Secure File Storage on Cloud using Hybrid Cryptography

A PROJECT REPORT

Submitted by

CH.EN.U4CSE19113	VENKATA KRISHNA REDDY
CH.EN.U4CSE19136	RAVI VENKAT JAYANTH

in partial fulfillment for the award of the degree of

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING

AMRITA SCHOOL OF COMPUTING, CHENNAI

AMRITA VISHWA VIDYAPEETHAM

CHENNAI - 601103

AMRITA VISHWA VIDYAPEETHAM

AMRITA SCHOOL OF COMPUTING,CHENNAI - 601103

AMRITA
VISHWA VIDYAPEETHAM

BONAFIDE CERTIFICATE

This is to certify that the project report entitled **"Secure File Storage on Cloud using Hybrid Cryptography"** submitted by

CH.EN.U4CSE19113	VENKATA KRISHNA REDDY
CH.EN.U4CSE19136	RAVI VENKAT JAYANTH

in partial fulfillment of the requirements as part of **Bachelor of Technology** in **"Computer Science and Engineering"** is a bonafide record of the work carried out under my guidance and supervision at Amrita School of Computing, Chennai.

Dr. SP CHOKKALINGAM
Associate Professor
Department of CSE

11/5/23
Dr. S SOUNTHARRAJAN
Associate Professor and Program Head
Department of CSE

This project report was evaluated by us on 18/05/2023

18/5/23
INTERNAL EXAMINER

EXTERNAL EXAMINER 18/5/2023

DECLARATION

I the undersigned solemnly declare that the thesis **SECURE FILE STORAGE ON CLOUD USING HYBRID CRYPTOGRAPHY** is based on my own work carried out during the course of our study under the supervision of **Dr. SP Chokkalingam** , Department of CSE, Computer Science & Engineering, and has not formed the basis for the award of any other degree or diploma,in this or any other Institution or University. In keeping with the ethical practice in reporting scientific information, due acknowledgement has been made wherever the findings of others have been cited.

Venkata Krishna Reddy
Venkata Krishna Reddy
Rvjayanth
Ravi Venkat Jayanth

ACKNOWLEDGEMENTS

The satisfaction that accompanies successful completion of any task would be incomplete without mention of people who made it possible, and whose constant encouragement and guidance have been source of inspiration throughout the course ofthis project work.

We offer our sincere pranams at the lotus feet of **”AMMA”, MATA AMRITANANDAMAYI DEVI** who showered her blessing upon us throughout the course of this project work.

We owe our gratitude to **Dr. V. Jayakumar**, Principal, Amrita School of computing, Chennai.

We thank **Dr. S. Sountharrajan,** Program Head-CSE, Amrita School of Computing, Chennai for his support and inspiration.

It is a great pleasure to express our gratitude and indebtedness to our project guide **Dr. SP Chokkalingam**, Department of Computer Science and Engineering, Amrita School of Computing, Chennai for her/his valuable guidance, encouragement, moral support, and affection throughout the project work.

Accept my endless gratitude to my Project Coordinator **Dr. A Padmvathi ,**Department of Computer Science and Engineering, Amrita School of Computing, Chennai, for the constant source of inspiration.

We would like to thank express our gratitude to project panel membersfor their suggestions, encouragement, and moral support during the process of project work and all faculty members for their academic support. Finally, we are forever grateful to our parents, who have loved, supported, and encouraged us in all our endeavors.

Venkata Krishna Reddy
Ravi Venkat Jayanth

ABSTRACT

Many sectors, including the military, education, and business, use the cloud to offer a wide range of services and store enormous amounts of data. Users can request access to, or retrieval of data kept in this cloud without having direct access to the server computer. Because to the rapidly growing use of cloud computing by IT industries and organizations, new software is made accessible at a low cost. The benefits of cloud computing include accessibility to knowledge at minimal cost. Cloud computing has a few advantages, including low costs and simple Internet access to knowledge. Keeping data from an unstable cloud and safely transmitting it is still a challenge. Our approach stores the data over a single cloud using AES, DES, and RSA algorithms, assuring the security and privacy of sensitive client data.

In this study, a hybrid cryptographic approach is suggested to store files securely on the cloud. The recommended approach combines the benefits of symmetric and asymmetric cryptography to guarantee the privacy, availability, and integrity of the stored files. For symmetric and asymmetric encryption, the system employs RSA and AES, respectively. The access to the files is restricted by a strong access control mechanism, and the encryption keys are safely produced and kept using a key management system. The suggested system can be utilized in a variety of applications, including the healthcare, financial, and governmental sectors, and it offers a high level of security for file storage on the cloud. The experimental findings show that the suggested method is efficient and successful in terms of performance and security.

It's crucial to store important files securely on the cloud to guard against unauthorized access. To obtain a high level of security, hybrid cryptography mixes symmetric and asymmetric encryption. This paper suggests a hybrid cryptographic file storage solution for the cloud. Asymmetric encryption is utilized in the system for key management, whereas symmetric encryption is used for file encryption and decryption. Additionally, the system includes mechanisms for key management and access control to guarantee the safe transfer of files between authorized users. The system is assessed using several measures, such as security, efficacy, and usability, and the findings show how well it performs in terms of offering safe file storage on cloud platforms. The suggested system can be used for a variety of cloud-based applications where security and privacy are top priorities, such as data sharing, backup, and disaster recovery.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVATIOS

AES	ADVANCED ENCRYPTION STANDARD
DES	DATA ENCRYPTION STANDARD
ACL	ACCESS CONTROL LIST
CSP	CLOUD SERVICE PROVIDER
DO	DATA OWNER

CHAPTER - 1

1.1 INTRODUCTION

Databases and programs hosted on remote servers accessible over the Internet are commonly referred to as the "cloud". Cloud servers are located in data centers around the world. Cloud computing frees users and businesses from maintaining physical servers and relying on personal computers to perform tasks.

These servers, so-called cloud servers, are distributed in different data centers around the world. By using cloud computing, individuals and organizations can eliminate the cumbersome tasks of maintaining physical servers and relying solely on their own computers to perform tasks. Instead, you can easily and remotely store data, run applications, and access computing power using the resources and infrastructure provided by cloud service providers.

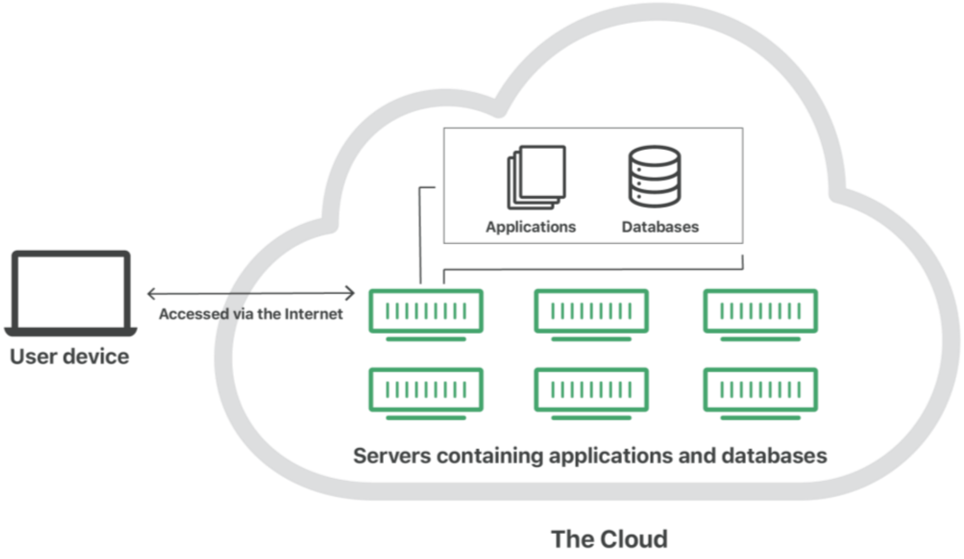

Applications
Databases
User device
Accessed via the Internet
Servers containing applications and databases
The Cloud

Fig 1.1 Cloud Flow diagram

Cryptography is a method for securing information and communication so that only those who were meant to can read and understand it. It does this by using codes.

1.1.1 Advanced Encryption Standard (AES)

The AES algorithm, also known as the Rijndael algorithm. The AES algorithm operates on distinct blocks of data, typically 128 bits in size, and utilizes encryption keys of varying lengths, including 128, 192, and 256 bits. Each block is encrypted independently, and the resulting ciphertext is obtained by combining the encrypted blocks. The AES algorithm is based on a substitution-permutation network (SPN) architecture. This design incorporates substitution and permutation operations to achieve secure encryption of data blocks. The AES (Advanced Encryption Standard) algorithm is comprised of multiple interconnected processes, which include bit shuffling and substitution operations.

These processes are designed to transform inputs into specific outputs as part of the encryption process, ensuring the confidentiality and integrity of the data being encrypted.

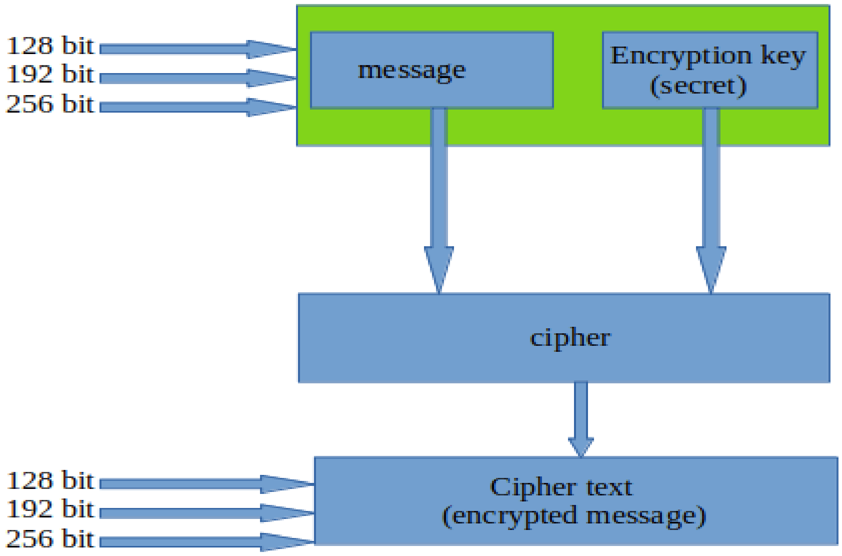


Fig 1.2 Flow diagram illustrating how AES encrypts data

1.1.2 Data Encryption Standard (DES)

It stands for Data Encryption Standard. The key size used by the DES algorithm is 56 bits. This key is used to convert plaintext into ciphertext and vice versa throughout the encryption and decryption procedures. Using a unique key, the DES algorithm converts a 64-bit block of plaintext into a corresponding 64-bit block of ciphertext. DES is a legacy encryption algorithm that is gradually being replaced by more secure algorithms with larger key sizes, such as AES (Advanced Encryption Standard).

DES was widely used as a standard encryption algorithm for many years due to its efficiency and widespread adoption, but its key size is now considered inadequate for modern security requirements. If the algorithm utilized an asymmetric encryption approach, the encryption key and the decryption key would not be the same.

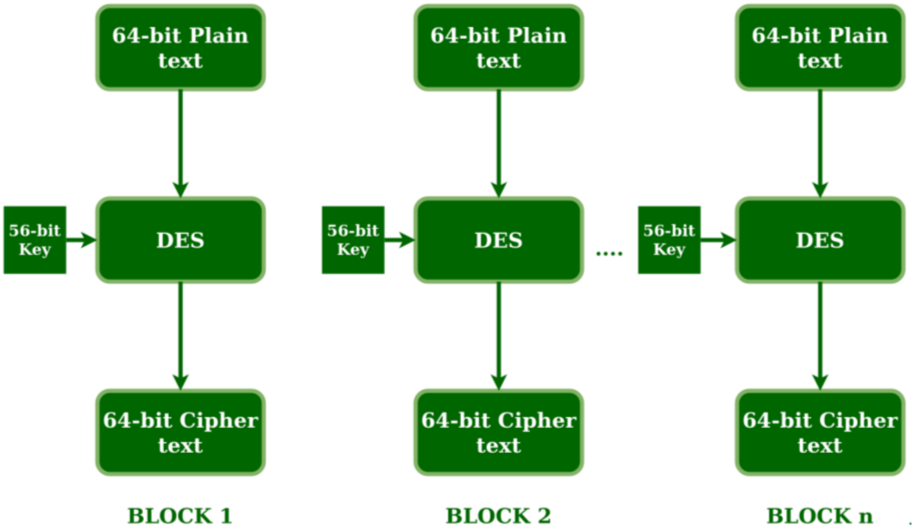


Fig 1.3 Structure of DES

1.1.3 RSA Algorithm

The public key and the private key are the two keys that are utilized in RSA for encryption and decryption, respectively. The private key is kept hidden by the owner and is used to decrypt the encrypted data, while the public key is shared with others and used to encrypt data. Numerous applications, including secure internet communication, digital signatures, and the encryption of sensitive data, make extensive use of RSA.

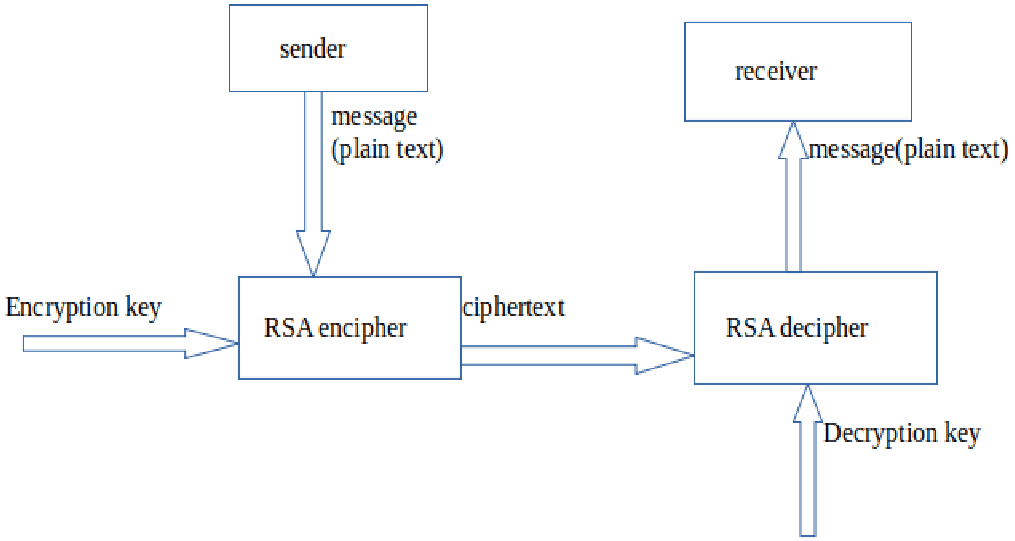


Fig 1.4 Flow diagram illustrating how RSA encrypts data

Cloud file storage security is a major problem for both consumers and businesses. In comparison to conventional on-premises storage options, cloud storage has many benefits, including adaptability, availability, and affordability. However, because the cloud storage infrastructure is frequently managed by a third party and accessed over the internet, these advantages come with security risks.

Hybrid cryptography can be used to secure cloud-stored files to lessen these concerns. Data confidentiality, integrity, and authenticity are provided by hybrid cryptography, which combines the advantages of symmetric and asymmetric cryptography. In hybrid cryptography, the symmetric key is protected using asymmetric encryption while the actual data is encrypted using symmetric encryption. This strategy guarantees that the data is secure even if the key is stolen. Before the data is uploaded to the cloud, it is encrypted locally using a symmetric key. The key is then delivered to the cloud after being encrypted using the recipient's public key.

The recipient downloads the encrypted file and uses their private key to decrypt the symmetric key when they need to view the data. The data can then be decrypted using the symmetric key. End-to-end encryption is provided through this method, making the data only accessible to the intended recipient.

File storage on the cloud is safe and effective when done with hybrid cryptography. It enables simple file sharing and collaboration while offering high security guarantees. It additionally offers a full security solution for cloud storage by encrypting data both in transit and at rest.

Introduction

Availability and portability are only a couple of the advantages that cloud storage offers, but it also creates security issues. To safeguard data both in transit and at rest, hybrid cryptography is a system that combines the advantages of symmetric and asymmetric encryption. In this method, an asymmetric key is used to encrypt the data after it has been encrypted with a symmetric key. By using this procedure, even when the symmetric key is compromised, the data will still be protected. By adopting hybrid cryptography, cloud storage providers may assure that their customers' data is protected from unwanted access, theft, and other security threats.

The system proposed outlines a method for securely storing files in the cloud through the utilization of a hybrid cryptography algorithm. This technology enables users to safely save data in online cloud storage since the files are stored in the cloud in encrypted form and only authorized users can access them. Before being uploaded to the cloud, the user's uploaded data will be encrypted and securely stored using a user-specific key.

User can upload a text file using the upload option. Then user's file will then be split into N separate portions. All these file sections will be encrypted with cryptographic techniques. Several types of encryptions will be utilized by each component. The encryption methods that will be utilized to safeguard these entire file components include AES, DES, and RSA. After being recreated and placed in the user's unique folder, the file was first decrypted. The same encryption techniques employed to secure these file segments will be employed again for their decryption. Once the components are reassembled, the decrypted file will be made available for the user to download.

As more and more private information is stored and shared online, secure file storage in the cloud is becoming more and more crucial. To increase the security of data storage, hybrid cryptography is a type of encryption that incorporates the advantages of both symmetric and asymmetric encryption. Symmetric encryption is quick and effective since it uses the same key for both encryption and decryption. The key, however, must be securely exchanged between the parties involved, which is a drawback. A pair of keys, a public key and a private key, are used for encryption and decryption in asymmetric encryption, on the other hand. This does away with the requirement for key sharing, but it takes longer and uses more resources than symmetric encryption.

In hybrid cryptography, the best aspects of both methods are combined. This technique encrypts the data using a symmetric encryption algorithm and the encryption key using an asymmetric encryption algorithm. Then, a second layer of security is added by storing the encrypted data and encrypted key on the cloud. The recipient's private key is used to first decrypt the encrypted key to retrieve the data, and the decrypted symmetric key is then used to decrypt the encrypted data.

1.2 Problem Definition

The security of sensitive data saved in the cloud is a developing problem as cloud storage usage increases. Data on the cloud has always been secured using traditional cryptographic methods, however these techniques are susceptible to hacking and brute force assaults. This issue has a solution in hybrid cryptography, which blends symmetric and asymmetric encryption.

Using hybrid cryptography, the problem statement for secure cloud file storage calls for the creation of a system that maintains data availability, confidentiality, and integrity while allowing authorized users to access the data. For strong defense against multiple sorts of assaults, this system should combine symmetric and asymmetric encryption. To handle the encryption and decryption process, the system should also offer a safe and effective key management strategy. This system's objective is to offer people and businesses a safe and dependable way to store files in the cloud so that they may safeguard their private information.

To establish a file storage system that ensures encryption and security, facilitating secure file transfer among users located remotely. To improve the security of file stored on cloud storage using AES, DES, RSA algorithms. To optimize the speed and efficiency of system by splitting the data in different chunks and storing those parts in different servers on cloud. To implement a robust data storage and retrieval system in the cloud, even in cases where the data owner lacks control, to ensure stringent security measures are in place.

The difficulty lies in developing and putting into practice a hybrid cryptography-based system that can offer efficient and safe file storage on cloud systems. Only authorized users should be able to view the files, and the system should ensure that the data is kept private and protected from unauthorized access, modification, or theft.

In simple words our problem statement here is depending on the file's length, divide the uploaded file into n pieces. Create a unique symmetric key K at random for each file that will be stored. Use the key K to symmetrically encrypt the file and then produce a public key and a private key pair of asymmetric keys then use asymmetric encryption to encrypt the symmetric key K using the recipient's public key. Securely keep the encrypted symmetric key and the encrypted file. Get the encrypted symmetric key and the encrypted file. Now, using the recipient's private key, decrypt the encrypted symmetric key. To decrypt the file, use the decrypted symmetric key. After decrypting, join all the files.

CHAPTER 2

LITERATURE SURVEY

"A Hybrid Cryptography-based Secure File Storage System for Cloud Computing" by K. V. Ramachandran, Naveen Kumar, and R. Sriramakavacham. This research suggests a hybrid cryptography-based strategy for protecting cloud file storage. To guarantee the secrecy, integrity, and validity of the stored files, the authors use symmetric and asymmetric encryption.

Ankit Gupta and Dheerendra Singh's "Hybrid Cryptography based Secure File Storage on Cloud." This research presents a safe file storage system for the cloud utilizing hybrid cryptography. The authors use a combination of RSA and AES encryption to secure data confidentiality and integrity. To ensure safe access to the stored files, the system also has key management and access control components.

"A Hybrid Cryptography-based Approach for Secure File Storage in Cloud Computing" by S. Senthil Kumaran and S. Santhosh K. This research suggests a hybrid cryptography-based strategy for protecting cloud file storage. To guarantee the confidentiality and integrity of the saved files, the authors combine AES and RSA encryption. The system also contains a key management mechanism for safe access control.

Hybrid Cryptography for Secure File Storage on the Cloud by K. In addition to P. N. Shriram. This research suggests a hybrid cryptography-based strategy for protecting cloud file storage. To protect the privacy and integrity of the saved files, the authors combine RSA and Blowfish encryption. The system also contains a key management mechanism for safe access control.

"Secure File Storage on Cloud using Hybrid Cryptography and Attribute-based Encryption" by R. M. and Anitha. Hemalatha. This research presents a secure data storage system for the clouds using hybrid encryption and attribute-based encryption. For data security and integrity, the authors combine AES and RSA encryption. For access control, they use attribute-based encryption. In order to distribute keys securely, the system also features a key management mechanism.

Manpreet Kaur and Hardeep Singh examine various methods for protecting information storage on the cloud using hybrid cryptography in their article, "Secure file storage on cloud using hybrid cryptography: a review." They explain the merits and disadvantages of alternative approaches, such as RSA with AES, ElGamal with AES, and RSA with Camellia, and present a comparison of their security properties.

Literature Survey

In a study conducted by Both S. Sivasankari and S. Sathish, the authors provide a comprehensive survey on the utilization of hybrid cryptography for secure file storage in the cloud. The research examines recent advancements in this field, shedding light on the current state of the art in cloud-based file security. They examine different encryption schemes, such as symmetric and asymmetric encryption, and hybrid approaches that combine the two. They also talk about potential future research directions and difficulties in putting such systems into practice.

According to J. In "Hybrid Cryptography for Secure File Storage on Cloud: A Survey," The authors, R. Santhi and V. N. Sumathy, evaluate a number of hybrid cryptography systems that have been suggested for safe cloud file storage. They assess these systems' effectiveness and security as well as their applicability for various kinds of data and applications. They also talk about possible directions for this research's advancement.

Secure File Storage on Cloud using Hybrid Cryptography: A Survey" by R. Ramya and R. Kavitha. This study presents a comprehensive evaluation of several hybrid cryptography algorithms used for safe information storage on the cloud. It examines the advantages and limits of each technique and also discusses the problems and future research prospects in this subject.

S. Srinivasan and K. Sathish Kumar's "Hybrid Cryptography based Secure File Storage in Cloud: A Review." The secure file storage in the cloud using hybrid cryptography is the main topic of this survey report. It compares various existing methods and assesses the advantages and disadvantages of different hybrid cryptography techniques.

By M. V. Bhatkar and S. K. Gupta, "A Survey on Secure File Storage on Cloud Using Hybrid Cryptography." This study gives a survey on hybrid cryptography-enabled safe file storage in the cloud. It addresses the benefits and drawbacks of different hybrid cryptography-based techniques, including AES-RSA, AES-ECIES, and RSA-ECIES. The report also identifies current research gaps and suggested future lines of inquiry.

"A Review of Secure File Storage on Cloud using Hybrid Cryptography" by N. G. Patel and J. M. Patel. This survey study presents an overview of safe file storage on the cloud using hybrid cryptography. It examines the currently used methods—including AES-RSA, AES-ECIES, and RSA-ECIES—and assesses how well they perform in terms of security, effectiveness, and scalability. The report also discusses the challenges and potential research directions in this field.

P. S. Verma and P. R. Dubey's "Hybrid Cryptography based Secure File Storage on Cloud: A Systematic Review." This paper presents a systematic review of hybrid cryptography-based secure file storage on the cloud. It investigates the existing approaches, such as AES-RSA, AES-ECIES, and RSA-ECIES, and their applicability for cloud-based file storage. The limitations and future research directions in this area are also mentioned in the paper.

Literature Survey

"Hybrid Cryptography Based File Storage Security in Cloud Computing" by Shangquan Wang, Xuelian Lin, and Shengyu He (2020): This study examines various hybrid cryptography techniques that can be applied to cloud-based secure file storage. The authors explain the elements that should be considered when choosing an appropriate scheme for a particular application, comparing the advantages and disadvantages of these schemes.

Bhupendra Singh, Ravi Tomar, and Manoj Misra's 2018 paper, "A Survey of Hybrid Cryptography Techniques for Cloud Computing," outlines the following: This paper offers a thorough analysis of hybrid cryptography methods that can be applied to cloud-based secure file storage. The authors go over the benefits and drawbacks of various hybrid cryptography systems and offer suggestions for choosing the best one based on particular needs.

"Secure File Storage on Cloud using Hybrid Cryptography: A Survey" by Gaurav Kumar, Kuldip Singh, and R. K. Jha (2017): In this study, cutting-edge hybrid cryptography methods for safe file storage in the cloud are reviewed. The authors assess the various schemes based on aspects such as security, efficiency, and usability, and make advice for picking an acceptable scheme depending on individual requirements.

Ajay Kumar and S. S. Tyagi's "Hybrid Cryptography for Secure Data Storage in Cloud Computing: A Survey" from 2016: This study examines the various hybrid cryptography methods that can be applied to cloud data storage security. The authors assess the various schemes based on aspects such as security, efficiency, and scalability, and make recommendations for picking an acceptable scheme depending on individual requirements.

"A Survey on Secure File Storage on Cloud Using Hybrid Cryptography," by J. V. Bhattar and S.K. Sharma Gupta. This paper provides an overview of hybrid cryptography-enabled secure cloud file storage. It covers the advantages and disadvantages of various hybrid cryptography-based methods, such as AES-RSA, AES-ECIES, and RSA-ECIES. The report also points up existing research gaps and suggests potential directions for further study.

The article "Secure Cloud Storage using Hybrid Cryptography and Access Control" was written by J. S. Meena et al. In this paper, a hybrid access control and encryption system for secure cloud storage is proposed. The system incorporates access control methods to guarantee that only authorized users may access the files and uses a combination of symmetric and asymmetric encryption to protect the data.

S. S. Kumar et al.'s "Enhancing Cloud Security Using Hybrid Cryptography" This work suggests a hybrid cryptography-based method for boosting cloud computing security. The system incorporates access control methods to guarantee that only authorized users may access the files and uses a combination of symmetric and asymmetric encryption to protect the data.

N. R. Patel et al., "Secure Data Storage in Cloud Computing using Hybrid Cryptography" In this paper, a hybrid cryptographic architecture for safe cloud data storage is proposed. The system incorporates a key management method to ensure the security of the keys and combines symmetric and asymmetric encryption to safeguard the data.

According to V. Dhawan and colleagues, "A Secure and Efficient Cloud Storage System using Hybrid Cryptography and Data Fragmentation" In this research, a hybrid cryptography and data fragmentation-based cloud storage system is proposed. The system separates the files into fragments that are dispersed across various cloud servers and encrypts them using a combination of symmetric and asymmetric methods. The system is effective and efficient, according to the findings of the experiments the authors conducted to assess the security and performance of the system.

R. Sharma et al.'s "A Hybrid Cryptography Based Secure Cloud Storage System with Key Management" In order to increase security, this study suggests a hybrid cryptography-based secure cloud storage solution. The system incorporates key management procedures to ensure that the keys are safely maintained and disseminated, as well as a combination of symmetric and asymmetric encryption to safeguard the files. The system is effective and efficient, according to the findings of the trials the authors conducted to assess the system's performance security.

The article "Secure Data Storage in Cloud Computing using Hybrid Cryptography" was written by S. K. Samanta ray et al. The authors of this work suggest a hybrid cryptography-based secure file storage system that encrypts and stores data on the cloud using a combination of the AES and RSA algorithms. HMAC is also used by the system to provide message integrity and authentication. The system is secure and effective, according to the findings of the trials the authors carried out to assess these factors.

The article "A Novel Approach for Secure Data Storage in Cloud Computing Using Hybrid Cryptography" was written by M. A. Ali et al. To protect the data, this research suggests a novel hybrid cryptography-based secure file storage system that combines symmetric and asymmetric encryption. A hybrid key management strategy is also used by the system to increase data protection. The system is effective and secure, according to the trials the authors carried out to assess its performance and security.

CHAPTER – 3

SYSTEM SPECIFICATIONS

3.1 SOFTWARE REQUIREMENTS

PHP

A popular scripting language used primarily for web development is called PHP, which stands for Hypertext Preprocessor. Because of how simple it is to understand and use, both novice and seasoned developers favor it.The straightforward syntax of PHP is one of the reasons it is regarded as being simple. Its syntax is similar to C, so it makes use of terms like loops, conditionals, and functions. Because of this, it is simple to read and comprehend, especially for programmers with previous exposure to other languages.

The fact that PHP integrates with HTML without any hiccups is another factor that adds to its user-friendliness. By directly integrating PHP code into HTML files, developers can combine dynamic server-side code with static client-side content. The creation of dynamic web pages and database interaction are both made simple by this integration.

Additionally, PHP includes a sizable number of in-built libraries and functions that simplify typical web development tasks. There is probably a PHP function or library that can help you, whether you need to work with strings, manage file uploads, or connect to a database. Developers can save time and effort by using this comprehensive set of tools rather than having to continually come up with new solutions for basic tasks.

Furthermore, PHP has a sizable and helpful community as well as excellent documentation. Comprehensive details on the features, functions, and best practices of the language are available in the official PHP documentation. The PHP community, which is made up of developers from all over the world, is renowned for its willingness to lend a hand and impart knowledge. There are many online guides, tutorials, and discussion boards where you can ask questions and receive guidance.

PHP is a powerful language that can handle complex web applications despite its simplicity of use. Developers can create modular, reusable code because it supports object-oriented programming. Additionally, PHP offers comprehensive support for a wide range of databases, including MySQL, PostgreSQL, and MongoDB, allowing developers to create robust and data-driven applications.

Mcrypt

For encryption and decryption in earlier versions of PHP, Mcrypt, a cryptographic library, was frequently used. It gave programmers access to a set of functions that they could use to encrypt their data using different algorithms. It's important to keep in mind that mcrypt is considered deprecated and is not advised for new projects as of my knowledge cutoff in September 2021. An overview of mcrypt's function and goal is given in the paragraphs that follow.

At its core, mcrypt was created to secure data by using encryption algorithms to convert it into an unreadable format known as ciphertext. The data is encrypted through the application of a secret key during this procedure. The encrypted data could only be unlocked and converted back to plaintext using the same key and the corresponding decryption algorithm.

The symmetric encryption algorithms AES, DES, and Blowfish were all supported by Mcrypt. The chosen key was then used to carry out a series of mathematical operations on each fixed-size block of data, which was typically 8 or 16 bytes in size, according to these algorithms. The data was securely transformed by applying these operations time and time again.

The data to be encrypted or decrypted, the encryption algorithm to be used, the key for the operation, and some additional parameters, such as an initialization vector (IV), were all required when using mcrypt. The IV was a random value used to make sure that even if the same plaintext was encrypted more than once with the same key, the final ciphertext would be different.

Openssl

A software library called OpenSSL aids in data security and encryption. In order to communicate securely over networks and safeguard sensitive data from unauthorized access, it offers a set of tools and features.Your data is secure thanks to OpenSSL's use of a digital lockbox. It employs an encryption technique, which converts your data into a code that can only be deciphered by authorized parties. When the information reaches its intended recipient, OpenSSL aids in unlocking and breaking the code, restoring the information's legibility.

OpenSSL provides a number of cryptographic operations, including the creation of secure keys, data encryption and decryption, and digital signature creation. With the help of these features, you can confirm the sender's legitimacy and maintain the integrity of your data while also keeping it private.For secure communication, many applications and protocols rely on OpenSSL. For instance, websites use OpenSSL to create secure connections (HTTPS) that guarantee the confidentiality of your sensitive information, such as passwords or credit card numbers, when you interact with them.

AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman) are just two of the many encryption algorithms that OpenSSL supports. An additional layer of security is added by these algorithms, which control how encryption and decryption are performed.

In numerous programs and systems all over the world, OpenSSL is widely used and adopted. It is an essential part of numerous web servers, email servers, VPNs, and other network-related software. Its feature set, flexibility, and dependability all contribute to its popularity.

MySQL

The open-source relational database management system known as MySQL is frequently used to store, manage, and retrieve structured data. It provides a quick and efficient way to set up enormous amounts of data in a structured manner. Two of MySQL's main benefits are that it is simple and easy to use. Creating, editing, and querying databases is made simple by this method. Thanks to its relatively simple syntax, even beginners can understand the basics and start using databases.

Several features that MySQL offers improve its usability. It provides a graphical user interface (GUI) that enables visual database interaction through programs like phpMyAdmin and MySQL Workbench. Simple tasks like creating tables, defining relationships between them, and executing queries are made simple by these tools.

Protections put in place to prevent unauthorized access, misuse, or breaches of data stored in a relational database management system (RDBMS) like MySQL. It is essential to maintain the integrity of your data and ensure the security of your SQL database in order to safeguard sensitive information.

Additional features that make MySQL simple to use include its comprehensive documentation and community support. Using the plethora of online tutorials, resources, and discussion boards, users can find answers to their questions, solve problems, and learn from the experiences of others. The active community that surrounds MySQL provides users of all experience levels with a wealth of knowledge and assistance.

As a result of MySQL's high scalability, managing applications of all sizes is also a breeze. Due to its effectiveness, it can manage databases with millions or even billions of rows, making it suitable for a range of projects and industries.

Xampp

It is possible to host dynamic websites and web applications on your computer with the help of the widely used open-source software package known as XAMPP. Cross-Platform compatibility, the Apache web server, the MySQL database management system, the PHP scripting language, and the Perl scripting language are all referred to collectively as XAMPP.

Developers can use XAMPP regardless of their preferred platform because it is built to operate flawlessly on a variety of operating systems, including Windows, macOS, Linux, and Solaris. It includes the dependable and strong web server Apache, which supports SSL/TLS encryption and virtual hosting functions. Additionally, the package includes MySQL, which enables effective database management, a crucial requirement for data archiving and retrieval on dynamic websites. Perl offers additional scripting capabilities for tasks like text processing and system administration, and PHP, another essential component of XAMPP, is a server-side scripting language used to create interactive and dynamic web content.

XAMPP streamlines installation and offers a ready-to-use local web server environment by combining Apache, MySQL, PHP, and Perl into a single installation package. As a result, there is no longer a need to install and configure every component individually, enabling developers to quickly set up a development environment for testing their web applications before releasing them to a live server.

AWS Cloud

Amazon offers a service known as AWS Cloud, or Amazon Web Services Cloud, which grants access to a diverse array of cloud computing services. These services enable individuals and businesses to utilize tools and resources over the internet, eliminating the need for physical infrastructure.

A noteworthy advantage of the AWS Cloud is its scalability, allowing users to easily adjust their computing resources to align with their requirements. This flexibility empowers businesses to swiftly adapt to changing consumer demands, resulting in improved efficiency and cost savings.

The AWS Cloud encompasses a broad spectrum of services, including processing power, storage options, networking solutions, databases, and more. Users can choose from various service models such as IaaS, PaaS, and SaaS to cater to their specific needs.

By leveraging the AWS Cloud, users can deploy applications, host websites, store and analyze vast amounts of data, implement robust security measures, and take advantage of cutting-edge technologies like machine learning and AI. The global presence of AWS data centers ensures reliability with minimal downtime, while management and monitoring tools simplify resource management, workflow automation, performance monitoring, and security and compliance enforcement.

AWS Cloud equips organizations with the adaptability, scalability, and dependability required to keep pace with the rapidly evolving digital landscape.

S3 Bucket

Data can be stored and retrieved with ease using Amazon Simple Storage Service (S3), a cloud storage service offered by Amazon Web Services (AWS). S3 buckets function as containers in the AWS cloud, much like file system folders. They provide excellent scalability, toughness, and security.

When you create an S3 bucket, you give it a distinctive name that becomes a part of its URL, making it reachable via the internet. S3 buckets have the capacity to store a sizable variety of items, from small files to sizable data sets. With their support for a hierarchical structure, you can group objects into folders and subfolders to organize them.

Strong access control is offered by S3 buckets, enabling you to define rules and permissions at the bucket or object level. Because of this, objects can only be read, written to, or deleted by authorized users. While lifecycle management helps automate transitions between storage classes and object expiration, versioning capabilities let you save and restore earlier versions of objects.

Using the AWS Management Console, command-line tools, SDKs, or APIs are just a few of the ways you can upload and download data to and from S3 buckets. In order to facilitate auditing and tracking of bucket activity, S3 also provides logging and monitoring features, such as server access logging and event notifications.

S3 supports replication within a single region as well as across multiple regions to improve data availability and durability. By maintaining multiple copies of your data, this replication feature aids in disaster recovery. You can use S3 as a data source for analytics or to incorporate it into workflows because it ties in seamlessly with other AWS services.

HTML

Web pages are made and their content is organized using the fundamental coding language known as HTML (Hypertext Markup Language). It uses tags and attributes to specify the organization and display of information on a webpage. For those new to web development, HTML is frequently regarded as an approachable language.

Tags, which are denoted by angle brackets (), are the foundation of HTML and composed of opening and closing pairs. An element's beginning is indicated by opening tags, and its ending by closing tags. The tag, for instance, is opened with and closed with to represent a heading.

By using different tags, HTML enables hierarchical content organization. Typically, an opening tag and tags come first in an HTML document. While the section holds the visible content, it typically contains meta-data such as the webpage title and character encoding.

Different tags are used to specify headings, paragraphs, lists, images, links, tables, forms, and more within the section. As an illustration, the tags and produce unordered and ordered lists, respectively, while the tag creates paragraphs. Using the tag, links can be made and images can be added.

An element's behavior or appearance can also be changed using attributes in HTML. The opening tag is supplemented with attributes, which are name-value pairs. For instance, the href attribute in the tag specifies the URL that the link points to.

The visual presentation of web pages can also be improved by combining HTML and CSS (Cascading Style Sheets). Colors, fonts, layout, and other website features can all be modified using CSS. Using the tag, CSS can be inserted into the HTML document or linked externally.

An HTML document can be viewed by simply opening it in a web browser, which decodes the HTML code and renders the webpage appropriately. A rendering engine is used by web browsers to read the HTML structure and apply the specified CSS styles, resulting in a user-friendly presentation of the content.

CSS

It enables web designers to separate a website's content from its visual aesthetic, making maintenance and updating simpler.

More intricate and imaginative layouts are now possible thanks to the use of CSS in web design. The color, font, size, and positioning of elements on a page can all be altered by designers using CSS. Older HTML-only designs could not achieve this level of control. CSS enables responsive design, which enables websites to adjust to various screen sizes and gadgets. This is essential in the mobile-first world of today, where users access websites using a variety of devices.

CSS has facilitated accessibility by giving users with disabilities options like altering font size or color contrast.

Bootstrap

Accurate parameter estimation and uncertainty assessment can be difficult in the real world of statistics and data analysis, especially when there are few data or complicated models. However, a potent method known as the bootstrap method exists and addresses these issues. In-depth discussion of the bootstrap method's theory, uses, and benefits is provided in this essay.

Understanding the Bootstrap Method involves resampling from the available data to estimate the sampling distribution of a statistic. This statistical technique, introduced by Efron in 1979, is non-parametric and useful for calculating standard errors and creating confidence intervals for parameters. The Bootstrap Method recognizes the informative nature of observed data regarding the underlying population distribution.

The operational principle of the Bootstrap Method relies on resampling the original data set multiple times, typically using random sampling with replacement. Each resample has the same size as the original data set but may contain duplicate observations or exclude some. The desired statistic is computed for each resample, generating a statistical distribution known as the bootstrap distribution.

CHAPTER – 4

SYSTEM DESIGN

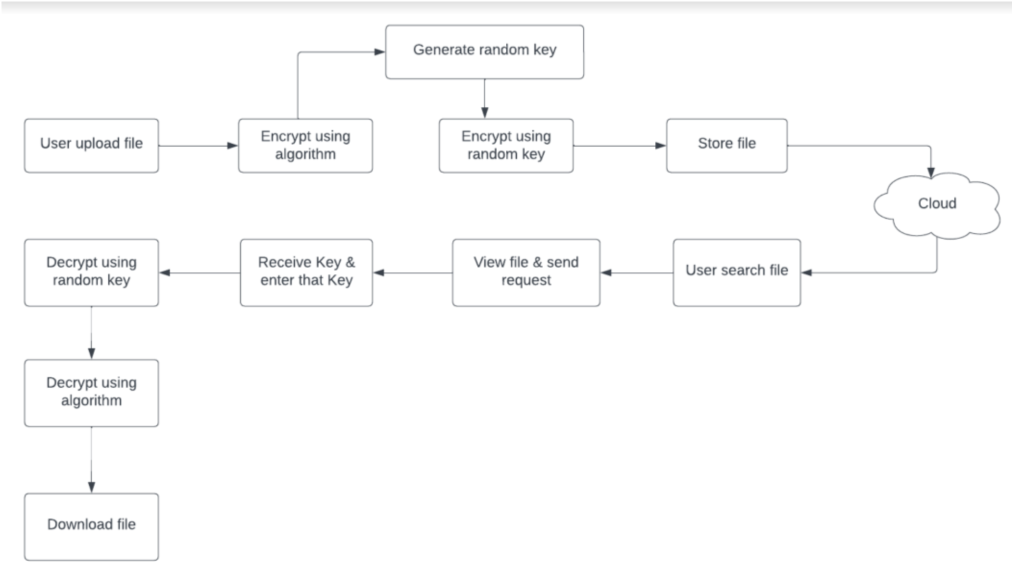


Fig 4.1 System Architecture

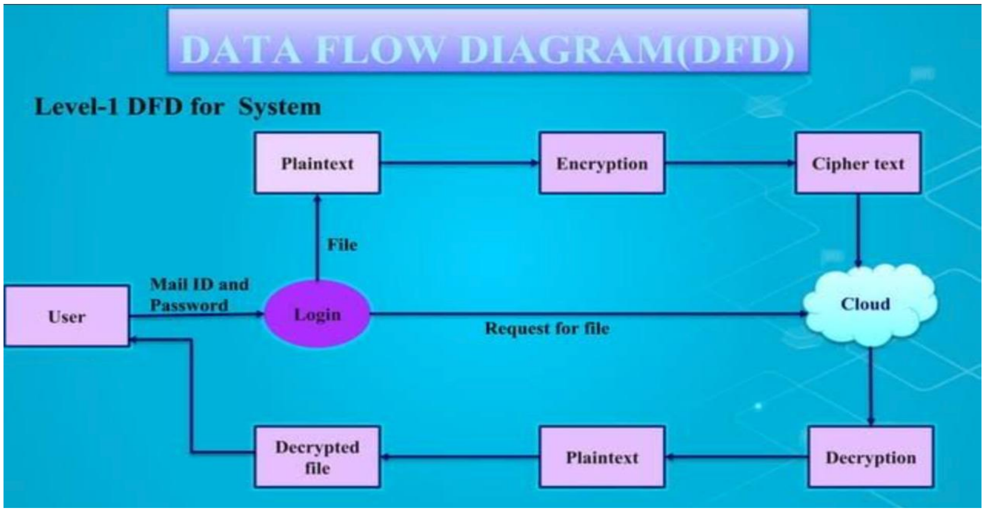


Fig 4.2 Level-1 DFD Diagram

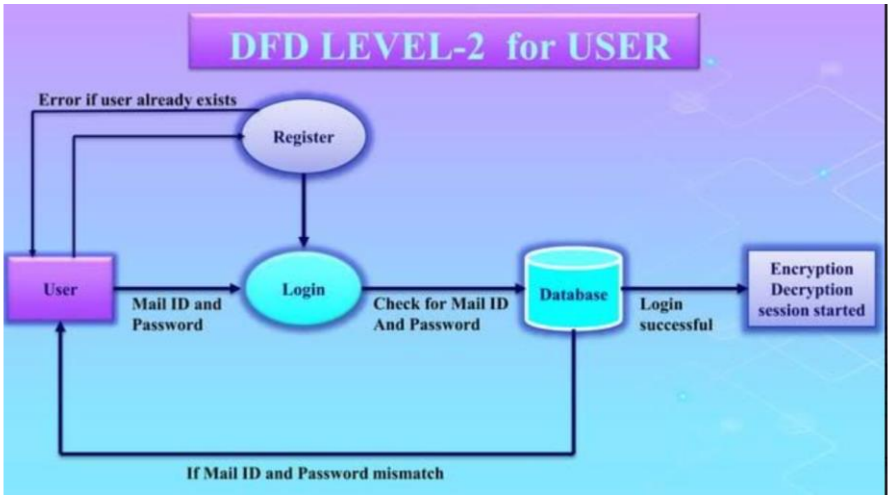

DFD LEVEL-2 for USER
Error if user already exists
Register
User
Mail ID and Password
Login
Check for Mail ID And Password
Database
Login successful
Encryption Decryption session started
If Mail ID and Password mismatch

Fig 4.3 Level-2 DFD Diagram

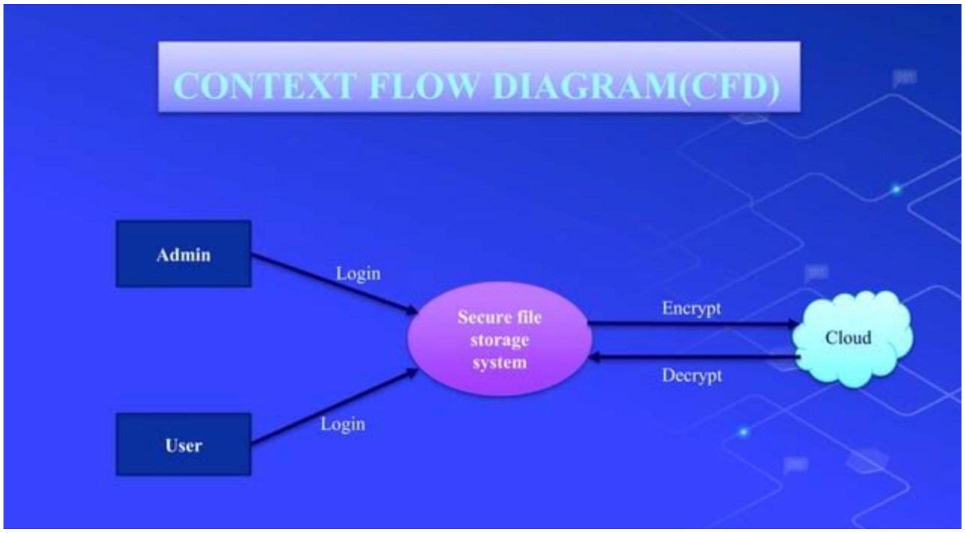


Fig 4.4 Context Flow Diagram

CHAPTER – 5

SYSTEM IMPLEMENTATION

5.1 Implementation Steps

To achieve the intended goal, a systematic methodology is recommended, which involves the following steps:

1. File Loading: The initial step involves uploading the desired file onto the server, where it will be securely stored and processed.

2. File Division: Upon successful uploading, the uploaded file is divided into multiple parts. This division is crucial for ensuring efficient encryption and allows for enhanced security and flexibility in managing the data.

3. Encryption: Each individual part of the file is subjected to encryption using a selected algorithm. To further enhance security, a unique encryption algorithm is chosen for each part, following a round-robin pattern. This approach adds an extra layer of protection, making it more challenging for potential attackers to decipher the encrypted data.

4. Key Protection: To ensure the confidentiality and integrity of the encryption keys, they are secured using a different algorithm. This additional layer of protection ensures that even if the encrypted data or keys are compromised, the overall security of the system remains intact. The key used to safeguard the encryption keys is then provided to the user as a public key. This enables authorized users to access and decrypt the encrypted file parts using the corresponding private key, while ensuring that unauthorized individuals cannot decipher the data.

By following this methodology, the data in the cloud can be effectively encrypted and decrypted using hybrid cryptography, maximizing security and providing a robust framework for protecting sensitive information.

To restore the encrypted file and retrieve the original data, the following steps should be followed:

1. Key Loading: Firstly, the key used for encryption needs to be loaded onto the server. This key is essential for decrypting the encrypted file parts and retrieving the original data.

2. Key Decryption: The encrypted keys of the algorithms used for encryption are decrypted using the loaded key. By decrypting the keys, the server gains access to the specific algorithms required for decryption.

3. File Decryption: Each of the N parts of the file, which were initially encrypted using the corresponding algorithms, are now decrypted using the same algorithms. This ensures that the data is transformed back into its original, readable form.

4. File Reconstruction: Once all the encrypted file parts have been successfully decrypted, they are combined and merged together to reconstruct the original file. The reconstructed file, containing the retrieved data, is then made available for download by the user.

By following these steps, the encrypted file can be effectively restored, ensuring that the user can retrieve and access the original data from the cloud server.

5.2 Model

The suggested model is designed to effectively address the security requirements of a cloud data center. The use of Blowfish for encrypting file slices ensures minimal processing time while achieving high throughput for both encryption and decryption, surpassing other symmetric algorithms. Additionally, the concept of splitting and merging files enhances the overall data security principle. By implementing the hybrid approach within a cloud environment, the remote server attains a heightened level of security, leading to increased trust among cloud users. This approach effectively addresses the challenges of data security and privacy protection by successfully achieving the fundamental goal of segregating sensitive data and implementing robust access control measures.

The process of cryptography involves transforming original data into an unintelligible format. It can be categorized into symmetric key cryptography and public key cryptography. These techniques utilize keys to convert data into an unreadable form, ensuring that only authorized individuals can access the data stored on cloud servers.

The resulting ciphertext is visible to everyone, but its meaning remains obscured without the proper decryption key.

By utilizing cloud storage, there is no need to establish and maintain costly and intricate on-site infrastructure for data storage and retrieval. This becomes particularly significant during emergency situations. The system's assortment of storage servers enables the provision of a reliable online backup solution. However, concerns about privacy arise when data is stored in the cloud and entrusted to a third-party entity.

Within this cloud environment, certain standard encryption algorithms are employed to ensure data privacy. However, these algorithms impose significant limitations on the storage system's capabilities, as they can only be applied to a limited range of tasks. The main objective of this project is to construct a secure repository that can cater to diverse purposes. However, accomplishing this task becomes challenging in the absence of centralized control over the storage system.

The integration of AES and proxy re-encryption facilitates secure data transmission, ensuring the confidentiality and integrity of the information. In the initial phase, data is encrypted using AES by the data owner, establishing a strong layer of protection. Ensuring the durability of stored data is of utmost importance, and numerous approaches for archiving information on remote servers have been suggested. One technique involves replicating messages, allowing each storage server to possess a copy of the message, thereby enhancing data reliability. Distributed storage systems are particularly suitable for implementing a decentralized erasure code, further enhancing the overall storage system's efficiency and resilience.

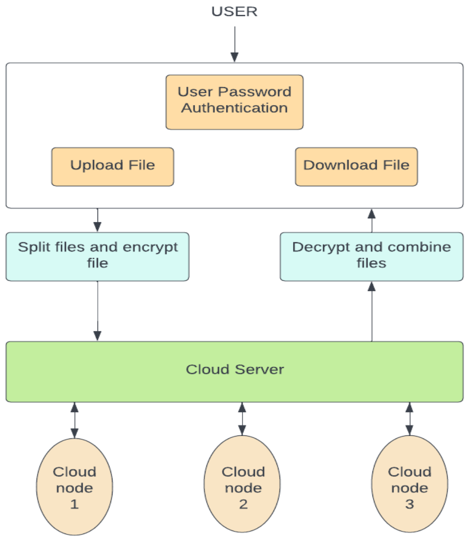

USER
User Password Authentication
Upload File
Download File
Split files and encrypt file
Decrypt and combine files
Cloud Server
Cloud node 1
Cloud node 2
Cloud node 3

Fig 5.1: control flow

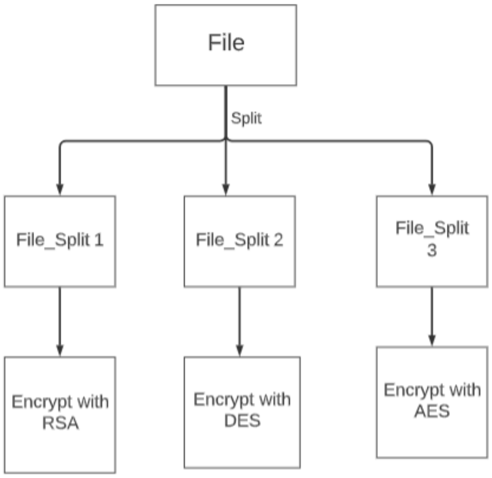


Fig 5.2: Splitting &Encrypting Files

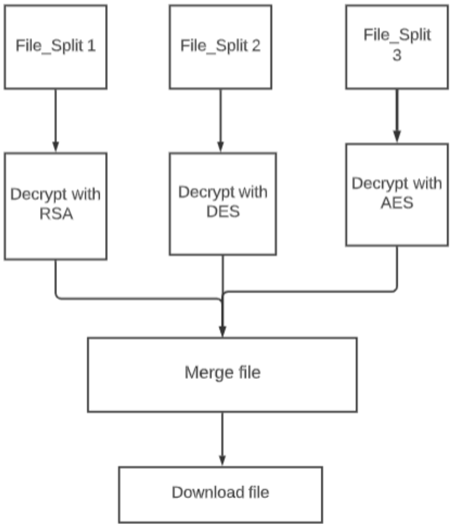


Fig 5.3: Decrypting and merging files

CHAPTER - 6

SYSTEM TESTING

Errors are the basis for the testing. Testing is a strategy used to look for every flaw or.a flaw in the work product.It offers a way to assess the value of parts, smaller groups, gatherings, and finished products. Consequently, it results in useful programming verify whether the framework satisfies the customer's requirements and wishes or not fail inappropriate. There are various test options available. Each type of test typically is required.

6.1 FUNCTIONAL TESTING

Practical testing shows deliberately that the capacity of companies and advanced needs, implementation paperwork and customer manuals can be accessed as determined. Realistic testing is concentrated on the following things: legal input: substantial data classes identified must be recognised. Invalid Input: eminent classes should be dismissed for invalid information. Capacities: capabilities identified must be developed. Return: differentiated usage rates must be established. Frameworks: Considerations or programs interacting should be summoned. The organization and preparing of minimalist tests focuses on the requirements, key limit.

6.2 SOFTWARE TESTING

Framework testing guarantees that the entire well-organize coding structure complies with requirements. To ensure both expected and unexpected results, a system is being tested.
The instance of frame testing is the framework blend test that is described in the agreement. that test frame is reliant on rivers and treatment descriptions, which emphasize pre-connected focus and mix of procedures.

6.3 WHITE BOX TESTING

White Box Test is an attempt where the item analyst knows or does nothing else with its inward operations, framework and language. That's why. It is used for testing areas that can not came from either a level of discovery.

6.4 BLACK BOX TESTING

This testing tries the item without studying the module's internal activities, design or language. Discovery evaluations, for instance the determination or reporting prerequisites, such as specific or essentials record, as most distinct kinds of tests, have to be made up from an impartial source archive. It is an attempt to handle the item being tested, because you cannot "see" in this as a discovery. The test provides information outlets as well as responds to the results without considering how the service works.

6.5 UNIT TESTING

Unit testing is typically conducted as an important aspect of the centralized product-lifecycle code and unit testing, despite the fact that coding and unit testing are not notable to be conducted as two special steps.

Test technique and strategy Field tests are conducted in specifics and helpful tests are written. Test destinations

- All field verses have to function legally.
- Distinguished link pages must be initiated.
- No delay must be allowed for the section screen, messages and responses.
- Make sure the parts are configured in the right way
- Sections of copy should not be allowed
- The user should be on the correct page for all the connections.

6.6 Testing of Authentication

Input	Output
Authenticated Key	The file can be decrypted.
Unauthorized Key	The file cannot be decrypted.

6.7 INTEGRATION TESTING

Programming integration testing involves gradually checking at least two co-ordinated programming components on a single stage to deliver deceptions caused by surrendering interfaces. The combination test involves monitoring that components or programming applications, such as sections in a item framework or–one phase up–organizational coding apps–can be combined without blundering. Test results: The above tests have been successfully passed. There have been no distortions.

6.8 ACCEPTANCE TESTING

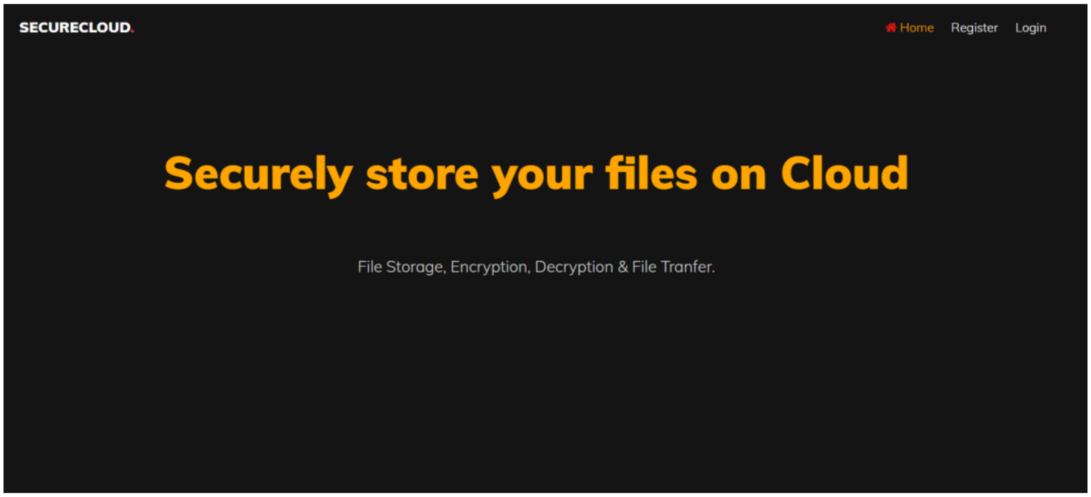
Testing of User Recognition is a key endeavor span and requires minimal investment from the end customer. The Framework also ensures that the valid test outcomes meet: all the above-mentioned experiments have been effectively passed. There have been no imperfections.

CHAPTER – 7

RESULTS AND ANALYSIS

It's important to note that implementing a secure file storage system involves various other considerations, such as access control, secure key management, and secure transmission of keys. Additionally, the choice of cryptographic algorithms and key sizes should follow industry best practices and standards.

When the user visits hits the website url in the internet browser. Home Page appears as the first page of the website . In home page user can see options to login and register.

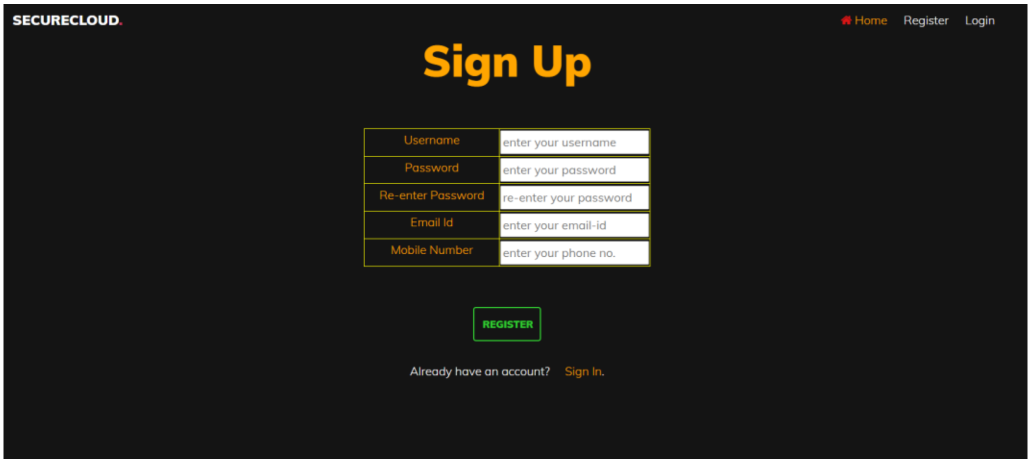


Securely store your files on Cloud

File Storage, Encryption, Decryption & File Tranfer.

Fig 7.1: Home Page

When user clicks on register button. It is typically used as a call-to-action to prompt users to sign up for an account by providing their personal information and creating login credentials. By clicking the "Register" button, users are usually redirected to a registration form where they can enter their details, such as name, email address, username, password, and any other required information.



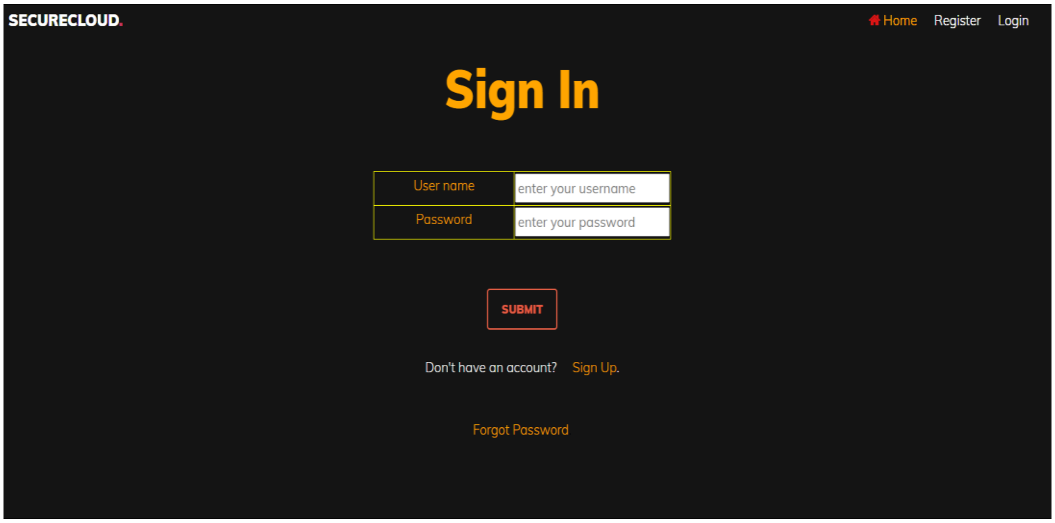
Sign Up

Username	enter your username
Password	enter your password
Re-enter Password	re-enter your password
Email Id	enter your email-id
Mobile Number	enter your phone no.

Already have an account? Sign In.

Fig 7.2: Register Page

Applications that require users to authenticate themselves to access their accounts or secure areas. The sign-in page typically prompts users to enter their login credentials, such as username or email and password, to verify identity and grant them access to their personalized content or features.



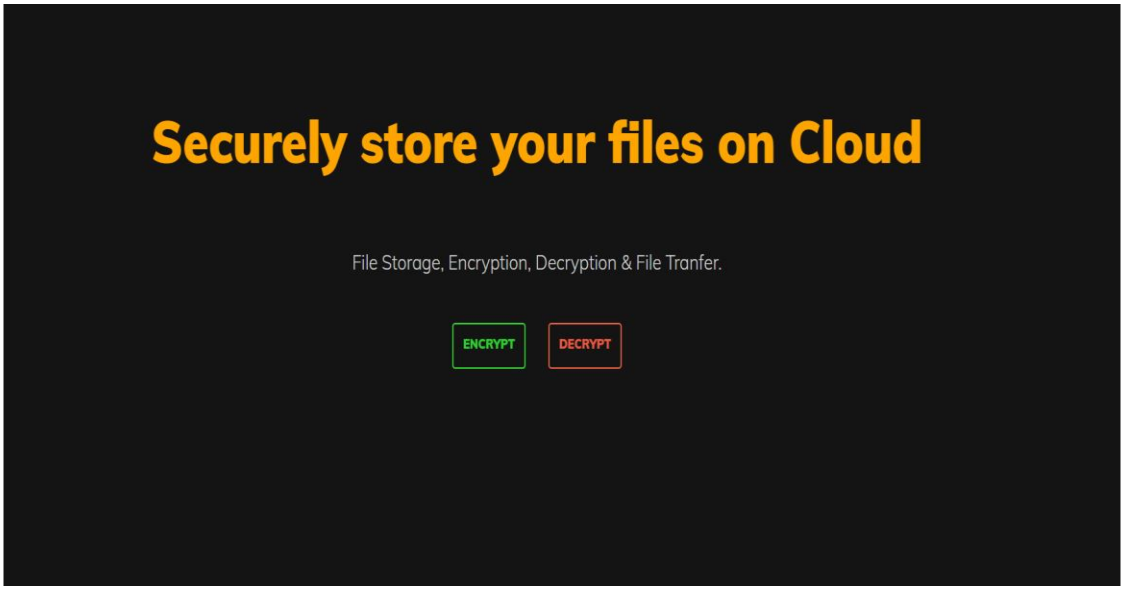
Sign In

User name	enter your username
Password	enter your password

Don't have an account? Sign Up.

Fig 7.3: Login Page

After a user successfully logs in, the landing page is typically the first page they see. The purpose of the home page is to provide a personalized and relevant experience for the logged-in user, offering easy access to key features. As you can see in Fig: 4.4 user can choose the options to encrypt or decrypt a file on his wish.

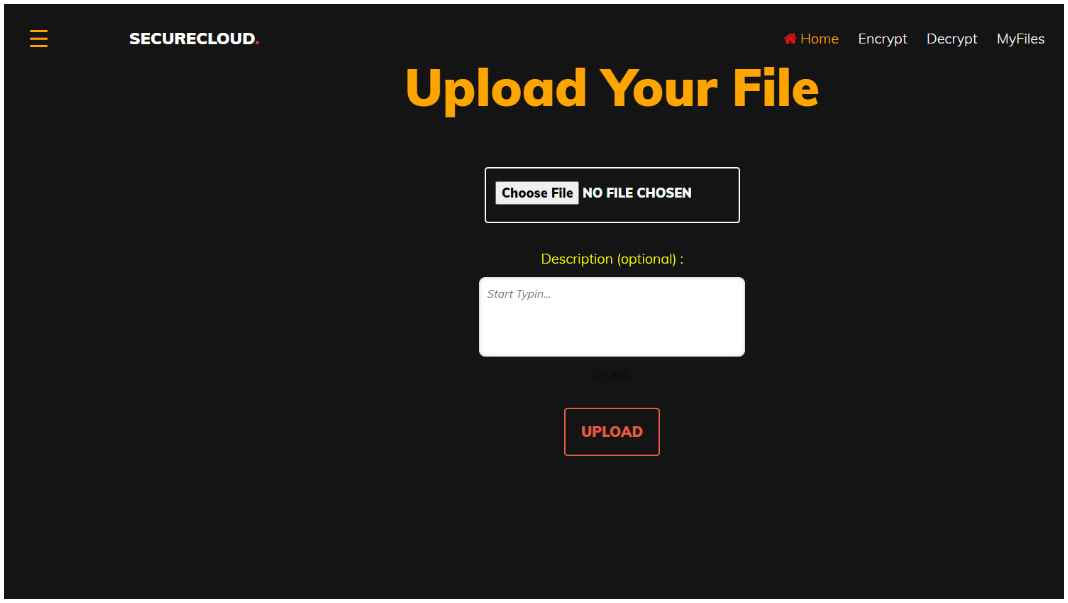


Securely store your files on Cloud

File Storage, Encryption, Decryption & File Tranfer.

Fig 7.4: Landing page after successful login

When the user wish to encrypt a file , they click on encrypt option from Fig:4.5 . By clicking on upload your file that allows users to upload a file and then divide or split it into smaller parts or sections. Description is a text filed box where user can write or mention about the details and notes about the particular file user in uploading



Upload Your File

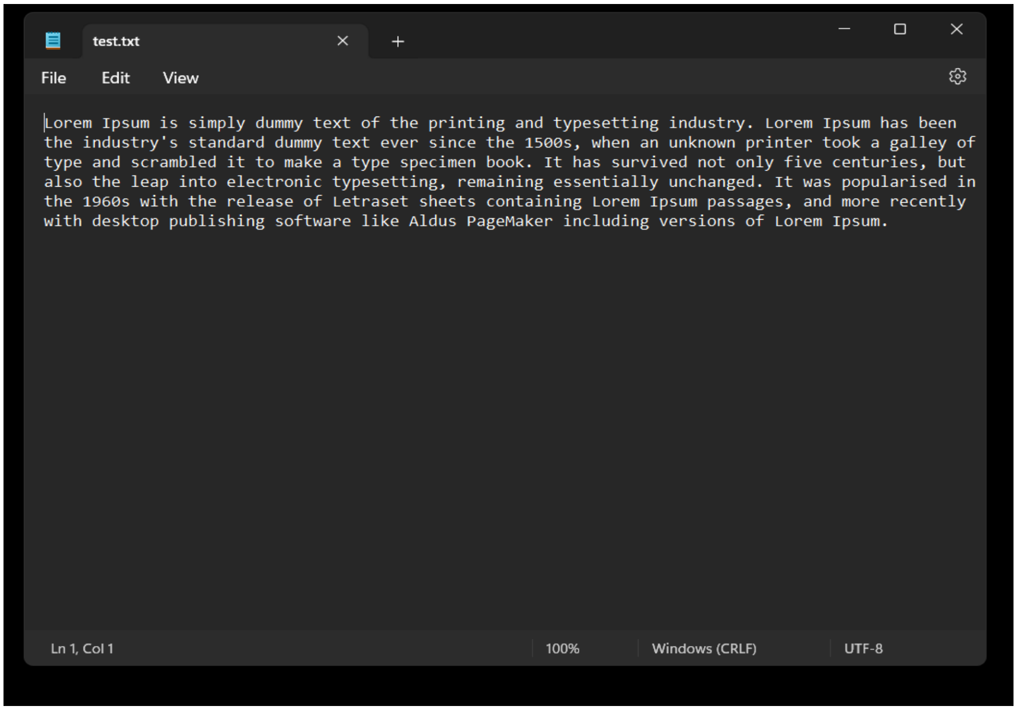
Choose File NO FILE CHOSEN

Description (optional) :

Start Typin...

0 / 300

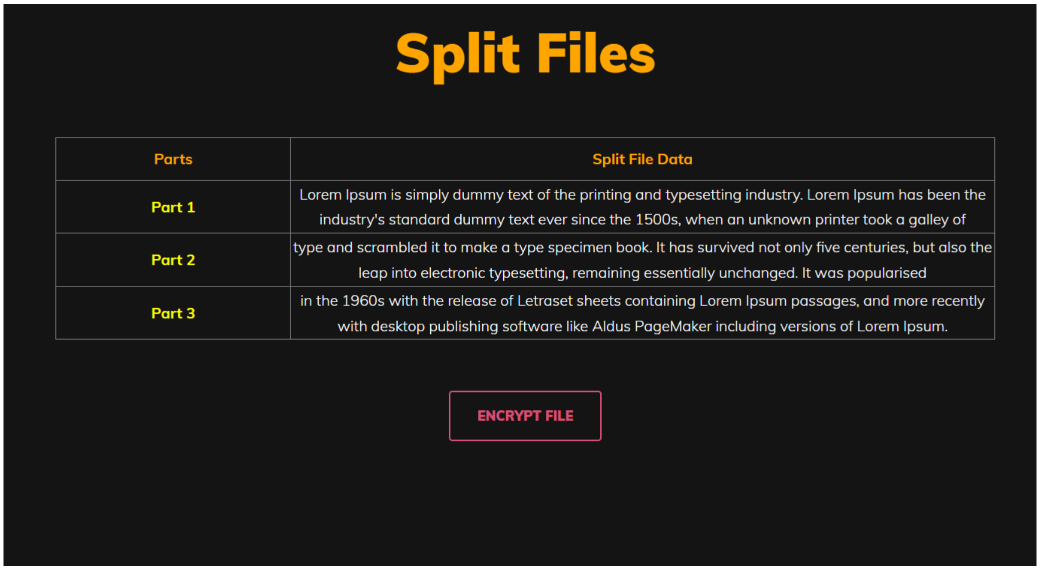
Fig 7.5: Upload file page



```
Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been
the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of
type and scrambled it to make a type specimen book. It has survived not only five centuries, but
also the leap into electronic typesetting, remaining essentially unchanged. It was popularised in
the 1960s with the release of Letraset sheets containing Lorem Ipsum passages, and more recently
with desktop publishing software like Aldus PageMaker including versions of Lorem Ipsum.
```

Fig 7.6: Uploaded file

The "Split File" feature often provides users with options to customize the splitting process. These options may include specifying the number of parts the file should be split into, defining the size of each part (e.g., in kilobytes or megabytes), or setting specific breakpoints within the file where the splitting should occur.

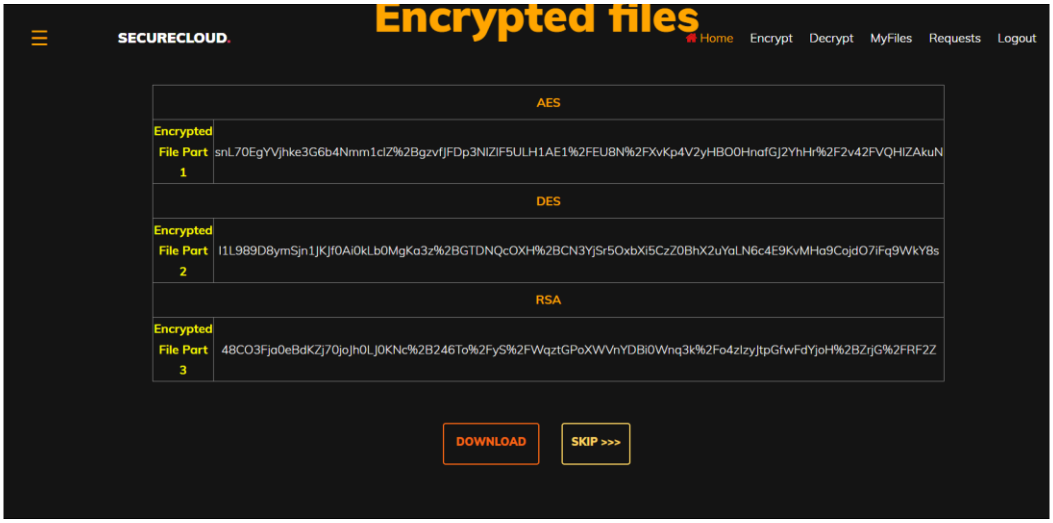


Split Files

Parts	Split File Data
Part 1	Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of
Part 2	type and scrambled it to make a type specimen book. It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged. It was popularised
Part 3	in the 1960s with the release of Letraset sheets containing Lorem Ipsum passages, and more recently with desktop publishing software like Aldus PageMaker including versions of Lorem Ipsum.

Fig 7.7: Split file before encrypting

Users may have the option to upload files directly to the encrypted files page. Upon upload, the files are encrypted using a cryptographic algorithm, ensuring the confidentiality and integrity of the data. The encryption process may be automatic or require the user to specify a passphrase or encryption key.

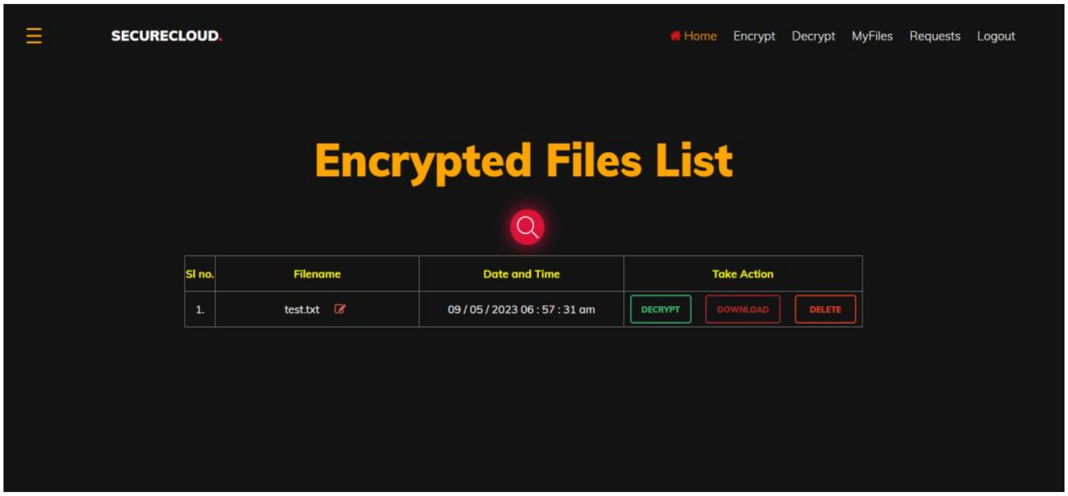


Encrypted files

AES	
Encrypted File Part 1	snL70EgYVjhke3G6b4Nmm1clZ%2BgzvfJFDp3NIZIF5ULH1AE1%2FEU8N%2FXvKp4V2yHBO0HnafGJ2YhHr%2F2v42FVQHIZAkuN
DES	
Encrypted File Part 2	I1L989D8ymSjn1JKJf0Ai0kLb0MgKa3z%2BGTDNQcOXH%2BCN3YjSr5OxbXi5CzZ0BhX2uYaLN6c4E9KvMHa9CojdO7iFq9WkY8s
RSA	
Encrypted File Part 3	48CO3Fja0eBdKZj70joJh0LJ0KNc%2B246To%2FyS%2FWqztGPoXWVnYDBi0Wnq3k%2Fo4zlzyJtpGfwFdYjoH%2BZrjG%2FRF2Z

Fig 7.8: Split files after encrypting

The page typically displays a list or grid view of the encrypted files associated with the user's account. Each file entry may include details such as file name, date of encryption. User can perform their desired action by clicking any of the Take Action .



Encrypted Files List

Sl no.	Filename	Date and Time	Take Action
1.	test.txt	09 / 05 / 2023 06 : 57 : 31 am	DECRYPT DOWNLOAD DELETE

Fig 7.9: All files hosted on server

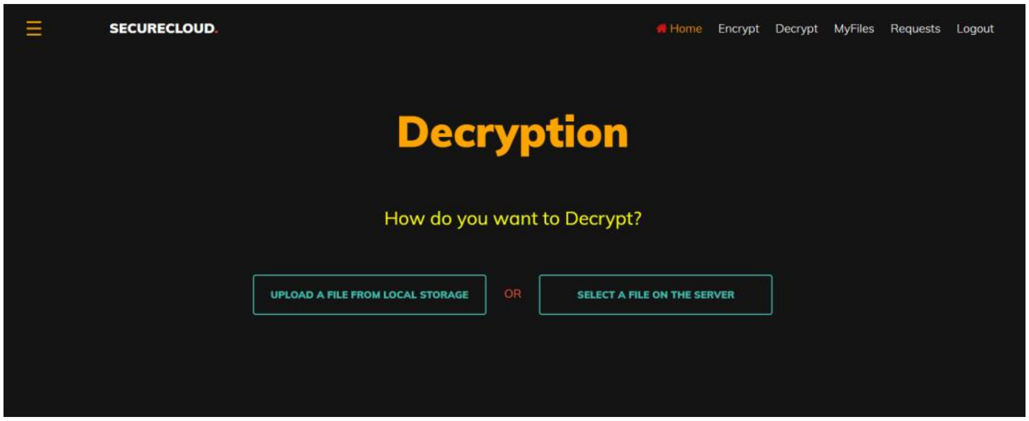
When it comes to uploading a file, there are two common scenarios: uploading a file from the local device and uploading a file from a server.

Uploading a File from the Local Device:

This scenario involves selecting a file from the user's local device, such as a computer or mobile device, and uploading it to a website or application

Uploading a File from a Server:

In some cases, users may have files stored on a remote server or cloud storage platform and want to upload them to a different server or application

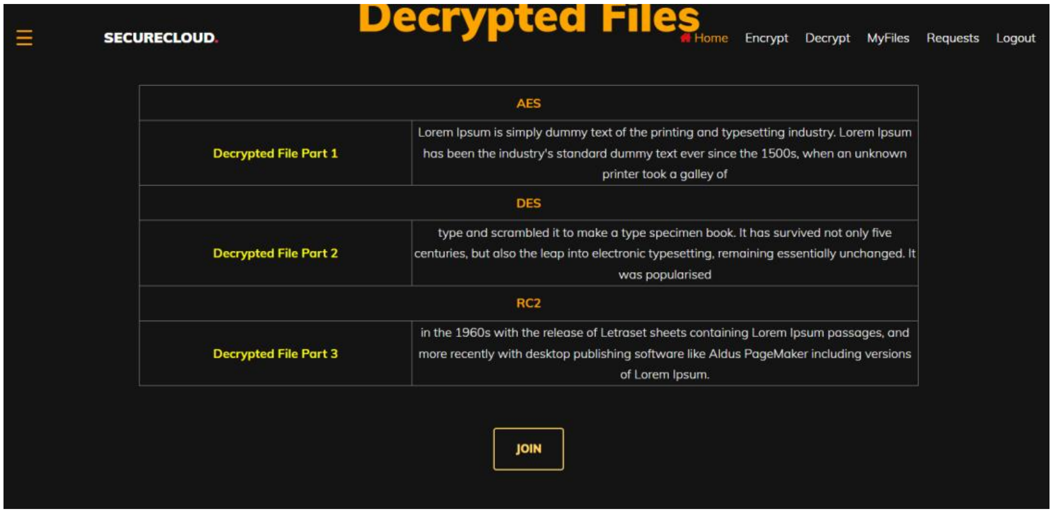


Decryption

How do you want to Decrypt?

Fig 7.10: Decryption page

Users have the ability to preview decrypted files directly within the decrypted files page in Fig: 4.11. This can include displaying the file content, generating file. The decryption process involves using the correct decryption key or passphrase to convert the encrypted data into its original form. Once decrypted, the files become accessible for download or further manipulation.

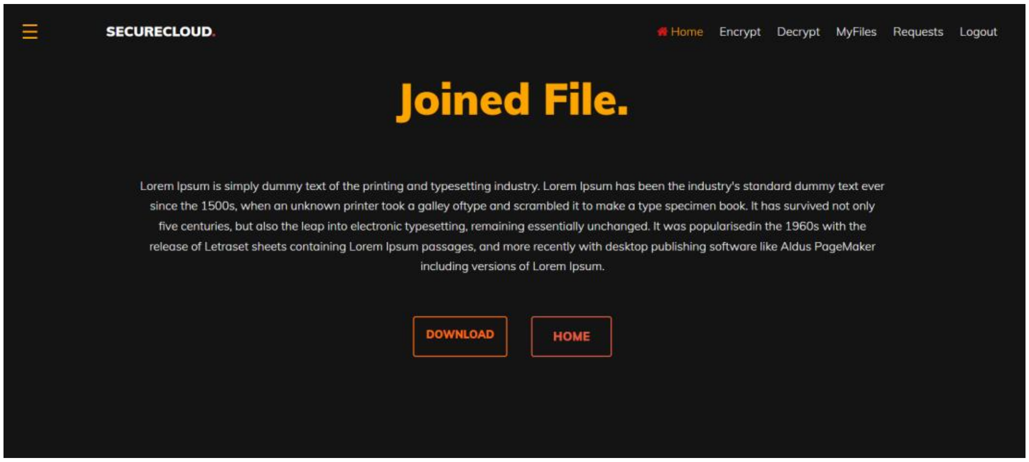


Decrypted Files

AES	
Decrypted File Part 1	Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of
DES	
Decrypted File Part 2	type and scrambled it to make a type specimen book. It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged. It was popularised
RC2	
Decrypted File Part 3	in the 1960s with the release of Letraset sheets containing Lorem Ipsum passages, and more recently with desktop publishing software like Aldus PageMaker including versions of Lorem Ipsum.

Fig 7.11: Decrypted splited files

Joined File page in Fig: 4.12 allows users to combine or join multiple split files back into their original form. Splitting files into smaller parts is often done for easier handling, distribution, or transmission. The join split files page provides users with a convenient way to merge these split files back together.



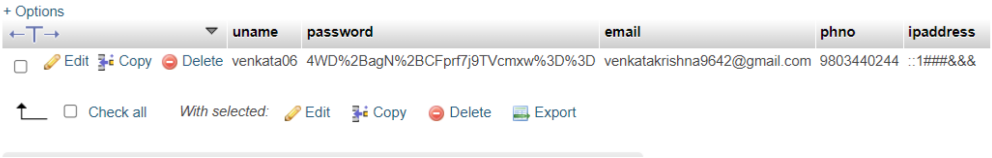
Joined File.

Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley oftype and scrambled it to make a type specimen book. It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged. It was popularisedin the 1960s with the release of Letraset sheets containing Lorem Ipsum passages, and more recently with desktop publishing software like Aldus PageMaker including versions of Lorem Ipsum.

Fig 7.12: After joining decrypted files

Backend MySQL Results:

Fig: 4.13 typically displays a list or table view of all the users in the system. Each user entry may include details such as username, email, phone no. etc..



+ Options

←T→	uname	password	email	phno	ipaddress
□ Edit Copy Delete	venkata06	4WD%2BagN%2BCFprf7j9TVcmxw%3D%3D	venkatakrishna9642@gmail.com	9803440244	::1###&&&

Fig 7.13: Users data

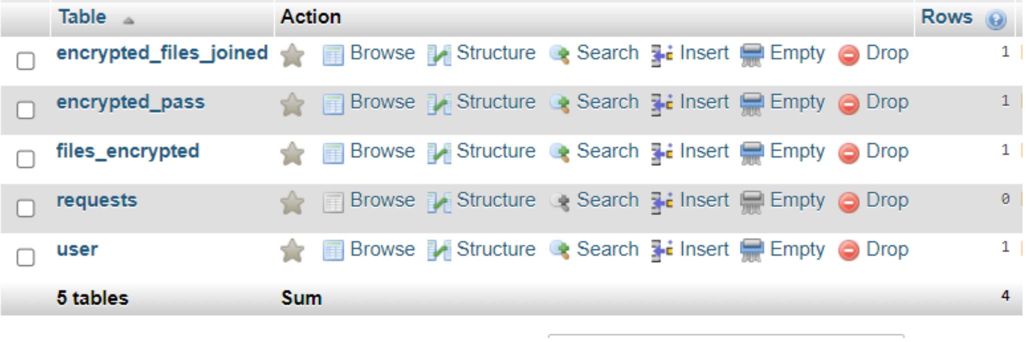


	Table	Action	Rows
□	encrypted_files_joined	Browse Structure Search Insert Empty Drop	1
□	encrypted_pass	Browse Structure Search Insert Empty Drop	1
□	files_encrypted	Browse Structure Search Insert Empty Drop	1
□	requests	Browse Structure Search Insert Empty Drop	0
□	user	Browse Structure Search Insert Empty Drop	1
	5 tables	Sum	4

Fig 7.14: Tables used in database

CHAPTER – 8

CONCLUSION AND FUTURE SCOPE

.

8.1 Summary of the work

The owner of the cloud server uploads the data via our technology. To strengthen file security in cloud computing, the source file is separated into numerous portions. Each encryption algorithm is employed to encrypt every component of the file. Cloud storage is used to store encrypted files. Each component of the file is stored on a different cloud database server. Even in the event of an attack, no critical data is compromised, as only a single fragment of each uploaded file, in any format, is stored on the cloud server.

8.2 Conclusion

The implementation of the suggested approach, including the encryption and decryption of files, is thoroughly described in the paper. The suggested solution provides a reliable and secure technique for storing files on the cloud, guaranteeing that information is shielded from unauthorized access or change. To guarantee that the system continues to be effective, potential vulnerabilities must be constantly addressed and updated, just like with any security solution. The suggested approach calls for symmetric AES and DES encryption of the data, followed by asymmetric RSA encryption of the AES and DES keys. The paper provides a detailed explanation of how the suggested approach is put into practice, including how files are encrypted and decrypted. The suggested solution offers a trustworthy and secure method for uploading files to the cloud, ensuring that data is protected from illegal access or modification. To ensure that the system remains to be successful, potential vulnerability must be regularly identified and revised, just as with any secure solution. According to the suggested method, the data would first be encrypted using symmetric AES and DES before the AES and DES keys would be encrypted using asymmetric RSA.

8.3 Future Scope

In this project we have considered only text files as of now. In future we can add more file types for securely storing. Implement better ways to share the key file to user like embedding the key in images etc. Hybrid cryptography is a useful method for protecting cloud-based data storage. Using hybrid cryptography, the following potential future improvements could be implemented to further increase the privacy of file storage in the cloud:

- Supports multiple type of file formats
- Instead of sending a plain text email, one can employ steganography, a technique for concealing information within an image, to hide the encryption key. By

embedding the key within the image and sending it as an email attachment, the key remains covertly concealed within the visual data.

- Request file from other user based on usernames or userId.
- Integrate with mail service to send notifications and alerts to users.

Multi-factor authentication: Hybrid cryptography could be paired with multi-factor authentication (MFA) to add an additional layer of protection. Before granting access to the encrypted data, MFA includes employing several authentication factors, such as a password and a biometric.

Zero-knowledge proofs: Zero-knowledge proofs (ZKP) allow one party to convince another that they are aware of specific details without disclosing those details. ZKP could be used to hybrid cryptography to improve secure data flow between many parties without disclosing the encryption key.

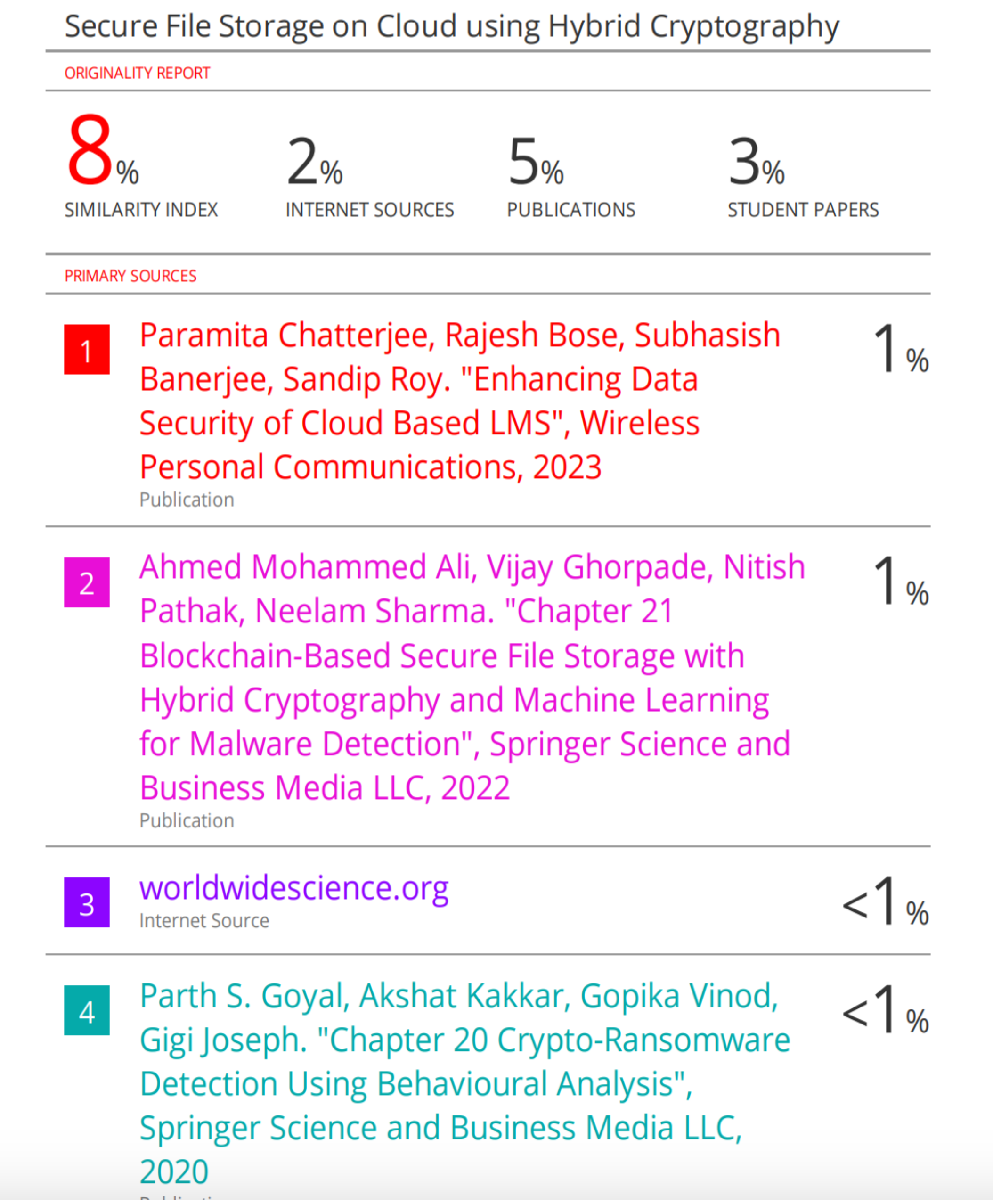
REFERENCES

1. "A Hybrid Cryptography-based Secure File Storage System for Cloud Computing" by K. V. Ramachandran, Naveen Kumar, and R. Sriramakavacham.
2. Ankit Gupta and Dheerendra Singh's "Hybrid Cryptography based Secure File Storage on Cloud."
3. "A Hybrid Cryptography-based Approach for Secure File Storage in Cloud Computing" by S. Senthil Kumaran and S. Santhosh K.
4. Hybrid Cryptography for Secure File Storage on the Cloud by P. N. Shriram.
5. "Secure File Storage on Cloud using Hybrid Cryptography and Attribute-based Encryption" by R. M. and Anitha. Hemalatha.
6. A survey of secure cloud file storage using hybrid cryptography is presented by S. Both Sivasankari and S. Sathish.
7. "Hybrid Cryptography for Secure File Storage on Cloud: A Survey," by R. Santhi and V. N. Sumathy.
8. S. Srinivasan and K. Sathish Kumar's "Hybrid Cryptography based Secure File Storage in Cloud: A Review."
9. "A Review of Secure File Storage on Cloud using Hybrid Cryptography" by N. G. Patel and J. M. Patel.
10. P. S. Verma and P. R. Dubey's "Hybrid Cryptography based Secure File Storage on Cloud: A Systematic Review."
11. "Hybrid Cryptography Based File Storage Security in Cloud Computing" by Shangquan Wang, Xuelian Lin, and Chengyu He.
12. "Secure File Storage on Cloud using Hybrid Cryptography: A Survey" by Gaurav Kumar, Kuldip Singh, and R. K. Jha
13. Ajay Kumar and S. S. Tyagi's "Hybrid Cryptography for Secure Data Storage in Cloud Computing: A Survey"
14. "Secure Data Storage in Cloud Computing using Hybrid Cryptography" by S. K. Samantaray et al.

References

15. "A Secure File Storage System for Cloud Computing using Hybrid Cryptography" by H. Alrawais et al.
16. "Secure Cloud Data Storage using Hybrid Cryptography and Steganography" by M. S. Thakur.
17. "A Novel Approach for Secure Data Storage in Cloud Computing using Hybrid Cryptography" by M. A. Ali et al.
18. "Secure and Efficient Cloud Storage System using Hybrid Cryptography and Proxy Re-Encryption" by P. Thakur.
19. "A Secure and Efficient Cloud Storage System using Hybrid Cryptography and Data Fragmentation" by V. Dhawan.
20. "An Efficient and Secure Cloud Storage System using Hybrid Cryptography and Access Control" by S. Singh et al.
21. "A Hybrid Cryptography Based Secure Data Storage and Retrieval for Cloud Computing" by N. Mittal.
22. "A Hybrid Cryptography Based Secure Cloud Storage System with Key Management" by R. Sharma.
23. "Secure Data Storage in Cloud Computing using Hybrid Cryptography" by N. R. Patel.
24. "Enhancing Cloud Security using Hybrid Cryptography" by S. S. Kumar et al.
25. "Secure Cloud Storage using Hybrid Cryptography and Access Control" by J. S. Meena et al.

Plagiarism Report



Secure File Storage on Cloud using Hybrid Cryptography

ORIGINALITY REPORT

8%	2%	5%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

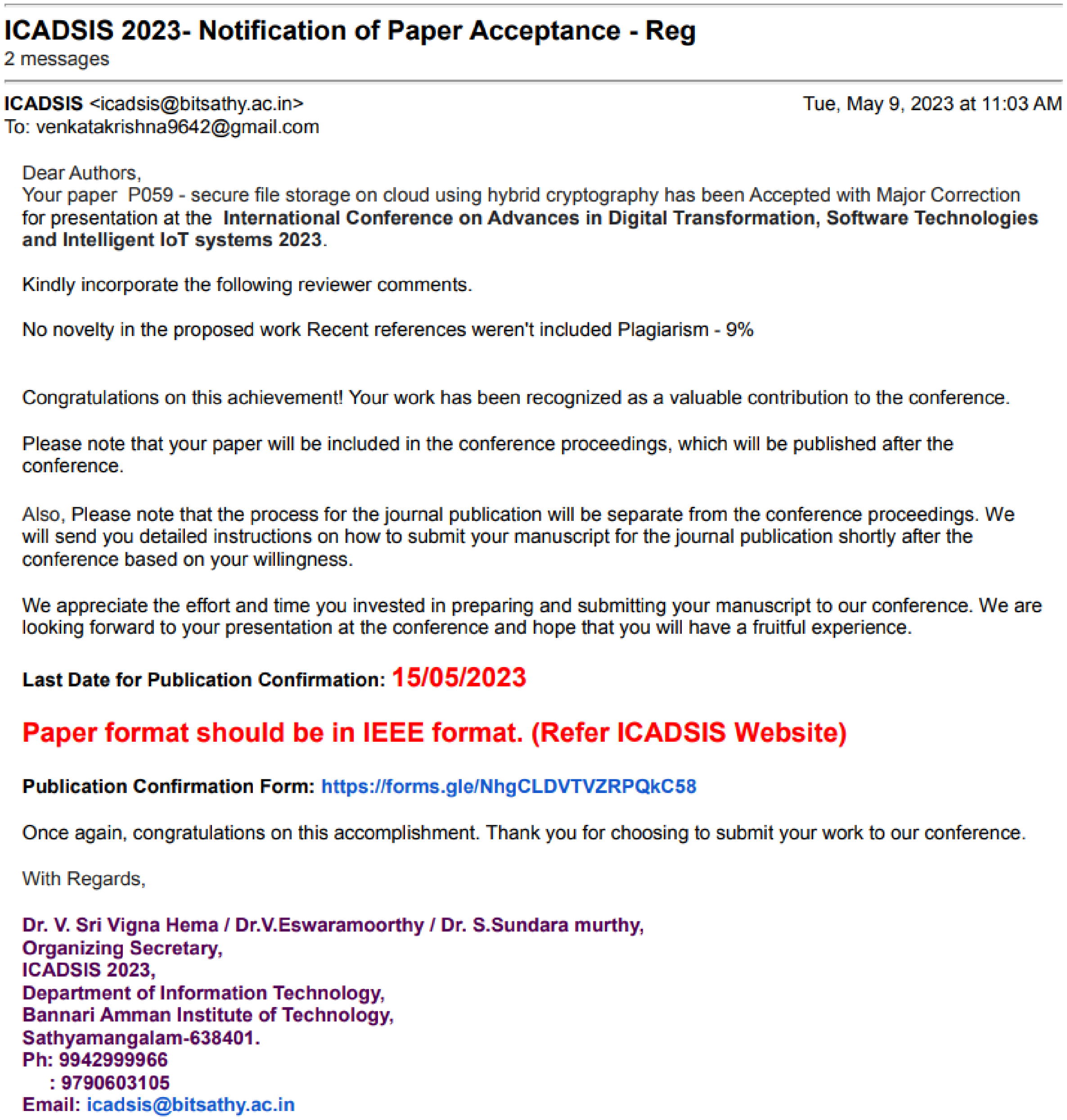
PRIMARY SOURCES

1	Paramita Chatterjee, Rajesh Bose, Subhasish Banerjee, Sandip Roy. "Enhancing Data Security of Cloud Based LMS", Wireless Personal Communications, 2023 Publication	1%
2	Ahmed Mohammed Ali, Vijay Ghorpade, Nitish Pathak, Neelam Sharma. "Chapter 21 Blockchain-Based Secure File Storage with Hybrid Cryptography and Machine Learning for Malware Detection", Springer Science and Business Media LLC, 2022 Publication	1%
3	worldwidescience.org Internet Source	<1%
4	Parth S. Goyal, Akshat Kakkar, Gopika Vinod, Gigi Joseph. "Chapter 20 Crypto-Ransomware Detection Using Behavioural Analysis", Springer Science and Business Media LLC, 2020	<1%

Publication

Our research paper, titled " **Secure File Storage On Cloud Using Hybrid Cryptography**," was accepted for presentation at the **International Conference on Advances in Digital Transformation, Software Technologies and Intelligent IoT systems 2023**..The Conference will be taking place next month and we will be proceeding for publication post the conference. We are hereby attaching our acceptance letter from the conference.

Acceptance Confirmation e-mail:



ICADSIS 2023- Notification of Paper Acceptance - Reg
2 messages

ICADSIS <icadsis@bitsathy.ac.in> Tue, May 9, 2023 at 11:03 AM
To: venkatakrishna9642@gmail.com

Dear Authors,
Your paper P059 - secure file storage on cloud using hybrid cryptography has been Accepted with Major Correction for presentation at the **International Conference on Advances in Digital Transformation, Software Technologies and Intelligent IoT systems 2023**.

Kindly incorporate the following reviewer comments.

No novelty in the proposed work Recent references weren't included Plagiarism - 9%

Congratulations on this achievement! Your work has been recognized as a valuable contribution to the conference.

Please note that your paper will be included in the conference proceedings, which will be published after the conference.

Also, Please note that the process for the journal publication will be separate from the conference proceedings. We will send you detailed instructions on how to submit your manuscript for the journal publication shortly after the conference based on your willingness.

We appreciate the effort and time you invested in preparing and submitting your manuscript to our conference. We are looking forward to your presentation at the conference and hope that you will have a fruitful experience.

Last Date for Publication Confirmation: 15/05/2023

Paper format should be in IEEE format. (Refer ICADSIS Website)

Publication Confirmation Form: https://forms.gle/NhgCLDVTVZRPQkC58

Once again, congratulations on this accomplishment. Thank you for choosing to submit your work to our conference.

With Regards,

Dr. V. Sri Vigna Hema / Dr.V.Eswaramoorthy / Dr. S.Sundara murthy,
Organizing Secretary,
ICADSIS 2023,
Department of Information Technology,
Bannari Amman Institute of Technology,
Sathyamangalam-638401.
Ph: 9942999966
: 9790603105
Email: icadsis@bitsathy.ac.in