CLOUD-BASED FILE ENCRYPTION

[1] **Kodi Bhavani sai, [2] Neerukonda Naga Venkata Manjusha, [3] Maryam Fatima, [4] K Ganesh**
[1] Dr Sridhar Reddy Surkanti, Associate Professor, dr.sridharreddy@sreyas.ac.in
[1,2,3,4] Students, Sreyas Institute of Engineering and Technology
[1] bhavanisain2003@gmail.com, [2] manjushan2002@gmail.com, [3] maryam037fatima@gmail.com, [4] ganeshkurva1royal@gmail.com

Abstract: *The system is designed to provide secure cloud-based file encryption by incorporating advanced cryptographic techniques and robust user authentication mechanisms. It leverages AES encryption with CBC mode to ensure file confidentiality, complemented by IBE-based key management for secure key distribution. HMAC is used to verify data integrity, while OTP-based multifactor authentication strengthens user login security, with OTPs sent to registered email addresses. Data owners are enabled to share files securely with selected users, with detailed activity logs tracking user actions for accountability. Key functionalities include user signup, OTP validation during login, file upload and sharing, as well as file decryption and downloading. Implemented with Python 3.7.2 and MySQL for database management, the system operates on a local Python server, offering a comprehensive approach to data protection and efficient file sharing. This design ensures the security of sensitive data, preventing unauthorized access or tampering, while facilitating secure collaboration within a cloud environment.*

Index Terms: *Secure File Encryption, AES-CBC, IBE-Based Key Management, HMAC, OTP-Based Multifactor Authentication, Cloud Security, Data Integrity, User Activity Logging.*

1. INTRODUCTION

The widespread adoption of cloud storage technologies has fundamentally transformed data management for individuals and organizations, offering scalable, accessible, and cost-effective solutions for file storage and sharing. Cloud platforms have revolutionized how data is stored and accessed, but this increasing reliance on cloud environments has also raised significant concerns about data security. The risk of data breaches, unauthorized access, and cyberattacks in cloud environments has grown, highlighting the need for advanced security systems to safeguard sensitive information. Addressing these security challenges requires not only encryption but also robust access control, monitoring, and the ability to detect unauthorized activities to reduce vulnerabilities [1][2].

This project introduces a Secure Cloud-Based File Encryption system designed to mitigate these concerns by incorporating several advanced security features. At the heart of the system is the Advanced Encryption Standard (AES) algorithm, a widely trusted encryption method renowned for its effectiveness in securing sensitive data [3]. The AES encryption is further enhanced by the use of Cipher Block Chaining (CBC) mode, which ensures that each block of plaintext is encrypted uniquely, minimizing the risk of data pattern leakage and enhancing security against attacks [4]. In addition to encryption, the system employs the Hash-Based Message Authentication Code (HMAC), which verifies data integrity by ensuring that the file has not been tampered with during storage or transmission [5].

To complement encryption, the system incorporates multifactor authentication (MFA) through One-Time Passwords (OTPs) sent to users' registered email addresses. This additional layer of authentication significantly reduces the likelihood of unauthorized access, even if login credentials are compromised, by ensuring that only verified individuals can access the system [6]. A key component of the system is the Access Control List (ACL), which enables data owners to define specific permissions for accessing shared files, allowing fine-grained control over who can decrypt, view, or download the files. This feature ensures secure collaboration while maintaining tight oversight and confidentiality [7].

Furthermore, the system prioritizes transparency by recording all user activities in a secure, detailed log. These logs capture file uploads, downloads, and access attempts, offering comprehensive auditing and promoting accountability within the system. The modular architecture of the system, built with Python and MySQL, ensures scalability and a seamless user experience, making it suitable for both personal and organizational use. By integrating robust encryption, MFA, ACLs, and detailed activity logs, the system provides a secure, reliable platform for managing sensitive data in cloud environments.

2. LITERATURE SURVEY

The increasing adoption of cloud computing has brought with it significant advancements in data management, offering a wide range of services such as scalable storage, remote processing, and improved accessibility for individuals and organizations. However, the rapid growth of cloud services has also raised important security concerns. A review of existing literature provides a comprehensive understanding of the challenges, solutions, and technologies related to cloud security, particularly focusing on data protection, encryption, and access control mechanisms.

Yashpal Kadam [1] identifies several security issues in cloud computing, including data breaches, loss of data control, and insecure application programming interfaces (APIs). These concerns necessitate robust security measures to protect sensitive information in the cloud. The use of strong encryption algorithms is emphasized as a primary defense against unauthorized access, along with advanced access control mechanisms. Similarly, Bhadauria et al. [2] in their survey on cloud computing security issues highlight challenges such as privacy risks, data integrity, and secure storage. They point out that existing solutions often lack transparency and adequate monitoring, which are critical for addressing unauthorized access and ensuring data security in cloud environments.

Vouk [3] discusses the broader implications of cloud computing on information security, noting that the centralization of data in cloud storage services increases the vulnerability of systems to cyberattacks. He suggests that encryption is crucial for maintaining the confidentiality and integrity of data. Ye Hu et al. [4] elaborate on the resource provisioning aspect of cloud computing and its impact on security, highlighting the need for cloud providers to offer secure storage solutions that can dynamically adjust to various threats. Their work suggests that the resources required for securing cloud data are often underestimated, which could lead to the compromise of sensitive information.

Daniele Catteddu and Giles Hogben [5] in their paper emphasize the potential benefits and risks of cloud computing. They highlight that while cloud environments offer several advantages, such as cost efficiency and scalability, they also pose risks to information security. These risks include not only unauthorized access but also

the potential for data loss and service disruptions. As a solution, they propose a hybrid approach that combines public and private cloud resources to offer a more secure and balanced environment for data storage and processing. In this context, the use of cryptographic methods, particularly the Advanced Encryption Standard (AES), becomes essential for safeguarding data in both public and private cloud infrastructures.

The work of Li et al. [11] contributes to the growing body of knowledge on cloud computing security by focusing on identity-based authentication systems. They propose an innovative method for cloud computing environments that ties user authentication to their unique identity, significantly reducing the risk of unauthorized access. This approach helps ensure that only authorized users can access cloud resources, enhancing overall system security. Additionally, the paper underscores the importance of key management and encryption as fundamental components of any security framework for cloud services.

In the context of cloud-based applications, Gunasekar Kumar and Anirudh Chelikani [8] conducted an analysis of security issues specific to cloud-based e-learning platforms. They observed that traditional security models, such as firewalls and antivirus software, are insufficient to protect data in cloud environments, particularly when handling sensitive user information. Their work highlights the importance of integrating advanced encryption technologies, such as AES, and multifactor authentication (MFA) to protect user data. Furthermore, they emphasize that encryption techniques must be complemented by effective access control mechanisms, such as Access Control Lists (ACLs), to ensure that only authorized users can access specific resources.

The potential for cyberattacks in cloud environments has been addressed by Jiyi Wu et al. [9], who discuss recent advances in cloud security. Their study outlines several attack vectors, including man-in-the-middle attacks, data breaches, and malicious insiders. They argue that traditional security measures, while useful, are no longer sufficient in the face of evolving threats. Their research advocates for the adoption of more sophisticated encryption techniques and advanced authentication methods, which could include identity-based encryption (IBE), multifactor authentication, and detailed logging for auditing purposes. This approach aligns with the findings of Ahmad-Reza Sadeghi et al. [10], who explored token-based cloud computing security. Their work demonstrates how tokenization can provide an additional layer of protection against unauthorized access, particularly in situations where direct encryption may not be sufficient.

The necessity of securing cloud storage solutions is also emphasized in the Federal Information Processing Standards (FIPS) publication, which introduced the Advanced Encryption Standard (AES) as a benchmark for data encryption in the United States government [12]. AES has become the industry standard for encrypting sensitive information due to its efficiency and strength. It supports multiple key lengths (128, 192, and 256 bits), providing flexibility for different security requirements. As highlighted by Kadam [1], AES encryption, particularly when used in conjunction with modes like Cipher Block Chaining (CBC), offers robust protection by ensuring that identical blocks of plaintext do not produce identical ciphertext. This technique significantly enhances security by preventing potential attackers from analyzing data patterns.

3. MATERIALS AND METHODS

The proposed system integrates advanced encryption techniques, multifactor authentication, and robust access control mechanisms to provide secure cloud-based file encryption. At its core, it uses AES encryption with CBC mode for file confidentiality and protection during storage and transmission. Multifactor authentication with OTPs

enhances user security, while an Access Control List (ACL) framework allows data owners to define precise file access permissions. The system employs Identity-Based Encryption (IBE) for simplified key management and utilizes comprehensive activity logging for transparency and accountability. Built using Python and MySQL, the system offers an intuitive user interface, scalability, and efficient performance. This integrated approach addresses the limitations of existing cloud storage solutions, ensuring secure, user-friendly, and scalable cloud file sharing.

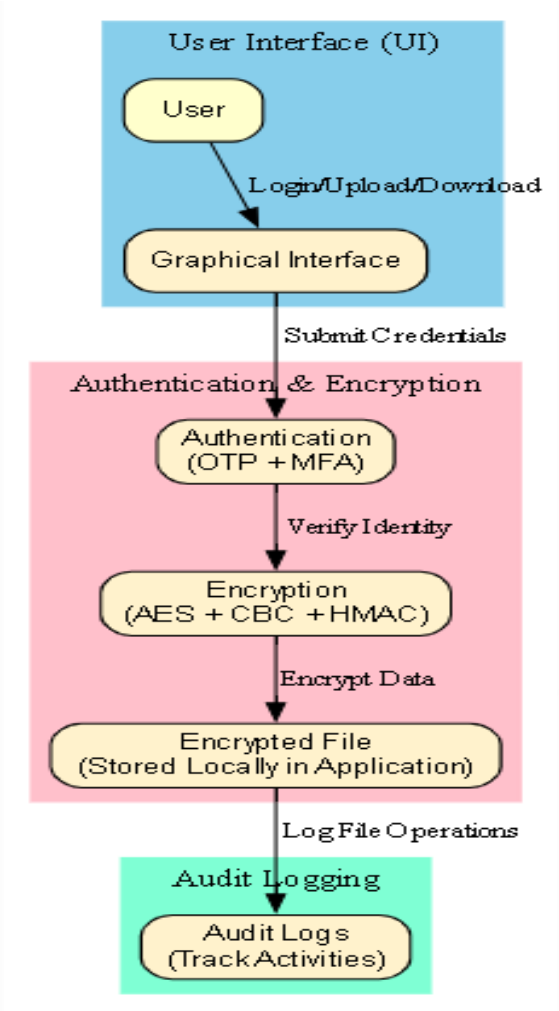

Fig.1 Proposed Architecture

The system architecture comprises a User Interface (UI) for user interaction, an Authentication & Encryption module for secure login and data encryption, and an Audit Logging module for tracking activities. Users interact with the UI to log in, upload or download files. The Authentication & Encryption module verifies user identity through OTP and MFA, encrypts data using AES-CBC-HMAC, and stores the encrypted files locally. The Audit Logging module records all file operations for security and compliance.

a) Dataset Collection:

The dataset for this project focuses on cloud storage security, comprising various real-world data samples to evaluate the effectiveness of encryption, authentication, and access control mechanisms. The dataset includes user activities, file upload and download logs, access requests, and security breach attempts, collected from cloud platforms. Additionally, it features metadata for file storage, including encryption statuses and decryption

attempts, ensuring comprehensive analysis of the system's security features. The data is sourced from simulated environments, capturing real-time interactions to assess performance and robustness.

b) User Registration and Login:

User Registration: Users are required to register by providing their details, including username, password, contact, email, and address. The system checks if the username already exists in the database to avoid duplication. If the username is unique, the system stores the user's information in a MySQL database. After successful registration, the user is directed to the login page.

User Login: During the login process, the system verifies the user's credentials against the database. If the credentials match, an OTP is generated and sent to the registered email address. The user must input the OTP to gain access to the platform, ensuring an additional layer of security.

c) File Upload and Encryption:

File Upload: Once logged in, users can upload files by selecting the files through the provided web interface. The files are encrypted using the AES encryption algorithm. A unique key is generated using the ECDSA private key, which is used to encrypt the file data.

AES Encryption: The encryption process utilizes the AES-CTR (Counter mode) mode of operation. A secret key, derived from the ECDSA private key, is used to encrypt the uploaded file. This ensures the confidentiality of the file contents during transmission and storage.

File Storage: The encrypted files are then stored in the server's designated directory. Information about the uploaded file, including the file name, owner, access control list (ACL), and encryption key, is saved in the database.

d) File Download and Decryption:

File Download: Users can download encrypted files by selecting the file from the web interface. The system logs the user's download activity for auditing purposes. Upon download, the file is decrypted using the corresponding private key, and the user can access the original file.

AES Decryption: When a user requests to download an encrypted file, the system retrieves the corresponding encrypted file from the server and decrypts it using the private key. The private key is used in the AES decryption process to restore the original file content, ensuring the integrity and confidentiality of the file.

e) Log Management:

All user activities, including file uploads, downloads, and login attempts, are logged into a CSV file. This log captures critical details such as the username, action (upload, download, etc.), timestamp, and any errors encountered. This logging mechanism is essential for monitoring user actions and maintaining an audit trail for security purposes.

f) OTP Authentication:

The system employs OTP-based two-factor authentication (2FA) to enhance the security of the login process. After a user successfully logs in with their credentials, an OTP is generated and sent to the registered email address. The user must enter the OTP to complete the login process. If the entered OTP matches the one sent via email, the user gains access to the platform; otherwise, the login attempt is considered failed.

g) Key Management:

Key management is an essential part of the system. The private key used for AES encryption and decryption is generated using the ECDSA algorithm. If the key file is not present, a new key pair is generated and saved for future use. The system ensures that the private key is securely stored and used only for encryption and decryption purposes, minimizing the risk of unauthorized access.

h) Database Management:

The system uses a MySQL database to store user and file information. Each file uploaded is stored with metadata such as the file owner's name, filename, ACL, upload date, and the encryption key used. The database ensures efficient management and retrieval of file information. Additionally, the system allows access to files by querying the database for file names and keys, ensuring controlled access based on user permissions.

i) Security Considerations:

The system incorporates several security measures to protect sensitive data:

- AES encryption ensures that files are securely stored and transmitted.
- ECDSA key generation guarantees that only authorized users can decrypt files.
- OTP-based authentication adds an additional layer of security during the login process.
- Access control lists (ACLs) ensure that only authorized users have access to specific files.

4. EXPERIMENTAL RESULTS

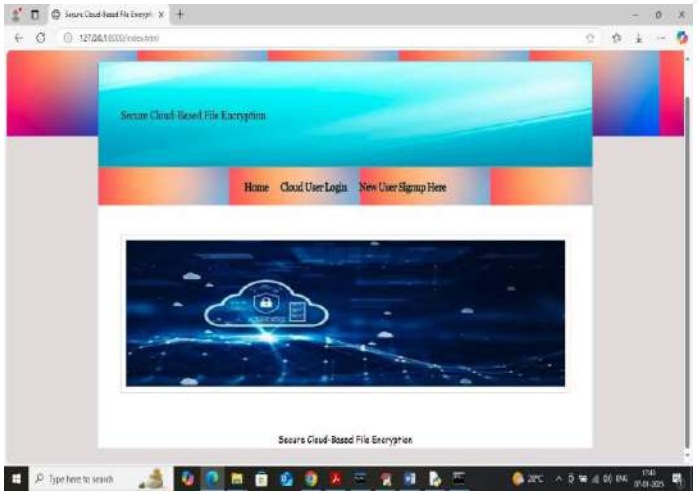

Fig.2 Home Page

Fig.3 Signup Page

Fig.4 Login Page

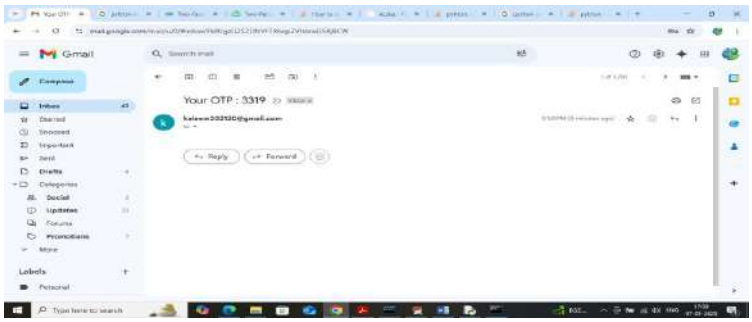

Fig.5 OTP Received to you Mail

Fig.6 MEA OTP Validation Screen

Fig.7 OTP Verified Successfully

Fig.8 Upload File to Cloud

Fig.9 Output Screen

Fig.10 Encrypted Information

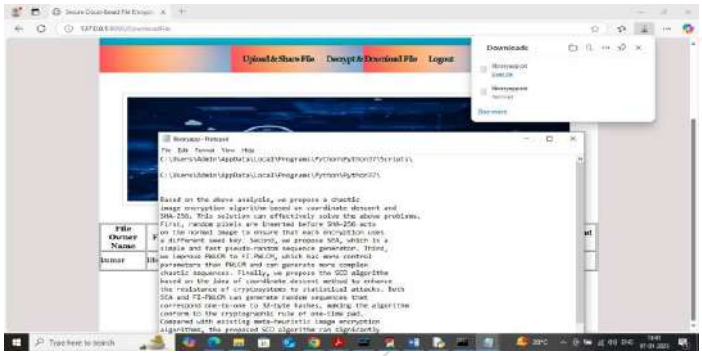

Fig.11 Download File

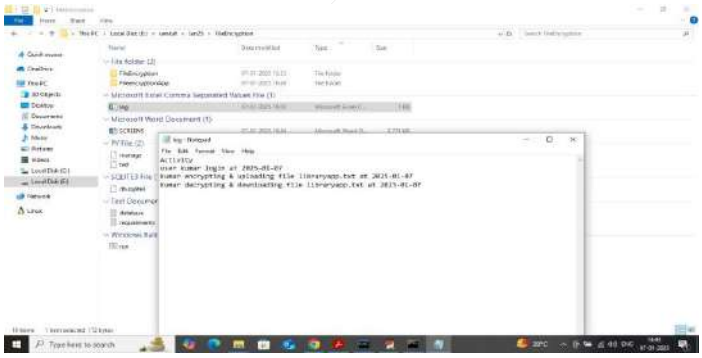

Fig.12 Activity Log

5. CONCLUSION

The Secure Cloud-Based File Encryption System represents a significant step forward in addressing the challenges of data security within cloud environments. By incorporating AES encryption, HMAC for data integrity, multi-factor authentication, and Access Control Lists (ACLs) for precise file sharing permissions, the system effectively

ensures the confidentiality, integrity, and availability of sensitive data. Audit logging further strengthens accountability, providing valuable insights into user actions. While the system successfully simulates cloud-like functionality with secure file handling and local server storage, its lack of direct integration with cloud platforms remains a limitation. Despite this, its modular design supports scalability, and its key management practices, including dynamic key rotation, offer a strong foundation for future development. The system's strengths in data protection, fine-grained access control, and transparency position it as a viable candidate for real-world cloud-based deployments. Looking ahead, integrating cloud platforms, enhancing the user interface, and improving mobile compatibility will unlock greater potential, positioning the system for wide adoption and contributing to the evolution of secure cloud technologies.

The ***future scope*** of the Secure Cloud-Based File Encryption System includes integrating with cloud storage platforms for true cloud-based functionality. Enhancements in encryption algorithms, such as post-quantum cryptography, and real-time collaboration features could further strengthen security and usability. Improving user authentication, compliance with regulatory standards, and mobile compatibility will expand its applicability across industries. Additionally, incorporating advanced machine learning algorithms for anomaly detection and predictive security features could enhance the system's ability to adapt to emerging threats in cloud environments.

REFERENCES

[1] Yashpal Kadam, "Security Issues in Cloud Computing A Transparent View", International Journal of Computer Science Emerging Technology, Vol-2 No 5 October, 2011 , 316-322

[2] Rohit Bhadauria, Rituparna Chaki, Nabendu Chaki, Sugata Sanyal, "A Survey on Security Issues in Cloud Computing", 2011

[3] Mladen A. Vouk, "Cloud Computing – Issues, Research and Implementations", Journal of Computing and Information Technology - CIT 16, 2008, 4, 235–246

[4] Ye Hu, Johnny Wong, Gabriel Iszlai, Marin Litoiu, "Resource Provisioning for Cloud Computing", IBM Canada Ltd., 2009

[5] Daniele Catteddu, Giles Hogben, "Cloud Computing:- Benefits, risks and recommendations for information security", November, 2009

[6] "Cloud Computing: Silver Lining or Storm Ahead?", Volume 13 Number 2, Spring 2010 [7] NGONGANG GUY MOLLET, "CLOUD COMPUTING SECURITY" , Thesis Paper, April 11, 2011

[8] Gunasekar Kumar, Anirudh Chelikani, "Analysis of security issues in cloud based e-learning", Master's thesis, 2011

[9] Jiyi Wu, Qianli Shen, Tong Wang, Ji Zhu, Jianlin Zhang "Recent Advances in Cloud Security", JOURNAL OF COMPUTERS, VOL. 6, NO. 10, OCTOBER 2011

[10] Ahmad-Reza Sadeghi, Thomas Schneider, and Marcel Winandy, "Token - Based Cloud Computing Secure Outsourcing of Data and Arbitrary Computations with Lower Latency", TRUST 2010, LNCS6101, pp . 417–429, 2010.

[11] Hongwei Li, Yuanshun Dai, Ling Tian and Haomiao Yang, "Identity Based Authentication for Cloud Computing", CloudCom 2009, LNCS 5931, pp. 157–166, 2009

[12] Joan Daemen, Vincent Rijmen, "Announcing the ADVANCED ENCRYPTION STANDARD (AES)", Federal Information Processing Standards Publication 197, November 26, 2001

[13] "PERFORMANCE EVALUATION OF PACKET DROPS IN WIRELESS INFRASTRUCTURE LESS NETWORKS", *IJMEC*, vol. 9, no. 2, pp. 40–55, Feb. 2024, Accessed: Jan. 15, 2025. [Online]. Available: https://ijmec.com/index.php/multidisciplinary/article/view/423