IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Secure Cloud: Cryptographic File Management System

MS. POONAM DHAMAL
Assistant Professor, Information Technology
G H Raisoni College of Engineering and Management, Pune, India

REWATI WARHADE, JAY SHELKE, GOVIND SURYAWANSHI
Undergraduate Students, Information Technology
G H Raisoni College of Engineering and Management, Pune, India

Abstract: The increasing adoption of cloud computing across various organizations and the IT sector has transformed how data is stored and accessed, offering a cost-effective and efficient solution for managing information. With the rapid shift towards cloud-based services, users can enjoy enhanced data accessibility through the Internet, enabling real -time collaboration and resource sharing. However, this is widespread reliance on cloud technology raises significant is concerns regarding data security and privacy, particularly when sensitive information is entrusted to cloud storage providers, some of which may be perceived as untrustworthy. The primary challenge lies in securely sharing and storing data while ensuring that it is remains protected from potential breaches or unauthorized access in entrusted cloud environments. As organizations migrate to the cloud, the need for robust encryption and decryption techniques becomes paramount. This paper proposes a comprehensive approach to safeguarding sensitive client information by employing a combination of well-established encryption algorithms, specifically Advanced Encryption Standard (AES), Data Encryption Standard (DES), and SHA-256.

Keyword: Cloud, Encryption/Decryption Technique, AES, DES and SHA-256.

I. INTRODUCTION

The project focuses on addressing critical need for secure data storage in the rapidly evolving landscape of cloud computing. As organizations increasing migrate sensitive information to cloud environments, concerns over data security and privacy have intensified. This project aims to develop a secure file storage system that utilizes cryptographic techniques to protect the data from unauthorized access, ensuring confidentiality, integrity, and the availability. By implementing a combination of symmetric and asymmetric encryption algorithms—specifically AES, DES, and SHA-256—this solution enables users to encrypt files before they are uploaded to the cloud, thereby safeguarding sensitive information from potential threats posed by entrusted cloud storage providers. The system will feature user authentication, a user-friendly interface, and robust logging mechanisms to monitor data access. Additionally, this project emphasizes the importance of data management practices that prioritize reliability and security, providing an accessible cloud environment for diverse users, including students and educators.AES, DES, and SHA-256, strive to empower users with the tools necessary to safeguard their data in an increasingly uncertain digital environment. Our goal is not only to enhance data security but also to foster a culture of trust and reliability in cloud computing, enabling users to leverage its benefits without compromising the safety of their vital information. The growing adoption of cloud computing has revolutionized how organizations and Individuals manage and store data. However, this rapid evolution has brought significant challenges concerning data security and privacy. As sensitive information increasingly migrates to cloud platforms, addressing these challenges through robust mechanisms that ensure data confidentiality, integrity, and availability becomes critical. This

project aims to develop a comprehensive Secure File Storage System tailored for the cloud environment. By leveraging advanced cryptographic techniques, the proposed system will protect data from unauthorized access and mitigate potential threats posed by entrusted cloud storage providers. The system incorporates a combination of symmetric and asymmetric Encrypt ion algorithms, including Advanced Encryption Standard (AES), Data Encryption Standard (DES), and SHA-256. These algorithms ensure that files are securely encrypted before being uploaded to the cloud, sensitive data even if the storage provider is

II. LITERATURE REVIEW

Houda Guesmi in 2017 introduces an identity-based cryptography model to enhance data storage confidentiality in cloud environments. Conducted at CRISTAL LAB, ENSI, Tunisia, the study emphasizes secure and efficient encryption mechanisms[1]. Reshma Suryawanshi & Santosh Shelke propose a public auditing and threshold cryptography scheme for improving cloud data storage security. This approach enables effective third-party auditing while maintaining data integrity and privacy[2]. Arjun Kumar, Byung Gook Lee & HoonJae Lee presents a framework for secure storage and data access in cloud computing. Conducted at Dongseo University, Korea, the study focuses on ubiquitous IT and cloud integrity[3]. Romani explores a cryptography API for next-generation key storage in cloud systems. Presented at the ECAI International Conference, it emphasizes modern encryption techniques for enhanced cloud security[4]. G. Murali in 2017 introduces the Cloud QKDP, a quantum key distribution protocol designed for cloud computing. Conducted at JNTUA College of Engineering, India, it integrates quantum cryptography for improved security[5]. Surya Nepal in 2011 This IEEE study focuses on secure storage services in hybrid cloud environments. The authors present mechanisms to balance security and flexibility in multi-cloud setups[6]. Kajal Chachapara study proposes cryptographic methods for secure data sharing in cloud computing. Presented at NUiCONE, it highlights encryption solutions tailored for collaborative environments[7]. K. Brindha & N. Jeyanthi in 2015 explores securing cloud data using visual cryptography. Conducted at VIT University, the study leverages innovative image-based techniques to enhance data protection[8]. Punam V. Maitri in 2019 research on implements hybrid cryptography algorithms for secure file storage in the cloud. Conducted at Dhole Patil College of Engineering, it combines multiple encryption methods for robust protection[9]. Md. Abu Musa & Md. Ashiq Mahmood proposes client-side cryptography for cloud system security. Conducted at KUET, Bangladesh, the study enhances user-controlled encryption to safeguard data[10].

III. METHODOLOGY

The Figure 3.a shows a secure file storage system in cloud computing using cryptography aims to ensure data confidentiality, integrity, and availability while allowing users to upload, store, and retrieve files securely. The system design incorporates encryption, decryption, and access control to protect data from unauthorized access and ensure the integrity of the stored files. Here is proposed system architecture for this type of system:

User Interface (UI) a web for users to interact with the cloud storage system. Client-Side Encryption Where the files are encrypted before being uploaded to the A Cloud storage. Cloud Storage The cloud infrastructure where files are stored, with encrypted content to ensure data privacy. Authentication & Authorization Server ensures that only authorized users have access to system and specific files.

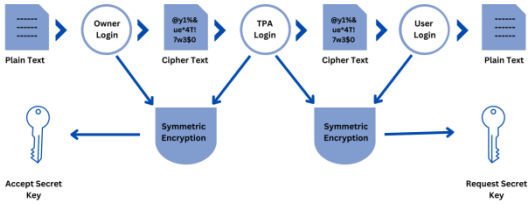


Figure 3.a: System Architecture of secure file system

Secure file storage workflow begins with the initiation of a process designed to ensure the confidentiality and the integrity of user data. Users authenticate themselves using secure methods such as a username-password combination or multi-factor authentication adding an extra layer of protection. Before uploading, files are encrypted using robust cryptographic algorithms like AES or RSA, safeguarding data against unauthorized access. The encrypted files are then uploaded to a central cloud server, which serves as the secure storage location. When needed, users can download the encrypted file from the cloud, ensuring data remains protected during transit via protocols like HTTPS. Once the file is downloaded, it is decrypted locally on the user's device using the appropriate decryption key, ensuring the information is accessible only to authorized users. This end-to-end secure workflow focuses on maintaining data security both in transit and at rest, protecting it from potential breaches and ensuring user confidence. The system consists of multiple entities designed to ensure smooth functionality and security. The User entity stores attributes like User ID, Name, Email, Password, and Role (Student/Educator/Other) and has a one-to-many relationship with the File entity, where users upload files. The Authentication entity is linked to the user for managing login details and status. File stores data about uploaded files such as File ID, File Name, File Size, and its encrypted key, linking to both the user and Cloud Storage where files are securely stored. Encryption handles the encryption of files, and file storage, with a one-to-many relationship with files. The Access Log tracks user actions such as viewing or downloading files and links both the user and the file. The Group entity allows users to form groups with a many-to-many relationship with User, and the Group File Access entity manages file permissions within groups.

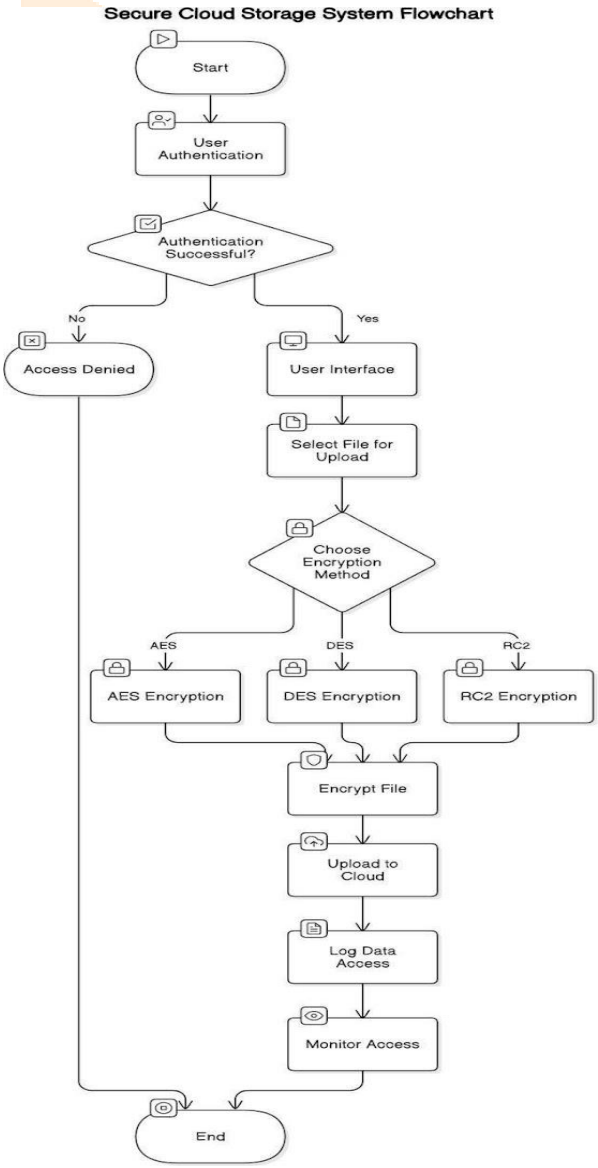


Figure 3.b: UML Diagram

The Figure 3.b shows flowchart for the Secure Cloud Storage System begins with user authentication. If authentication is successful, the user is directed to the user interface where they can select a file for upload. Once a file is selected, the user is prompted to choose an encryption method, with options including AES, DES, or RC2 encryption. After the encryption method is selected, the file is encrypted, and then uploaded to the cloud storage. The system logs data access and monitors file access to ensure security and track user actions. If authentication fails, access is denied, and the process ends. The system provides a secure and organized flow for file handling, ensuring encryption and monitoring are in place to protect data during storage and access.

The secure file storage workflow begins with the initiation of a process designed to ensure the confidentiality and the integrity of user data. Users authenticate themselves using secure methods such as a username-password combination or multi-factor authentication, adding an extra layer of protection. Before uploading, files are encrypted using robust cryptographic algorithms like AES or RSA, safeguarding data against unauthorized access. The encrypted files are then uploaded to a central cloud server, which serves as the secure storage location. When needed, users can download the encrypted file from the cloud, ensuring data remains protected during transit via protocols like HTTPS. Once the file is downloaded, it is decrypted locally on the user's device using the appropriate decryption key, ensuring the information is accessible only to authorized users. This end-to-end secure workflow focuses on maintaining data security both in transit and at rest, protecting it from potential breaches and ensuring user confidence. The Figure III.2 shows flowchart for the Secure Cloud Storage System begins with user authentication. If authentication is successful, the user is directed to the user interface where they can select a file for upload. Once a file is selected, the user is prompted to choose an encryption method, with options including AES, DES, or RC2 encryption. After the encryption method is selected, the file is encrypted, and then uploaded to the cloud storage. The system logs data access and monitors file access to ensure security and track user actions. If authentication fails, access is denied, and the process ends. The system provides a secure and organized flow for file handling, ensuring encryption and monitoring are in place to protect data during storage and access.

IV. RESULT AND DISCUSSION

The system was successfully shown Enhanced Data Security Successful implementation of symmetric and asymmetric cryptographic algorithms will ensure files are securely encrypted and decrypted, protecting the sensitive data from unauthorized access. User authentication ensures robust access control by verifying the identity of users before granting access to the system. This mechanism prevents unauthorized access, safeguarding sensitive data. By implementing secure login credentials or multi-factor authentication, it enhances the overall security of the cloud system, maintaining data integrity and user privacy.

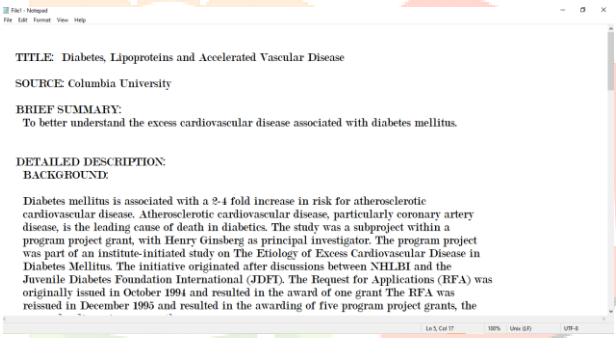
The Figure 4.a shows interface in the image showcases the "Secure File Storage System using Cloud Computing", designed to prioritize data security for users and organizations. Contains options like "Homepage", "User Login", "TPA (Third Party Administrator) Login", "Owner Login", "Investigator Login", "About Us" and "Contact Us" allowing different user roles to access their respective functionalities. Clearly labeled as "Secure File Storage System using Cloud Computing" indicating the purpose of the platform. Provides a login area for users to securely enter their credentials (e.g. username or email).

Figure 4.a: Interface of the Storage System

The Figure 4.b shows image shows the User Login Page for a Secure File Storage System using Cloud Computing. The design presents a professional and user- friendly interface with the following elements Header Section: Login Form, Select Role, Enter Credentials, Login Button, Create New User and Footer Section. Also this is a login page for end user for registration and login.

Figure 4.b: Login and Registration

The Figure 4.c shows the input file functionality for securely saving files in the project involves several crucial components to ensure data security, compliance and user accessibility. The interface provides real-time feedback to the user about the upload status, including success, encryption confirmation, or any errors encountered. Encryption ensures that unauthorized access is prevented, even if the file is intercepted during transfer or stored in the cloud. The database maintains a mapping between the encrypted file and the user's profile, including ownership and access permissions.


TITLE: Diabetes, Lipoproteins and Accelerated Vascular Disease

SOURCE: Columbia University

BRIEF SUMMARY:
To better understand the excess cardiovascular disease associated with diabetes mellitus.

DETAILED DESCRIPTION:
BACKGROUND:

Diabetes mellitus is associated with a 2-4 fold increase in risk for atherosclerotic cardiovascular disease. Atherosclerotic cardiovascular disease, particularly coronary artery disease, is the leading cause of death in diabetics. The study was a subproject within a program project grant, with Henry Ginsberg as principal investigator. The program project was part of an institute-initiated study on The Etiology of Excess Cardiovascular Disease in Diabetes Mellitus. The initiative originated after discussions between NHLBI and the Juvenile Diabetes Foundation International (JDFI). The Request for Applications (RFA) was originally issued in October 1994 and resulted in the award of one grant The RFA was reissued in December 1995 and resulted in the awarding of five program project grants, the

Figure 4.c: Input File

The Figure 4.e shows an encrypted file is a data file that has undergone process of encoding to prevent unauthorized access. Encryption ensures the confidentiality and security of sensitive information by converting the original file, also known as plaintext, into a scrambled, unreadable format called cipher text. Decryption, which requires a specific key, reverses the process, restoring the file to its original state and In the Figure 4.d the files and Splited in multiple files because of security and every piece of the data ran through the algorithm produces a unique hash that cannot be duplicated by any other piece of the data. The resulting digital signature is also unique as it depends on the hash that's generated out of the data.

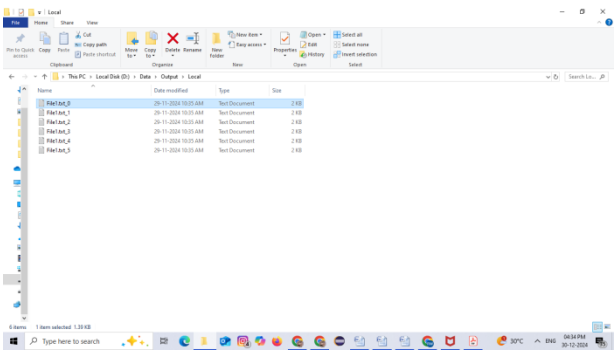


Figure 4.d: Splited Files

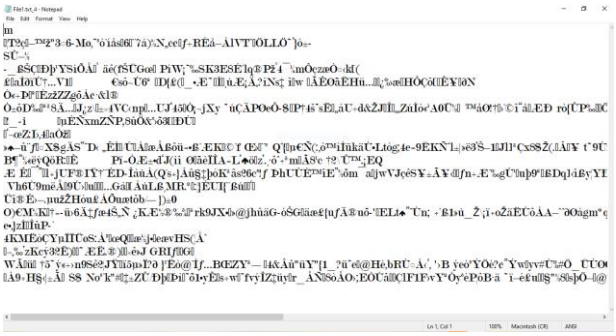


Figure 4.e: Output File

V. Conclusion

The primary objective of this project is to securely store and the access data in the cloud, where the owner has no direct control over the data. To achieve this, we leverage Elliptic Curve Cryptography (ECC) for encryption, ensuring the protection of sensitive the data in the cloud. The cloud architecture is designed to enhance performance during data storage and retrieval, with ECC providing an efficient encryption and decryption process. This approach improves security while maintaining high performance. Additionally, our solution addresses the challenge of group data sharing; ensuring that only authorized members of a group can access the shared data. We are actively working to refine this process, ensuring both secure and efficient access to shared cloud data. The future work is user behavior analytics Implement mechanisms to analyze the user behavior, detect anomalies, and identify the potential threats, thereby enhancing the security and protection of the cloud storage system.

REFERENCES

1] H. Guesmi and L. A. Saïdane, "Improved Data Storage Confidentiality in Cloud Computing Using Identity-Based Cryptography," CRISTAL LAB, National School of Computer Science (ENSI), Tunisia, 2017.
2] R. Suryawanshi and S. Shelke, "Improving Data Storage Security in Cloud Environment Using Public Auditing and Threshold Cryptography Scheme," Sinhagad Academy of Engineering, 2017.
3] A. Kumar, B. G. Lee, and H. J. Lee, "Secure Storage and Access of Data in Cloud Computing," 1Department of Ubiquitous-IT, Department of Computer and Information Engineering, Dongseo University, Busan, Korea, 2011.
4] ECAI Conference, "A Cryptography API: Next Generation Key Storage Provider for Cryptography in the Cloud," 10th Edition Electronics, Computers and Artificial Intelligence, 28–30 June 2018, Iasi, Romania.
5] G. Murali, "Cloud QKDP: Quantum Key Distribution Protocol for Cloud Computing," Asst. Prof., Dept. of CSE, JNTUA College of Engineering, Pulivendula, Andhra Pradesh, India, 2017.
6] S. Nepal, C. Friedrich, L. Henry, and S. Chen, "A Secure Storage Service in the Hybrid Cloud," in 2011 Fourth IEEE International Conference on Utility and Cloud Computing, IEEE, 2011.
7] K. Chachapara, "Secure Sharing with Cryptography in Cloud Computing," in 2013 Nirma University International Conference on Engineering (NUiCONE), Department of Computer Science & Engineering, TIT Engineering & Technology, RGPV University, Bhopal, India, 2013.
8] K. Brindha and N. Jeyanthi, "Securing Cloud Data Using Visual Cryptography," in 2015 International Conference on Innovation Information in Computing Technologies (ICIICT), VIT University, Vellore, Chennai, India, 2015.
9] P. V. Maitri, "Secure File Storage in Cloud Computing Using Hybrid Cryptography Algorithm," Department of Computer Engineering, Dhole Patil College of Engineering, Pune, India, 2019.
10] M. A. Musa and M. A. Mahmood, "Client-Side Cryptography Based Security for Cloud Computing System," Institute of Information and Communication Technology, Khulna University of Engineering & Technology (KUET), Khulna, Bangladesh, 2018.