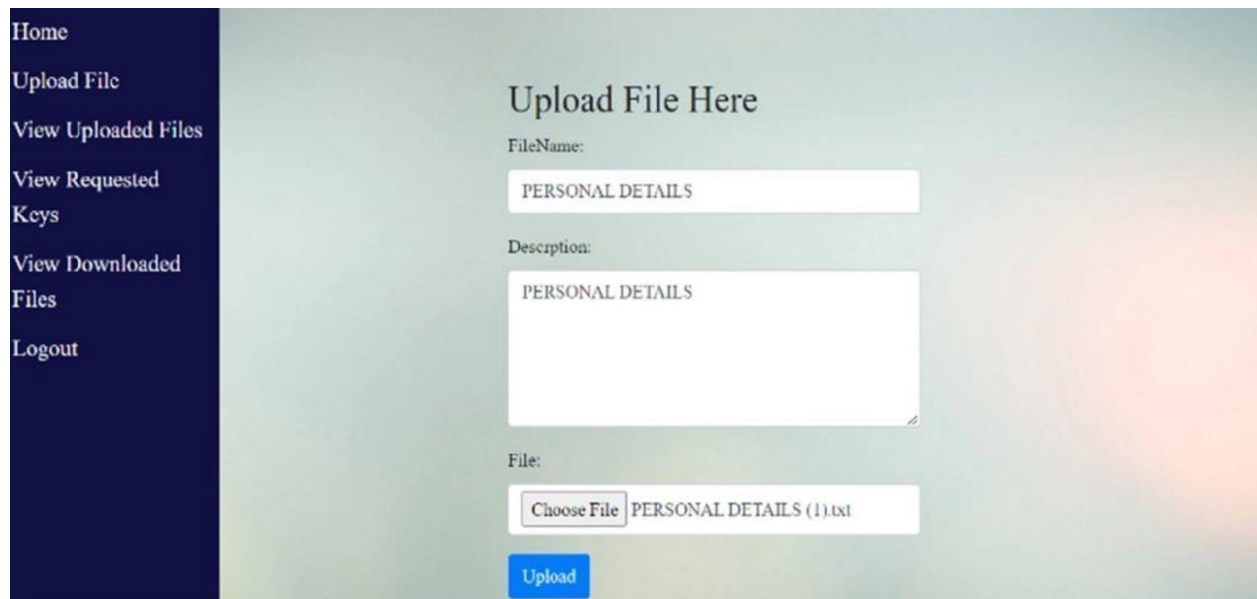


Fig 5.4: Owner Uploading File



Fig 5.5: User-keyrequest activation

Home

Send Access Request

View Files

View Requested Files

View Downloaded Files

Logout

Key Verification

Key:

Submit

Fig 5.5: User-key verification page to download

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

Fig 5.6: User-requested file

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 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.

With the growing demands on the cloud storage platforms, simplifying the Interface and solidifying the underlying security is the main concern as the sharing of an individual's data is not as private as one assumes. The vulnerability of cloud storage and lack of security results in the loss of millions of data. Thus, in order to enhance the process of security for the storage and sharing of data we've created this web application which uses a cryptographic approach to secure the user data. We can also improve our proposed algorithm for encrypting and decrypting larger files. We can add push notifications and shareable links that'll expire after the stipulated time. Additionally, we can add other authentications like GitHub and Twitter.

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, SeptemberOctober, 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.

Vision

To become a premier institute transforming our students to be global professionals.

Mission

M1: Develop competent Human Resources, and create state-of-the-art infrastructure to impart quality education and to support research.

M2: Adopt tertiary approach in teaching – learning pedagogy that transforms students to become professionally competent technocrats and entrepreneurs.

M3: Nurture and train students to develop the qualities of global professionals.

Department of Computer Science and Engineering

Vision

To impart quality education in the field of Computer Science and Engineering with emphasis on innovative thinking, communication and leadership skills to meet the global challenges in IT paradigm.

Mission

M1: Focus on student centric approach through experiential learning and necessary infrastructure.

M2: Develop innovative thinking, communication and leadership skills by creating conducive environment and relevant training.

M3: Enrich students by developing the traits of global professionals.



CAMBRIDGE INSTITUTE OF TECHNOLOGY

K. R. PURAM, BENGALURU - 560036