Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 44 No. 4 (2023)

Optimizing the Application of Hybrid Cryptographic Methods for Secure File Storage and Retrieval

[1] Chandrakala B M, [2]Latha A P, [3]B.V. Shruti
[1]Associate Professor, Department of Information science and Engineering, Dayananda Sagar College of Engineering, Shavige Malleshwara hills, Kumaraswamy Layout, Bangalore -560078.
[2]Assistant Professor, Department of Information science and Engineering, Dayananda Sagar College of Engineering, Shavige Malleshwara hills, Kumaraswamy layout, Bangalore -560078.
[3]Associate Professor, Department of Computer Science and Engineering, Nitte Meenakshi Institute of Technology,
Bangalore -560064

*Corresponding author E-mail: chandrakalabm-ise@dayanandasagar.edu

Abstract: In the modern digital era, the protection of sensitive data from unauthorized access is of utmost importance. A key concern in this regard is secure file storage. To address this issue, hybrid cryptography offers a viable solution by combining the strengths of various encryption techniques in both a vertical and horizontal manner. In hybrid cryptography, the original symmetric key is encrypted with a different symmetric key, while the actual data is encrypted using yet another symmetric key. This approach allows for quick and efficient encryption and decryption of the data, while also providing the added security of multiple encryption methods for authentication. By employing hybrid cryptography, organizations can ensure the securestorage of their critical data, safeguarding it against unauthorized access and potential data breaches.
Keywords: Hybrid cryptography, encryption, decryption, Protection, vulnerabilities, file storage.

1. Introduction

The instances of security breaches have been increasing exponentially. Some security breaches compel enterprises to disable their websites and mobile apps temporarily, whereas others make companies lose a significant percentage of their annual turnover. Secure file storage is essential for businesses to effectively manage their data. The potential consequences of a data breach, such as financial loss, legal liabilities, and damage to the organization's reputation, underscore the importance of safeguarding sensitive information from unauthorized access and tampering. Hybrid cryptography is an approach that combines multiple encryption methods to enhance file storage security. In hybrid cryptography, files are divided into multiple parts, each encrypted using different encryption techniques. This method complicates the decryption process for attackers, as they would need to reverse several encryption techniques instead of just one, making it more difficult for them to access the file's contents. By employing multiple encryption techniques, the security of stored files is significantly enhanced. Hybrid cryptography finds applications in various sectors, including the military, healthcare, and financial industries, where the secure preservation of sensitive data is paramount. The utilization of hybrid cryptography for secure file storage offers several advantages. Firstly, itprovides a high level of protection, as decrypting the stored files becomes more challenging for attackers. Secondly, it offers resistance against attacks that exploit vulnerabilities in a single encryption method. Lastly, it enables the utilization of different encryption techniques, each withits own strengths and weaknesses, thereby further bolstering the security of the stored data.

2. Literature Survey

The paper [1] underscores the significance of cloud computing across diverse sectors, including the military, educational institutions, and industries, for various purposes such as data storage. In the cloud environment, users can conveniently access and retrievetheir data upon request, without needing direct access to the server computer.

The primary focus of the paper [2] revolves around three key tasks. Firstly, it addresses the secure upload of data onto the cloud, ensuring that even the administrator remains unaware of its contents. Secondly, it

emphasizes the secure download of data, ensuring the integrity of the retrieved information. Lastly, it highlights the proper usage andsharing of public, private, and secret keys involved in the encryption and decryption processes. The paper acknowledges the vulnerability of using a single key for both encryption and decryption, which can be susceptible to malicious attacks.

The paper [3] focuses on introducing a hybrid algorithm to bolster the security of cloud data through the utilization of encryption algorithms. The primary objective of employing these encryption algorithms is to safeguard and efficiently store vast volumes of information in the cloud. The research combines homomorphic encryption and blowfish encryption techniques to enhance the overall security of cloud storage.

In the paper [4], a study was conducted to evaluate the implementation of the Blowfish algorithm in conjunction with AES. The researchers aimed to optimize the performance of each algorithm by measuring their speed across different packet sizes. The experiment involved calculating the throughput for both encryption and decryption processes using AES, resulting in a time of 1.261816 seconds for 64 bits. The corresponding CPU time was recorded as 1.54440990 seconds. Similarly, the Blowfish algorithm exhibited an encryption and decryption time of 0.850568721 seconds for 64 bits, with a CPU time of 0.07800050 seconds.

In the paper [5], a study is proposed to address the criticality of safeguarding passwords and other sensitive information, such as credentials and personal details, from theft. To achieve the desired level of security, the researchers implement a secure file transfer system based on encryption and authorization mechanisms. Storing such information in plain text form introduces a significant vulnerability and exposes it to risks posed by malicious external entities like attackers, eavesdroppers, and spyware who seek to exploitthis information. To mitigate these vulnerabilities and minimize the usefulness of compromised information, the encryption and authentication systems employ various methods. The paper introduces a method that utilizes three hybrid encryption techniques:

AES Algorithm for file encryption, asymmetric RSA encryption for securing the AES password, and HMAC for symmetric password encryption.

In [6] The paper presents a secure file storage system that focuses on ensuring the confidentiality, integrity, and authenticity of files stored in a cloud environment. The authors propose a hybrid cryptography approach that combines symmetric andasymmetric encryption algorithms. Symmetric encryption, such as AES, is used to encrypt the file, while asymmetric encryption, such as RSA, is employed to encrypt the symmetric key. This hybrid approach provides both efficiency and security in the file storage process.To maintain the integrity of the files, cryptographic hash functions like SHA-256 are utilized. The hash value of each file is calculated and stored alongside the file, allowing for later verification of its integrity. Additionally, the paper addresses the issue of secure key distribution by introducing a key distribution center (KDC). The KDCgenerates unique session keys for authorized users, encrypts them with their respective public keys, and securely sends them. This ensures that only authorized users can access the files, enhancing the overall security of the system.

In the paper [7] to meet the necessary security standards for cloud data centers, the encryption of file fragments is achieved using the Blowfish algorithm. Blowfish is distinguished from other symmetric encryption methods by its fast encryption and decryption processes and high throughput. The division and reassembly of files further enhance data security. The implementation of a hybrid approach within the cloud environment bolsters the security of remote servers, instilling greater trust among usersof cloud services. By addressing concerns related to data security and privacy protection, the challenge of segregating sensitive data and implementing access control is effectivelytackled. Cryptographic techniques are employed to convert original data into an illegible format, providing safeguarding measures.

3. Proposed Method

The instances of security breaches have been increasing exponentially. Some security breaches compel enterprises to disable their websites and mobile apps temporarily, whereas others make companies lose a significant percentage of their annual turnover. No enterprise can combat emerging data breaches and cybersecurity issues without implementing a robust encryption strategy. So we wanted to develop a web application which can encrypt and decrypt the uploadedfile so that the confidentiality of the data is maintained with user satisfaction.

The objectives of the proposed work are as follows:

- Guaranteeing the confidentiality of sensitive information through the implementation of key encryption, utilizing multiple layers and algorithms in parallel.
- Enabling fast and efficient encryption and decryption of files by incorporating hybridcryptography techniques.
- Ensuring the security of encryption keys by employing multi-level encryption for theirstorage.
- Facilitating user access to stored files, promoting both availability and authorization.
- The overarching goal of this project is to employ hybrid cryptography to safeguard storedfiles from unauthorized access and tampering.

4. Analysis & Design

4.1 Analysis

Secure file storage implemented with the help of hybrid cryptography and cloud enables a lot oflayers of security which can be crucial in terms of strengthening security and robustness of a system. The project uses a combination of multiple encryption algorithms which are tried and tested alongside adding an additional layer of security in the cloud using Amazon Boto3 kit in the cloud. The design of the project is listed below as follows:

- The system works in 2 stages of Encryption and Decryption phases. Using the interfaceprovided by the front-end design, the user can input files of their choosing which is to besecurely stored.
- The file provided by the user is fed in the backend which will be passed through theencryption phase and decryption phase when requested.
- The encryption phase detects the type of the file whether to be text file or media file.
- If a media file is detected, it is encrypted using Fernet algorithm, if text file is detected, thefile is split into 4 equal parts and encrypted using 4 different designated algorithms namely aesgcm, ChaCha20 Poly-1305, Fernet and MultiFernet.
- Encrypted file is stored in Amazon Boto3 Cloud and managed using their KeyManagement System
- The encrypted file can be retrieved and decrypted upon user request. Media files aredecrypted using Fernet key, text file parts are decrypted individually then merged.

Overall, this work uses the strength of multiple encryption algorithms, cloud technology for ubiquitous access, and methodology of encapsulation and abstraction to provide additional layersof security.

4.2 System Design

The system design for "Secure File Storage Using Hybrid Cryptography" ensures the secure storage and management of sensitive files. By utilizing hybrid cryptography techniques, files are divided and encrypted using multiple encryption algorithms. The system includes modules for file upload, encryption, decryption, key management, and access control. It incorporates securitymeasures such as secure communication protocols and robust authentication. The user interfaceis designed for easy file management. The system ensures fast and efficient encryption/decryption processes, handles errors, and provides logging functionalities. Deployment and maintenance strategies are considered, and scalability is addressed. Overall, the system design offers a comprehensive solution for secure file storage.

User Interface Design: Design a user-friendly interface for the web application, ensuring easy navigation and intuitive file management. Include screens for file upload, file retrieval, user authentication, and access control. Incorporate visual elements and feedback mechanisms to enhance the user experience.

File Upload and Storage: Specify the process of uploading files securely to the system. Discuss the mechanisms for validating file formats, handling large file sizes, and preventing unauthorized access during the upload process. Define the storage mechanism, including database design and file organization techniques.

Encryption: Outline the encryption process using hybrid cryptography techniques. Describe the selection and integration of multiple encryption algorithms to enhance file security. Explain the key generation process for each encryption algorithm used. Discuss the encryption parameters and how they are stored alongside the encrypted files.

Decryption: Detail the decryption process for retrieving files securely. Explain the mechanism for identifying the encryption algorithms and keys required for decryption. Specify the order and techniques used to decrypt the file parts encrypted withdifferent algorithms.

Key Management: Define the multi-level encryption technique for secure storage and retrieval of encryption keys. Discuss how encryption keys are generated, protected, and associated with each file. Describethe key management system, including key storage, access control, and key revocation mechanisms.

Access Control: Specify the mechanisms for user authentication and authorization.

Discuss user roles and permissions to ensure only authorized users can access specific files.Explain how access control is enforced at both the file and system levels.

Security Measures: Describe additional security measures beyond encryption, such as secure communication protocols (e.g., SSL/TLS) and secure user authentication methods (e.g., password hashing, two-factor authentication). Discuss mechanisms for detecting and preventing security threats, such as brute-force attacks or unauthorized access attempts. Address potential vulnerabilities andpropose mitigation strategies.

Performance Considerations: Discuss performance optimization techniques to ensure fast and efficient encryption and decryption processes.

Consider factors such as parallel processing, caching, and compression to minimize processing time and resource usage. Address scalability concerns and propose strategies for handling increasing user demands and file storage requirements.

Error Handling and Logging: Describe error handling mechanisms to handle exceptions and ensure system stability. Implement logging mechanisms to record system activities, including file uploads, access attempts, and encryption/decryption operations. Discuss how logs can be utilized for system monitoring, troubleshooting, and auditing purposes.

Deployment and Maintenance: Outline the deployment strategy, including server requirements and configuration. Discuss strategies for system updates, backup and recovery, and disaster management. Address maintenance considerations, including system monitoring, performance tuning, and periodicsecurity audits.

4.2.1 System Architecture Diagram

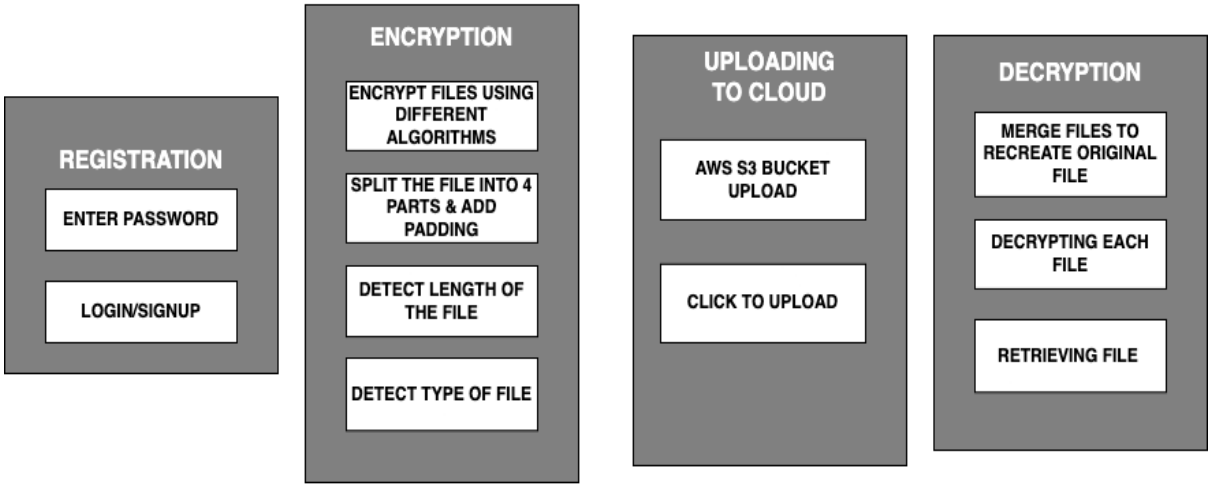

Fig 1: System Architecture Diagram

4.2.2 Data Flow Diagram

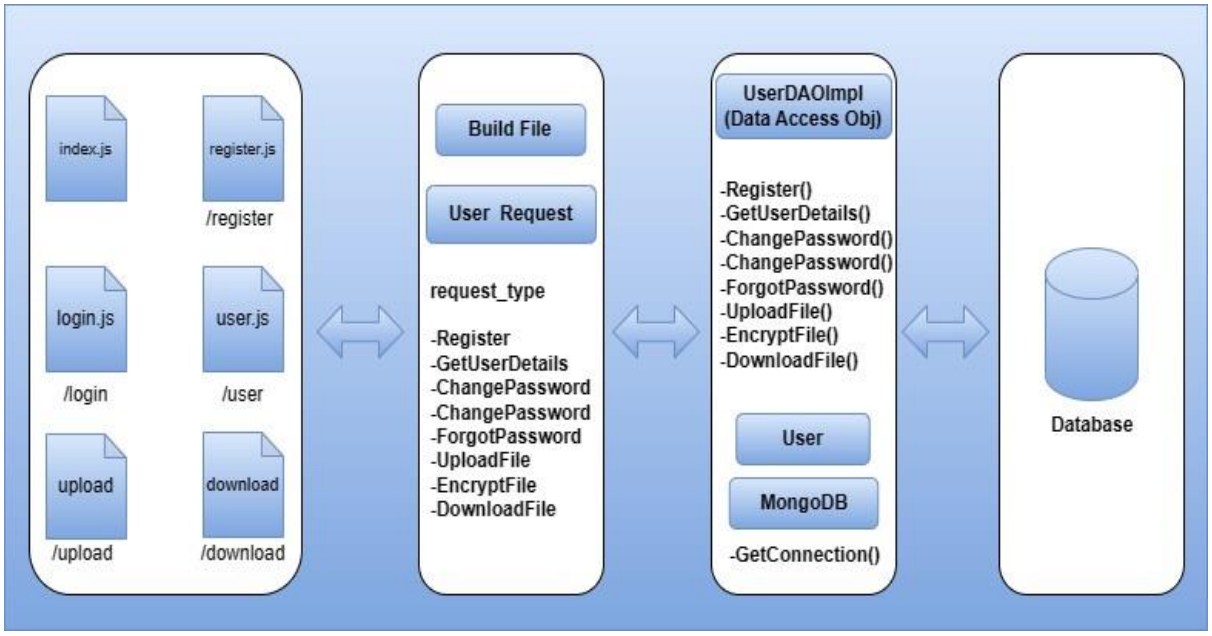

Fig 2: User Account Module Diagram

User Account Module:

Products Module

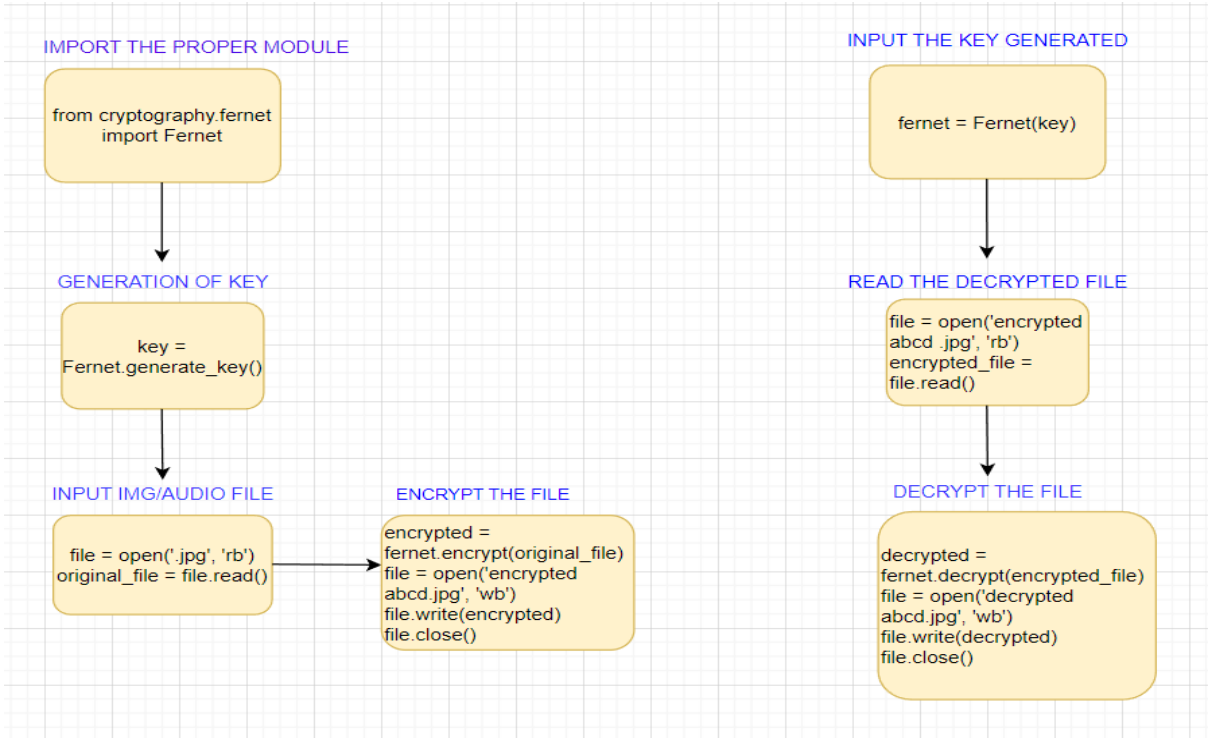

Fig 3: Encryption and Decryption of IMG/AUD Files

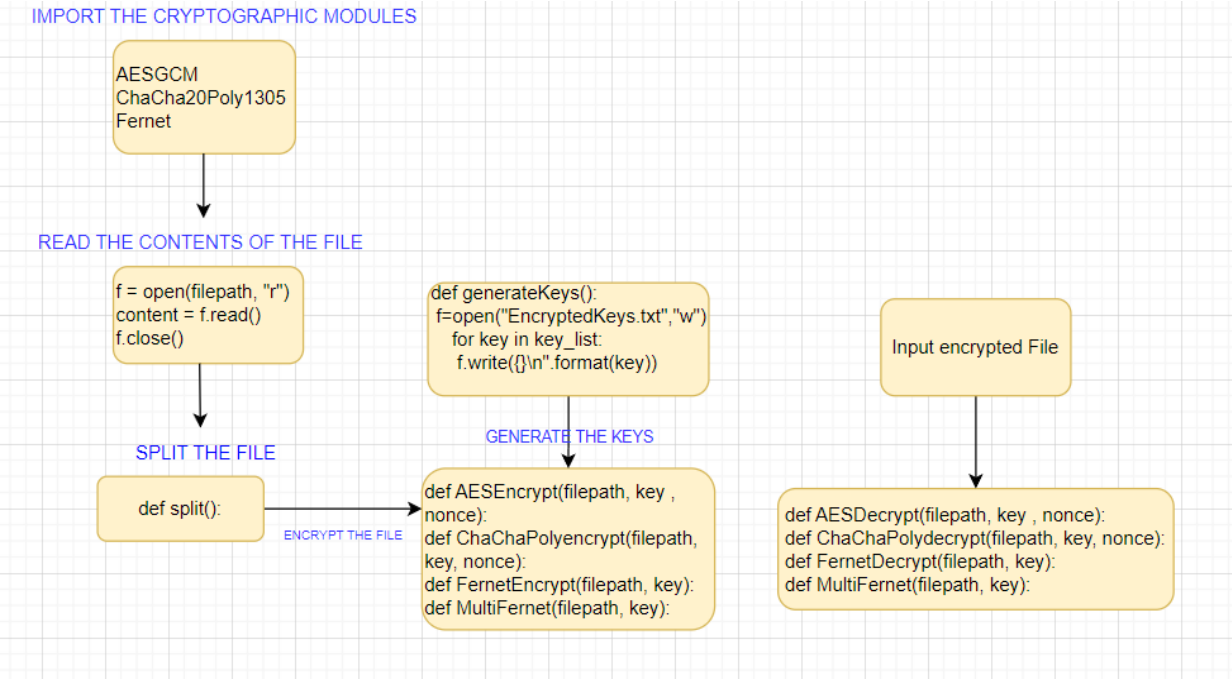

Fig 4: Encryption and Decryption of IMG/AUD Files

5. Implementation

The implementation phase involves translating the proposed solution into a tangible working end-to-end system. This section provides an overview of the whole process of implementation by highlighting the critical factors like the languages used, the libraries/modules used, and different key considerations involved in bringing this **Secure File Storage System** to life. It serves as a bridge between the conceptual idea and the actual realization of the full-stack working system that does the proposed tasks.

The implementation phase involves the execution and integration of different elements necessaryfor the secure file storage system using hybrid cryptography. This encompasses setting up the required hardware, developing the necessary software components, integrating encryption algorithms, establishing secure connections, and ensuring the seamless transmission of data tothe cloud platform. Through the implementation stage, the system is designed to functionsmoothly, meeting the desired goals of securely storing files using hybrid cryptography.

5.1 Implementation Method

PSEUDO CODE

1. Identify the existing system and find the runtime complexity of all the algorithms.
2. Identify appropriate algorithms which are much more efficient and provide better security and create a proposed system.
3. Generate cryptographic keys for all the algorithms - AESGCM, ChaCha20Poly-1305, Fernet, MultiFernet.
4. Detect the type of file and encrypt the file according to the file type. Media/audio files, it's encrypted using Fernet Algorithm; text files are encrypted in a hybrid format using four different algorithms.
5. Text files are split into four equal parts and each part is encrypted using a different algorithm.
6. These encrypted files are sent over to the cloud storage (AWS S3 Bucket).
7. During the decryption phase, the files are retrieved from S3 Bucket, and the files are decrypted.

8. If it's a text file, the decrypted files are merged to form the original file. If it's a media file, it's decrypted without any loss or compression.
9. We have also implemented a registration and a login page for users in authentication.

6. Results

- In our secure file storage system utilizing hybrid cryptography, the encryption and decryption process is seamlessly performed on the files. We employ a combination of robust cryptographic algorithms, including AES-GCM, ChaCha20Poly-1305, Fernet, and MultiFernet. These algorithms, known as stream ciphers, operate on the file data bit-by-bit, ensuring efficient and secure encryption and decryption.
- Improved efficiency in file encryption and decryption is detected. As the file size increases, stream ciphers become more efficient and take less time to encrypt the files.
- As we are using 128 bits key in AES-GCM and 256 bit keys in ChaCha20Poly-1305, Fernet and MultiFernet, essentially if someone tries to brute force the key, it will take around following time for brute force - $2^{128} + 2^{256} + 2^{256} + 2^{256}$ $secs$. This makes it a very robust and secure system.

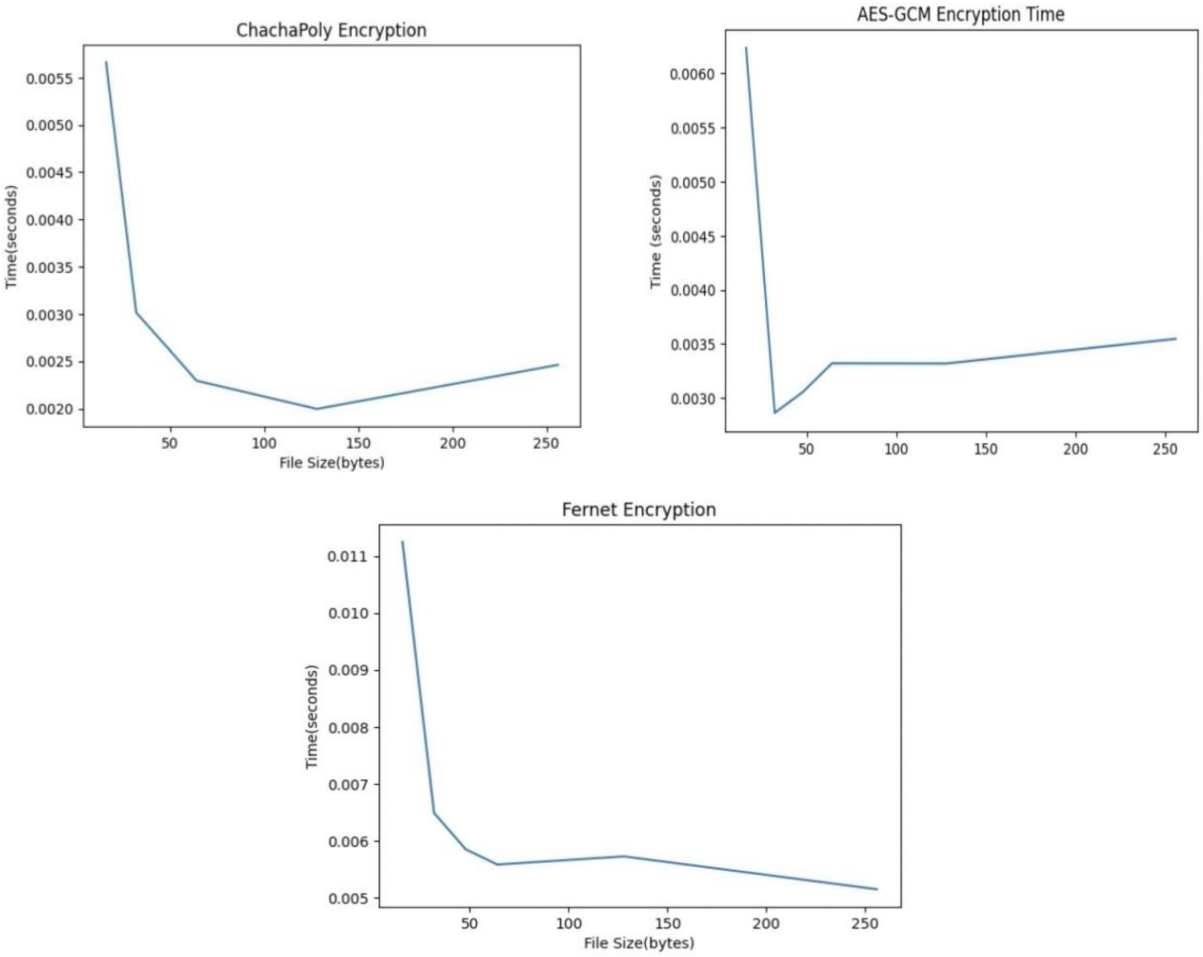

Fig 5: Time analysis of different algorithms used**.**

7. Conclusion

In conclusion, our project successfully demonstrated the effectiveness of using hybrid cryptography for secure file storage. By employing symmetric encryption algorithms, we were able to ensure the confidentiality

and integrity of stored files in the cloud. This approach offers robust protection against unauthorized access and data breaches. Our research highlights the significance of hybrid cryptography in safeguarding sensitive information and addresses the growing concerns surrounding data security in cloudstorage. Furthermore, the project underscores the importance of secure file storage practices in maintaining privacy and compliance with data protection regulations. Overall, our project exemplifies thepotential of hybrid cryptography in enhancing the security of file storage systems and underscores its relevance in today's digital landscape.

References

[1] Kumar, U., & Prakash, J. (2020). Secure File Storage on Cloud Using Hybrid Cryptography Algorithm. International Journal of Creative Research Thoughts (IJCRT), 8(12), 338-344. Retrieved from https://www.ijcrt.org/papers/IJCRT2007048.pdf

[2] Mahalle, Vishwanath & Shahade, Aniket. (2014). Enhancing the data security in Cloud by implementing hybrid (Rsa & Aes) encryption algorithm. 10.1109/INPAC.2014.6981152.

[3] Sajay, K. R., Suvanam Sasidhar Babu and Yellepeddi Vijayalakshmi. “Enhancing the security of cloud data using hybrid encryption algorithm.” Journal of Ambient Intelligence and Humanized Computing (2019): n. pag.

[4] Chaitali, Haldankar., Sonia, Kuwelkar. (2014). Implementation of aes and blowfish algorithm. International Journal of Research in Engineering and Technology, 03(15), 143-146. Available from: 10.15623/IJRET.2014.0315026

[5] E. S. I. Harba, “Secure Data Encryption Through a Combination of AES, RSA and HMAC”, Eng. Technol. Appl. Sci. Res., vol. 7, no. 4, pp. 1781–1785, Aug. 2017.

[6] P. Bharathi, G. Annam, J. B. Kandi, V. K. Duggana and A. T., "Secure File Storage using Hybrid Cryptography," 2021 6th International Conference on Communication and Electronics Systems (ICCES), Coimbatre, India, 2021, pp. 1-6, doi: 10.1109/ICCES51350.2021.9489026

[7] Gokulraj, S. and Ananthi, P. and Baby, R. and Janani, E., Secure File Storage Using Hybrid Cryptography (March 11, 2021). Available at SSRN: https://ssrn.com/abstract=3802668 or http://dx.doi.org/10.2139/ssrn.3802668