Cloud-Based Secure File Storage Using Hybrid Cryptography

Mrs. Supriya M [2] D K Chandana[1]

[2]*Assistant Professor, Department of MCA, BIET, Davanagere*

[1]*Student,4th Semester MCA, Department of MCA, BIET, Davanagere*

ABSTRACT:

In the era of pervasive cloud computing, ensuring the security and confidentiality of sensitive data stored on cloud platforms is a critical challenge. This paper proposes a "Cloud-Based Secure File Storage Using Hybrid Cryptography" system that leverages a novel hybrid encryption approach, combining symmetric and asymmetric cryptographic algorithms, to provide robust and efficient data protection. The proposed methodology involves dividing files into multiple segments, encrypting each segment with rotating encryption algorithms, and securing encryption keys through an additional encryption layer. This multi-layered security architecture significantly mitigates the risks of unauthorized access and data breaches, ensuring only authorized users can retrieve and decrypt stored files. The system also offers comprehensive administrative and user functionalities, including secure file upload, retrieval, and an integrated support FAQ, thereby enhancing both security and usability for cloud-based file storage.

Keywords: Cloud Security, Hybrid Cryptography, File Encryption, Data Confidentiality, Symmetric Encryption, Asymmetric Encryption, Secure Cloud Storage, Key Management, Data Integrity

I. INTRODUCTION

In recent years, cloud computing has revolutionized the way individuals and organizations store, manage, and access data. The cloud offers scalable storage solutions, cost efficiency, and ubiquitous accessibility, making it an indispensable component of modern IT infrastructure. However, the convenience of cloud storage comes with significant security concerns, especially regarding the confidentiality, integrity, and availability of sensitive data. With the increasing migration of critical information to cloud platforms, ensuring robust data security has become paramount to prevent unauthorized access, data breaches, and potential misuse.

Cloud environments are inherently vulnerable to various cyber threats such as hacking, insider attacks, data leakage, and denial-of-service attacks. These vulnerabilities are exacerbated by the multi-tenant nature of cloud infrastructure, where multiple users share physical resources, increasing the risk of data exposure. Moreover, regulatory frameworks such as GDPR, HIPAA, and others impose stringent requirements on data privacy and protection, compelling cloud service providers and users to adopt advanced security mechanisms. Traditional security measures such as access control and firewalls, while necessary, are insufficient to address the complex threat landscape faced by cloud storage systems.

Encryption stands out as one of the most effective techniques to secure data in the cloud. By transforming data into an unreadable format, encryption ensures that even if unauthorized users gain access to stored files, they cannot interpret the content without the appropriate decryption keys. However, the choice of encryption algorithms and key management strategies significantly impacts the security and performance of cloud storage systems. Symmetric encryption algorithms, such as AES (Advanced Encryption Standard), are computationally efficient and suitable for encrypting large volumes of data but require secure key distribution. Conversely, asymmetric encryption algorithms, such as RSA (Rivest-Shamir-Adleman), facilitate secure key exchange but are computationally intensive and less suitable for bulk data encryption.

To leverage the advantages of both symmetric and asymmetric encryption while mitigating their individual limitations, hybrid cryptography has emerged as a promising solution. Hybrid cryptography combines the speed and efficiency of symmetric encryption for data encryption with the secure key exchange capabilities of asymmetric encryption. This approach enhances overall system security and performance, making it highly suitable for cloud-based secure file storage.

This paper proposes a novel cloud-based secure file storage system utilizing hybrid cryptography to protect sensitive data stored on cloud servers. The system divides files into multiple parts and encrypts each segment using different symmetric algorithms in a rotating manner, thereby increasing the complexity for potential attackers. The encryption keys themselves are further protected using asymmetric encryption, adding an additional layer of security. This multi-layered encryption strategy ensures that even if one encryption layer is compromised, the data remains protected.

Furthermore, the system incorporates robust key management mechanisms that restrict access to authorized users only, ensuring secure file upload, storage, and retrieval processes. Administrators have comprehensive control over user management and support through features such as user registration oversight and an FAQ section to assist users. This combination of security, usability, and administrative control makes the proposed system a reliable platform for secure cloud storage.

In summary, the proposed hybrid cryptography-based cloud storage system addresses the critical challenges of data confidentiality, integrity, and access control in cloud environments. By integrating multiple encryption techniques and secure key management, it offers a scalable and efficient solution that mitigates the risks associated with cloud data storage. The following sections of this paper detail the system architecture, encryption methodology, implementation, and performance evaluation, demonstrating the effectiveness of the proposed approach in enhancing cloud data security.

II.RELATED WORK

CLOUD BASED SECURE FILES STORAGE USING HYBRID CRYPTOGRAPHY, Authors- Rakshitha Gaikwad N, Cloud computing has transformed data storage by offering unparalleled scalability, accessibility, and cost-efficiency, but it also raises significant concerns about data security and privacy. This paper explores the use of hybrid cryptography—an approach that combines symmetric and asymmetric encryption—to enhance the protection of sensitive files stored in the cloud. By leveraging the speed of symmetric algorithms for data encryption and the secure key management of asymmetric techniques, hybrid cryptography strengthens defenses against unauthorized access and cyber threats. Through a detailed examination of its principles and implementation, the paper demonstrates that hybrid cryptography is an effective strategy for safeguarding critical information in modern cloud environments.[1]

Secure File Storage on Cloud using Hybrid Cryptography, Authors- Aditya Poduval, Abhijeet Doke, Hitesh Nemade, Rohan Nikam , This paper presents a novel security mechanism for cloud data storage that combines multiple symmetric cryptographic algorithms with steganography to enhance data protection. The proposed system splits files into three parts, encrypts each part using AES, 3DES, and RC6 algorithms with 128-bit keys, and utilizes multithreading for simultaneous encryption. Key information—including the encryption algorithm and key used for each part—is securely embedded within an image using the LSB steganography technique. This integrated approach ensures robust security for cloud-stored data by leveraging the strengths of both advanced encryption and steganographic methods.[2]

Secure File Storage on Cloud Using Hybrid Cryptography, Authors- Brundashree, Hangsha Subba, Gautam, Prof.Kavya V, Abdul Mujeeb, This paper introduces a hybrid cryptographic system for secure cloud storage that combines AES and RSA encryption to address ongoing security concerns such as unauthorized access and data breaches. By employing adaptive key management and data dispersal strategies, the system ensures data confidentiality, integrity, and accessibility. Performance evaluations demonstrate that the proposed approach effectively protects sensitive information in the cloud while maintaining high computational efficiency.[3]

Secure file storage using hybrid cryptography, Author- Vaishnavee, Fathima, Dr. S. Latha3, This study proposes a comprehensive secure file storage system that leverages hybrid cryptography by combining multiple symmetric algorithms (AES, Fernet, ChaCha20) and an asymmetric algorithm for key security. Files are split into three segments, each encrypted with a different symmetric method, while keys are derived using Argon2 and digitally signed with ECDSA. All encrypted segments, keys, and signatures are stored in a password-protected zip file with strict access controls, ensuring that only authorized users can access the data. This approach delivers robust security by providing confidentiality, integrity, authentication, access control, and non-repudiation for sensitive information.[4]

Secure File Storage in Cloud Using Hybrid Encryption, Authors- Kiran Kurian, Lekshmi S Nair, Rinu Maria Jose, Rosa Mariam John, This project introduces a new security model for cloud data storage using hybrid cryptography, addressing vulnerabilities such as unauthorized access and integrity violations. By integrating RSA for secure data transfer and AES for encrypted file management, the system ensures robust protection of user data in cloud environments. The approach leverages the efficiency and security advantages of both algorithms, providing enhanced safety for cloud-based applications and services.[5]

Secure File Storage Using AES & RSA Algorithm in Cloud Computing, Authors-JEGANATHAN C, ANIRUDHAN N.H, ATHUL ROHAN P, SONU A, This paper proposes a secure file storage system leveraging hybrid cryptography—combining AES and RSA algorithms—to address the growing need for robust data protection in cloud computing. The system offers a user-friendly web portal for uploading files, which are encrypted using both AES and RSA before being stored in the cloud. Users can easily retrieve and decrypt their files through the portal, ensuring secure and efficient access. This approach enhances data confidentiality and security, providing a practical solution for safeguarding sensitive information in today's digital landscape.[6]

Secure File Storage using Hybrid Cryptography, Authors: S. Gokulraj, P. Ananthi, R. Baby, and E. Janani (Velalar College of Engineering & Technology, India). This project enhances cloud data security by employing hybrid cryptography, combining AES, DES, and RSA to encrypt different sections of user-uploaded data. Keys for each encryption are securely hidden within an image using LSB steganography. The encrypted data segments are stored in the cloud, and users must extract the keys from the image to decrypt their files. This multi-layered approach significantly strengthens protection against key leaks and unauthorized access, offering a more robust solution than using a single encryption method.[7]

Secure File Storage Using Hybrid Cryptography in Cloud Computing, Authors: S. Saxena & M. Verma, This work addresses cloud data security by implementing hybrid encryption, combining AES in CTR and CCM modes to ensure both confidentiality and authenticity of data stored in the cloud. The encrypted files are divided into multiple parts and distributed across different database tables, further enhancing protection against external threats and attacks. Experimental analysis demonstrates that this approach effectively strengthens the security and efficiency of cloud storage services.[8]

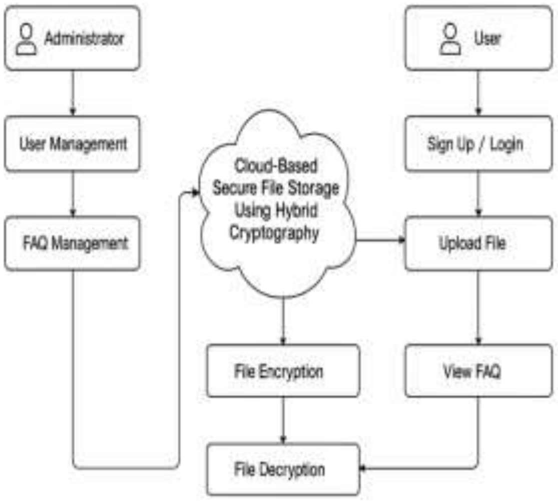
SECURE FILE STORAGE ON CLOUD USING HYBRID CRYPTOGRAPHY, Authors- P. Oliva Joicy, V. Prathyusha, M. Rekha, Dr. Swapna, The proposed model enhances cloud data security by using a hybrid encryption approach that combines AES, DES, and RSA to efficiently encrypt file slices, ensuring high throughput and minimal processing time. By splitting and merging data, the system strengthens security and access control, addressing privacy concerns and increasing user trust in cloud services. Only authorized users can decrypt the ciphertext, ensuring that sensitive information remains protected even though encrypted data is visible on the cloud server.[9]

Secure File Storage & Sharing on Cloud Using Cryptography, Authors- Madhumala RB, Sujan Chhetri, Akshatha KC, Hitesh Jain, This paper proposes a secure file transfer and storage system that uses cryptography to protect sensitive business data on the cloud. The application ensures that all user files are encrypted before storage, preventing unauthorized access, manipulation, or deletion by attackers. It features secure user authentication, allows users to encrypt and decrypt files without altering their size, and restricts file access and modification rights exclusively to the owner. Additionally, the system provides a secure chat platform for user communication, further enhancing data privacy and security.[10]

III. METHODOLOG

Proposed Methodology

The proposed methodology for "Cloud-Based Secure File Storage Using Hybrid Cryptography" integrates both symmetric and asymmetric encryption techniques to maximize data security and efficiency. The process is structured in distinct phases for encryption, storage, and decryption, as detailed below:



Fig_no3.1. Proposed Methodology

1. User Registration and Authentication

Users begin by registering on the platform, providing necessary credentials and contact information. Upon registration, users authenticate themselves through a secure login process. Robust authentication mechanisms ensure that only authorized users gain access to the file storage system.

2. File Upload and Segmentation

Once authenticated, users can upload files to the cloud storage platform. Each uploaded file is automatically divided into multiple segments or chunks. This segmentation enhances security by ensuring that no single segment contains the entire file content, making unauthorized reconstruction more difficult.

3. Hybrid Encryption of File Segments

Each file segment is encrypted using a different symmetric encryption algorithm (such as AES, DES, or Blowfish) in a rotating or randomized manner. This multi-algorithm approach leverages the speed of symmetric cryptography while increasing cryptographic complexity. The symmetric keys used for each segment are unique and generated per upload session.

4. Asymmetric Encryption of Symmetric Keys

To secure the symmetric keys, each key is encrypted using an asymmetric encryption algorithm (e.g., RSA). The user's public key is used for this encryption, ensuring that only the intended user, possessing the corresponding private key, can decrypt and access the symmetric keys required for file decryption.

5. Secure Cloud Storage

The encrypted file segments and their corresponding encrypted symmetric keys are uploaded and stored on the cloud server. Metadata linking segments to their keys and user accounts is maintained in a secure, access-controlled database.

6. File Retrieval and Decryption

When a user requests to download a file, the system retrieves the relevant encrypted segments and their encrypted symmetric keys. The user's private key is used to decrypt the symmetric keys. Each segment is then decrypted using its respective symmetric key and algorithm. The original file is reconstructed by merging the decrypted segments.

7. Key Management and Access Control

All key management operations, including key generation, encryption, and storage, are handled securely within the platform. Access to files and keys is strictly controlled through user authentication and authorization checks, ensuring that only legitimate users can retrieve and decrypt their files.

8. Administrator and User Support Features

Administrators can manage user accounts, monitor system activity, and maintain an FAQ section to assist users. The user interface, typically implemented as a web application (e.g., using Flask or Django), allows users to upload/download files, view FAQs, and manage their accounts efficiently.

IV. TECHNOLOGIES USED

1. Python

Python is a versatile, high-level programming language that supports a wide ecosystem of libraries and frameworks, making it a leading choice for data analysis, scientific computing, machine learning, and web development. Libraries such as Pandas and NumPy are especially popular in Python: Pandas provides powerful and flexible data structures like DataFrames for easy manipulation, cleaning, and analysis of structured data, while NumPy offers efficient operations on large, multi-dimensional arrays and matrices, serving as the computational backbone for many scientific and analytical tasks. Python's extensive standard library, clear syntax, and strong community support further enhance its appeal across a wide range of applications, from prototyping to production-level systems

2.cryptography.fernet

`cryptography. fernet` is a module within the Python `cryptography` library that provides symmetric encryption and decryption using the Fernet specification. Fernet guarantees that a message encrypted using it cannot be manipulated or read without the key. It uses AES in CBC mode with a 128-bit key for encryption and HMAC using SHA256 for authentication, ensuring both confidentiality and integrity of the data. Fernet is designed to be easy to use and secure by default, making it a popular choice for encrypting sensitive data in Python applications.

3.**cryptography.hazmat.primitives.ciphers.aead** The cryptography.hazmat.primitives.ciphers.aead module offers implementations of Authenticated Encryption with Associated Data (AEAD) ciphers, such as AES-GCM and ChaCha20-Poly1305. AEAD ciphers provide both encryption and authentication in a single step, ensuring that the data is not only confidential but also protected against tampering. These ciphers are widely used in modern cryptographic protocols and are recommended for scenarios where both security and performance are critical.

4.**cryptography.hazmat.backends.default_backend**

Thecryptography.hazmat.backends.default_backend is a function in the Python `cryptography` library that returns the default cryptographic backend for the current platform. This backend provides the underlying implementation for various cryptographic primitives, such as ciphers, hashes, and key storage. By using the default backend, developers can leverage a well-tested, secure, and performant foundation for cryptographic operations without needing to configure or select specific backend libraries manually[5][6]. This abstraction simplifies development and ensures compatibility across different environments.

5.**cryptography.hazmat.primitives.asymmetric.rsa**The cryptography.hazmat.primitives.asymmetric. rsa` module provides tools for implementing RSA (Rivest-Shamir-Adleman) asymmetric encryption and digital signatures in Python. RSA is a widely used public-key cryptosystem that enables secure key exchange, encryption, and authentication. This module supports key generation, encryption and decryption, as well as signing and verifying messages, making it a fundamental component for secure communication and key management in cryptographic applications.

V Result:

Encrypt file

User can upload and encrypt file here.

Decrypt file

User can decrypt file here

VI. CONCLUSION

The proposed cloud-based secure file storage system using hybrid cryptography effectively addresses the critical challenges of data confidentiality, integrity, and secure key management in cloud environments. By combining the efficiency of symmetric encryption algorithms with the robust key protection provided by asymmetric encryption, the system ensures multi-layered security for sensitive files stored on the cloud. The segmentation of files and the rotation of encryption algorithms further enhance resistance against unauthorized access and cryptanalysis. Additionally, the integration of secure user authentication and comprehensive administrative controls contributes to a reliable and user-friendly platform. Overall, this hybrid cryptographic approach offers a scalable, efficient, and highly secure solution for safeguarding cloud-stored data, thereby fostering greater trust and adoption of cloud services in sensitive and critical applications.

REFERENCES

1. Cloud based secure files storage using hybrid cryptography, Authors- Rakshitha Gaikwad N, Publisher- International Research Journal of Modernization in Engineering Technology and Science, e-ISSN: 2582-5208, Volume:06/Issue:06/June-2024

2. Secure File Storage on Cloud using Hybrid Cryptography, Authors- Aditya Poduval, Abhijeet Doke, Hitesh Nemade, Rohan Nikam, Publisher- International Journal of Computer Sciences and Engineering,Vol.-7, Issue-1, Jan 2019 E-ISSN: 2347-2693

3. Secure File Storage on Cloud Using Hybrid Cryptography, Authors- Brundashree, Hangsha Subba, Gautam, Prof.Kavya V, Abdul Mujeeb, Publisher- International Journal on Science and Technology (IJSAT), E-ISSN: 2229-7677, Website: www.ijsat.org

4. Secure file storage using hybrid cryptography, Author- Vaishnavee, Fathima, Dr. S. Latha3, Publisher- IJCRT , 2023 IJCRT | Volume 11, Issue 5 May 2023 | ISSN: 2320-2882

5. Secure File Storage in Cloud Using Hybrid Encryption, Authors- Kiran Kurian, Lekshmi S Nair, Rinu Maria Jose, Rosa Mariam John, publisher- International Journal of Engineering Research & Technology (IJERT), NCASCD – 2023

6. Secure File Storage Using AES & RSA Algorithm in Cloud Computing, Authors- JEGANATHAN C, ANIRUDHAN N.H, ATHUL ROHAN P, SONU A ,Publisher-2024 JETIR March 2024, Volume 11, Issue 3 www.jetir.org(ISSN-2349-5162)

7. Secure File Storage using Hybrid Cryptography, Authors: S. Gokulraj, P. Ananthi, R. Baby, and E. Janani (Velalar College of Engineering & Technology, India), Publisher: SSRN (Social Science Research Network), Posted: April 2, 2021 (written March 11, 2021), DOI:10.2139/ssrn.3802668

8. Secure File Storage Using Hybrid Cryptography in Cloud Computing, Authors: S. Saxena & M. Verma, Published in: 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), held in 2016, organized by IEEE, Publication: IEEE Xplore conference proceedings

9. SECURE FILE STORAGE ON CLOUD USING HYBRID CRYPTOGRAPHY, Authors- P. Oliva Joicy, V. Prathyusha, M. Rekha, Dr. Swapna, Publisher- International Journal for innovative Engineering and Mangagement Research, Vol11 Issue 06, April 2022 ISSN 2456 – 5083

10. Secure File Storage & Sharing on Cloud Using Cryptography, Authors- Madhumala RB, Sujan Chhetri, Akshatha KC, Hitesh Jain, Publisher- International Journal of Computer Science and Mobile Computing, ISSN 2320–088X IJCSMC, Vol. 10, Issue. 5, May 2021.