www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

SECURE MULTI-MODAL FILE STORAGE ARCHITECTURE UTILIZING HYBRID CRYPTOGRAPHIC ALGORITHMS FOR ENHANCED DATA PROTECTION

[1]Mrs.KANAKANDLA VASUDHA,[2]ANAGANTI LIKITHA,[3] BHUKYA SAI CHANDU,[4] BURAM SRIJITH

[1]ASSISTANT PROFESSOR),CSE, TEEGALA KRISHNA REDDY ENGINEERING COLLEGE.

[2345]B.TECH. SCHOLAR, CSE, TEEGALA KRISHNA REDDY ENGINEERING COLLEGE.

ABSTRACT

Security is a major concern in a wide range of applications, from cloud storage to messaging platforms. Various approaches have been proposed to ensure data protection in the cloud, such as the use of AES (Advanced Encryption Standard). However, existing systems often fall short when relying solely on a single form of encryption like AES, especially when adapted to specific user requirements. A major limitation of this scheme is that each encryption operation depends on encryption keys—if these keys are compromised, the entire dataset becomes vulnerable. Therefore, a more secure solution is required.In this project, hybrid cryptography is employed, combining traditional encryption techniques with AES to enhance security. When a user uploads data, it is encrypted using AES. To retrieve the data, users must first extract the encryption keys, which are then used to decrypt the AES-encrypted content. This approach significantly strengthens data security by introducing an additional layer of protection.

Index Terms — Data Security, AES Encryption, Hybrid Cryptography, Cloud Storage, Key Management, Data Protection, Secure Data Retrieval, Encryption Keys.

1.INTRODUCTION

1.1 PROBLEM STATEMENT:

Today, cloud-based platforms are becoming more popular when it comes to file storage because they are easier to use and scale. However, this growing dependence is also causing serious security issues. Traditional file storage systems—whether on-premises or through the cloud—struggle to guarantee confidentiality, secure access, and data or integrity. Furthermore, they tend to utilize either symmetric or asymmetric cryptography in isolation, which brings its own problems.

Symmetric encryption offers swift processing of large files but does not distribute secret keys

securely. On the other hand, while asymmetric encryption exchanges control over the keys safely, it uses a lot of computational power to encrypt large amounts of data.

In addition, most users are unable to control their encryption keys, which makes sensitive data more susceptible to leaks. Most of these solutions also lack multi-factor authentication, role-based access controls, and integrity verification through hashing, which adds to their unreliability when defending users against advanced threats.

What's clear is that there isn't a reliable full-comprehensive file storage solution available. With advanced asymmetric encryption combined with symmetric cryptographic approaches, it would be possible to develop a more secure piece of technology to defend sophisticated cyber threats while ensuring regulatory compliance.

To guarantee end-to-end protection of sensitive data, user-centric access mechanisms and secure key storage are also necessary. By creating a safe cloud storage solution, controlled key management, encrypted file upload, secure decryption, and secure retrieval, this project seeks to close these important gaps while preserving data integrity and thwarting unwanted access.

1.2 DESCRIPTION:

The goal of this project, "Secure Multi-Modal File Storage Architecture Utilizing Hybrid Cryptographic Algorithms for Enhanced Data Protection," is to offer a very effective and safe way to store and retrieve files via cloud-based platforms. In a world where data breaches are frequent and cyber threats are becoming more complex; it responds to the growing need for data privacy and protection.

The system employs a hybrid cryptographic technique, combining asymmetric encryption (like ECC) for safe key exchange with symmetric encryption (like AES) for quick and effective file encryption. Performance and strong security are guaranteed by this combination. Modules for user authentication, file encryption and decryption, key generation and storage, and cloud-based file storage and retrieval are all included in the project.

Files uploaded by users are encrypted using the hybrid algorithm. The cloud securely manages and stores the encryption keys. Confidentiality and data integrity are maintained throughout the process by allowing authorized users to access and decrypt their files when necessary, using the appropriate keys.

Multi-factor authentication, hash-based file integrity verification, and role-based access control are additional security features that make the platform scalable and user-centric in addition to being secure. All things considered, this project offers a workable and trustworthy answer to the problems relating to key management and safe cloud file storage.

2.LITERATURE SURVEY

There is now more emphasis on protecting sensitive data from cyber threats and unauthorized access because of our growing reliance on cloud computing and online data storage services. Using a variety of cryptographic techniques, numerous studies and systems have been proposed to address these issues. However, performance and security are frequently traded off in current solutions, particularly when handling massive data transmission and storage.

1. File storage systems with symmetric encryption

AES (Advanced Encryption Standard) and other symmetric encryption methods are popular because of how quickly and effectively they can encrypt vast amounts of data. AES is a strong block cipher encryption standard that is still very effective for file-level security, according to research by Daemen and Rijmen (2002). However, the difficulty of secure keys is a significant disadvantage distribution, since total data exposure may result from any key compromise.

2. Asymmetric Key Exchange Encryption

Asymmetric encryption techniques like RSA and Elliptic Curve Cryptography (ECC) have been employed for secure key exchange to solve problems with key distribution. Because of its strength-per-key-bit advantage over RSA, ECC has drawn attention and is appropriate for cloud and mobile environments. According to research by Koblitz and Menezes (1998), asymmetric algorithms are computationally costly and unfeasible for directly encrypting large amounts of data.

3. Models of Hybrid Cryptography

The necessity of hybrid cryptographic systems that combine the secure key exchange capabilities of asymmetric cryptography with the effectiveness of symmetric encryption has been highlighted by several recent studies. For example, a Patil et al. (2019) model showed how to use AES and RSA in a hybrid approach to improve security and performance. However,

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

RSA has more overhead than ECC, particularly in settings with limited resources.

4. Safe Key Storage and Management

The significance of strong key management frameworks is also emphasized in the literature. Although enterprise-level security systems such as KMIP (Key Management Interoperability Protocol) have been proposed, they are frequently complicated and unsuitable for environments that are lightweight and user-controlled. Since careless handling can render even the strongest encryption ineffective, secure key storage—particularly in the cloud—remains a major area of research interest.

5. Access Control and Cloud Storage

While existing solutions such as AWS S3, Dropbox, and Google Cloud Storage offer basic encryption features, they typically lack fine-grained access control and user-controlled encryption mechanisms. Scholarly research supports the integration of to improve security, use multi-factor authentication (MFA) and role-based access control (RBAC). RBAC and encryption together can greatly lower unwanted access to cloud storage systems, according to Zhang et al. (2020).

3.SYSTEM ANALYSIS

3.1 EXISTING SYSTEM:

File storage systems nowadays mostly depend on local storage methods or traditional cloud-based solutions. Even though these systems are accessible and convenient, they frequently don't provide complete security against contemporary cyberthreats. Current systems usually use either symmetric or asymmetric cryptographic methods, but not both, which results in performance and security issues.

Drawbacks:

- Lack of user-controlled encryption keys.
- Limited scalability and accessibility.
- Lack of Hybrid Cryptography.

3.2 PROPOSED SYSTEM:

In order to overcome the shortcomings of current systems, the suggested system offers a safe file storage platform that makes use of hybrid cryptography. High performance and strong security are guaranteed by the system's combination of symmetric and asymmetric encryption techniques. Large files can be efficiently encrypted using symmetric encryption (like AES), and encryption keys can be safely

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

exchanged using asymmetric encryption (like ECC). The platform incorporates cutting-edge features like role-based access control to prevent unwanted access, hashing algorithms for file integrity verification, and multi-factor authentication to further improve security.

Advantages:

- High Accuracy
- High Efficiency
- Enhanced Security
- Convenience
- Cost Effective
- Improved User Acceptance

4.SYSTEM DESIGN

4.1 SYSTEM ARCHITECTURE

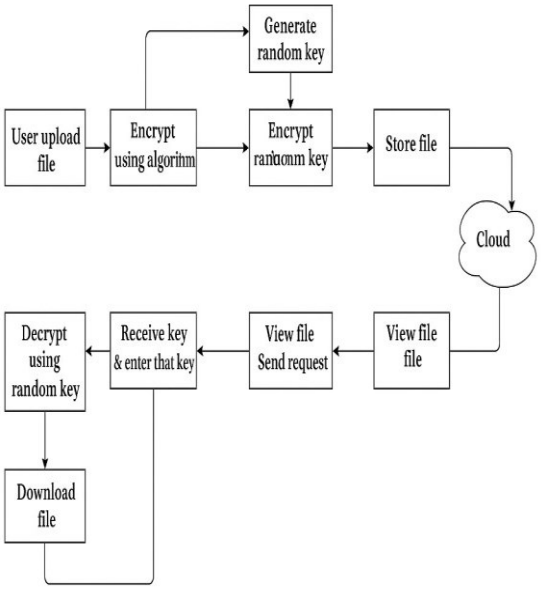

Fig 4.1: System Architecture

The system architecture is designed to ensure Secure file storage and retrieval using a Hybrid cryptographic model that combines symmetric and asymmetric encryption techniques. It is modular in nature, promoting scalability, maintainability, and layered security. The architecture is divided into several key components, each responsible for specific functionality in the secure file lifecycle — from user authentication to encryption, cloud storage, and decryption.

5.IMPLEMENTATION

5.1 OVERVIEW

1. User Module:

Index in Cosmos
MAY 2025, Volume 15, ISSUE 2
UGC Approved Journal

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

Major Sub-Modules:

Authentication Module – Handles secure user login and registration.

File Upload & Encryption Module – Manages file upload, encryption.

File Decryption & Download Module – Facilitates key upload, file decryption, and download.

Functionality:

Enables users to securely upload, encrypt, store, decrypt, and download files using hybrid cryptography.

2. File Upload Module:

Major Sub-Modules:

File Selection Interface – Allow users to select and upload a file from their device.

File Validation Module – Check file type, size, and integrity before upload.

Encryption Handler – Encrypt the uploaded file securely using hybrid cryptography.

Functionality:

Securely manages user file uploads by validating, encrypting, and preparing files for safe storage.

3. File Encrypt and Decrypt Module:

Sub-modules:

Key Management Module — Handles the generation and management of random and algorithmic encryption keys.

Encryption Module — Encrypts the file data either using random keys or standard cryptographic algorithms.

Decryption Module — Decrypts the stored/encrypted files using the appropriate key or algorithm.

Functionality:

Securely encrypts files before cloud storage and decrypts them upon retrieval using a combination of random key generation and encryption algorithms.

4. Cloud Storage Module:

Sub-modules:

File Upload Module — Handles storing encrypted files securely in the cloud.

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

File Retrieval Module — Fetches encrypted files from the cloud storage upon user request.

Key Storage Module — Stores and manages encryption keys securely for future decryption.

Functionality:

Securely stores encrypted files and their encryption keys in the cloud and retrieves them for authorized decryption and access.

6. OUTPUT SCREENS

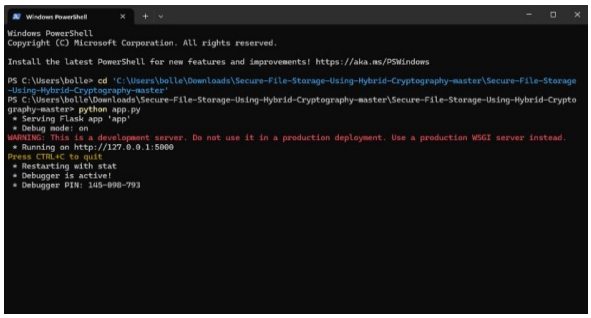

Fig 6.1 Running the backend server and testing the initial APIs

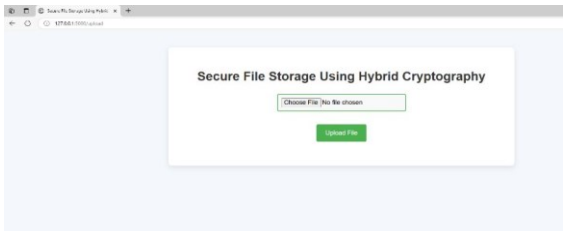

Fig 6.2 Uploading a file

Fig 6.3 Successfully uploaded the file

Fig 6.4 Downloaded the key that is provided for encryption and decryption

Fig 6.5 Back to the home page, now click the restore for restoring the uploaded file

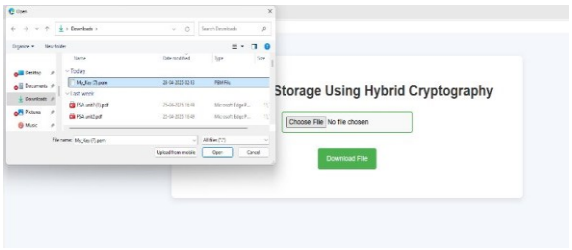

Fig 6.6 Previous downloaded key is uploaded and click the download file

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

Fig 6.7 Downloaded the encrypted file successfully

7. CONCLUSION

One of the most urgent issues in cloud computing, data security and confidentiality, is fully addressed by the project "Secure Multi-Modal File Storage Architecture Utilizing Hybrid Cryptographic Algorithms for Enhanced Data Protection." This system guarantees that users can safely store, access, and manage sensitive data in a time when cloud storage is essential and digital transformation is pervasive.

The project creates a hybrid cryptographic model that strikes a balance between performance and robust security by utilizing the advantages of both symmetric (AES) and asymmetric (ECC) encryption algorithms. While ECC secures the symmetric keys without sacrificing computational efficiency, AES offers high-speed encryption for large files. Without both encryption layers and the right credentials, this dual-layered protection makes it nearly impossible for unauthorized individuals to access cloud data, even if it is compromised.

Through features like multi-factor authentication, hash-based integrity verification, and role-based access control, the system also places a high priority on user control and trust. Together, these features guarantee that only authorized users can access data and that any corruption or change to stored files is quickly identified. Additionally, the architecture encourages scalability and modularity, facilitating future growth and integration with more extensive enterprise systems.

The project illustrates how sensitive data can be safely stored and easily retrieved by using secure key handling, cloud-based encrypted file storage, and trustworthy decryption and integrity checks upon retrieval. It solves a problem that many current systems are unable to successfully handle: the gap between robust cryptographic enforcement and user usability.

Additionally, the project creates a basic framework that can be expanded to more specialized fields where confidentiality, integrity, and compliance are crucial, like

government communications, financial data, legal documentation, and medical records. Wider future applicability is made possible by its architecture, which also opens the door for integration with distributed ledgers, AI-based monitoring, and regulatory compliance modules.

In conclusion, the project's successful completion not only confirms that hybrid encryption is feasible in cloud settings, but it also emphasizes how crucial user-driven control and layered security are to protecting digital assets. This system could be used as a model for institutional and industrial deployment and establishes a standard for future research and development in secure cloud storage.

8.FUTURE ENHANCEMENT

In future developments, this hybrid cryptographic system can be extended to support multi-factor authentication and dynamic key generation mechanisms to further reduce the risk of key compromise. Integrating blockchain technology for decentralized key management could enhance transparency and trust. Additionally, real-time intrusion detection systems (IDS) could be implemented to monitor unauthorized access attempts. Enhancing user interface design and scalability for large-scale cloud environments will also improve usability and performance. Support for mobile platforms and cross-platform compatibility can make the system more accessible and practical in diverse user scenarios.

9. REFERENCES

[1] Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th Edition). Pearson Education.

[2] Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of Applied Cryptography. CRC Press.

[3] NIST. (2001). Announcing the Advanced Encryption Standard (AES). FIPS PUB 197. U.S. Department of Commerce.https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

[4] Hankerson, D., Vanstone, S., & Menezes, A. (2004). Guide to Elliptic Curve Cryptography. Springer.

[5] Wang, C., Wang, Q., Ren, K., Cao, N., & Lou, W. (2012). Toward Secure and Dependable Storage Services in Cloud

Computing. IEEE Transactions on Services Computing, 5(2), 220–232.https://doi.org/10.1109/TSC.2011.35

[6] Zhou, Z., & Huang, D. (2013). Efficient and Secure Data Storage Operations for Mobile Cloud Computing. In Proceedings of the 8th International Conference on Network and Service Management (pp. 37–45). IEEE.