IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 8, August 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 8, August 2023 ||

| DOI:10.15680/IJIRSET.2023.1208015 |

A Secure File Storage using Hybrid Cryptography

Altamish Chowdhury [1], Dr. Mohan Aradhya [2]

P.G. Student, Department of Master of Computer Applications, RV College of Engineering, Bengaluru, India[1]

Assistant Professor, Department of Master of Computer Applications, RV College of Engineering, Bengaluru, India[2]

ABSTRACT: The growing reliance on cloud storage for file management has led to concerns regarding unauthorized access to sensitive data. This research project addresses the need for secure file storage by proposing a hybrid cryptography-based solution. By combining multiple symmetric algorithms, the project aims to enhance the security of stored files while eliminating the use of asymmetric algorithms. The proposed system utilizes a combination of encryption techniques to ensure confidentiality, integrity, and authenticity of the stored data. The project focuses on designing an efficient and reliable file storage architecture that can resist various attack vectors. Experimental evaluations will be conducted to assess the performance and security of the proposed solution, providing insights into its feasibility and effectiveness. The findings of this research project have the potential to contribute to the development of secure file storage mechanisms in cloud environments, mitigating the risks of unauthorized data access.

KEYWORDS: Secure file storage, Hybrid cryptography, Unauthorized access, Symmetric algorithms, Cloud environment.

I. INTRODUCTION

The administration and storage of information in cloud environments has grown in popularity as a result of the cloud computing industry's quick development. The safeguarding of critical data kept on the cloud has come under scrutiny due to this convenience, though. Unauthorized access to files poses a significant threat, potentially leading to data breaches, privacy violations, and financial losses. To allay these worries, this research project focuses on the development of a secure file storage solution using hybrid cryptography.

Traditional encryption methods often rely on a single algorithm, either symmetric or asymmetric, for securing data. However, this project takes a different approach by exclusively utilizing multiple symmetric algorithms and avoiding the use of asymmetric algorithms. By leveraging the strengths of symmetric encryption, the proposed solution aims to provide robust security while minimizing computational overhead.

The major goal of this research project is to design an efficient and reliable file storage architecture that ensures the confidentiality, integrity, and authenticity of stored files. By employing a hybrid cryptography approach, which combines multiple symmetric algorithms, the system intends to mitigate the risks of unauthorized access and enhance the overall security of cloud-based file storage.

II. LITERATURE REVIEW

To investigate the body of knowledge already available on hybrid cryptography and safe file storage, there has been a careful literature evaluation done. This review included a thorough examination of pertinent journal papers, conference proceedings, and research materials. Multiple search engines and databases, including Google Scholar, IEEE Xplore, and the ACM Digital Library, were employed to find relevant information so as to guarantee inclusivity. The literature review examines the essential traits and metrics used in various secure file storage approaches, with a focus on hybrid cryptography. The review identifies each method's unique advantages and disadvantages through a comparative examination. This evaluation not only provides important insights into the state-of-the-art methodologies, but it also highlights prospective research holes and indicates lines of inquiry for future studies in the creation of hybrid cryptographic safe file storage systems.

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 8, August 2023 ||

| DOI:10.15680/IJIRSET.2023.1208015 |

[1] Cloud storage and chat messaging are only two applications where security is a major problem. When relying solely on one type of encryption, such as AES, DES, or RSA, existing systems frequently experience failure. The proposed remedy combines three new approaches with existing encryption algorithms to create hybrid cryptography. Three separate pieces of data are encrypted using RSA, DES, and AES. The keys are kept in an image through LSB steganography, and the encrypted files are kept in the cloud. Before importing data from the server, users must obtain the keys, which they may utilize to decrypt the data with AES, DES, and RSA, boosting record security.

[2] File protection is a big problem in the case of cloud security in relation to cloud computing. Researchers provide a hybrid strategy that uses cryptography to resolve this issue by achieving high standards of data security and privacy. This approach implements an amalgamated algorithm that offers strong security and discretion for patient data by combining ECC with Blowfish. The suggested approach gets over the drawbacks of conventional symmetrical and asymmetrical approaches, guaranteeing the access to and the accuracy of cloud services.

[3] Although security issues prevent cloud computing from being widely used, it makes use of massive clusters of controllable resources for efficient resource utilisation. Contrary to the currently used AES and RSA methods, this document provides a hybrid cryptographic protocol employing the Blowfish and Paillier encryption algorithms. The technique decreases computation time and ciphertext size, enhancing cloud storage. While performance study and security analysis utilizing the Hardening Index and firewall protection are being done, simulations demonstrate improved security with the aid of compression. The Paillier and Blowfish hybrid approach outperforms the current RSA and AES techniques.

[4] Big data has problems with unauthorized access, theft, and storage. For the storage of massive data, researchers are inventing security procedures. The development of an encryption technique for multi-cloud storage, which enables users to save data across different services, is the main emphasis of this article. Processes for uploading, slicing, indexing, distributing, decrypting, retrieving, and combining data are all included in the framework. In order to offer security before storing data in multi-cloud systems, a hybrid encryption technique was created. Real-time cloud storage simulation analysis demonstrated the algorithm's advantage over benchmark methods.

[5] As a result of its low cost and simplicity, cloud migration is growing in popularity. However, computer users may have trouble locating adequate room for their data storage. Information security is essential to address this, and hybrid encryption is employed to ensure security. This study focused on user authentication and inappropriate hybrid algorithm implementation to provide information on hybrid cryptography from 2015 to the beginning of 2019. The failure to consider user authentication and the inappropriate application of hybrid algorithms constitute the identified research gap.

III. METHODOLOGY

The research aims to address the growing need for robust and efficient file storage solutions that ensure data security. In today's digital age, where data breaches and unauthorized access are prevalent, it is crucial to adopt advanced encryption techniques to safeguard sensitive information. The project’s recommended methodology entails a two-level encryption process, combining the AES, 3DES, and Blowfish algorithms, followed by file segmentation for efficient storage.

The first level of encryption utilizes the Advanced Encryption Standard (AES) algorithm, a widely recognized and trusted encryption technique. AES employs a cryptographic technique with symmetric keys, which ensures the secrecy and reliability of the files being stored. This initial layer of protection offers a strong defense against unauthorized access and data breaches.

The size of the file being stored determines the second degree of encryption. For larger files, the Triple Data Encryption Standard (3DES) algorithm is applied. 3DES is aa algorithm for symmetric encryption that applies the Data Encryption Standard (DES) cipher three times in a row, each iteration utilizing a new set of keys. This strategy offers improved security for larger files by boosting the complexity of the encryption process.

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 8, August 2023 ||

| DOI:10.15680/IJIRSET.2023.1208015 |

For smaller files, the Blowfish algorithm is used in the second level of encryption. Blowfish is a block cipher with symmetric keys that operates on variable-length blocks. It offers a high degree of protection and performance, making it well-suited for encrypting smaller files efficiently.

After the two-level encryption process, the encrypted format is segmented into smaller, manageable portions. This division enables for easy uploading and storage in various storage platforms such as cloud services or other storage solutions. By breaking down the encrypted file into smaller segments, it becomes more convenient to transfer and manage the data securely.

After the two-level encryption process and file segmentation, the encrypted file is stored securely. When a user wants to download the file, they must have the file owner's consent. The download process involves reversing the segmentation, combining the file segments back together. Subject to the size of the combined file, the decryption algorithm works upon it, similar to the encryption process of the second level. The AES decryption takes place at the end, resulting in the retrieval of the final original file. This strategy guarantees that only authorized users with appropriate permissions can access and retrieve the decrypted file, maintaining data security throughout the storage and retrieval process.

The proposed methodology of using hybrid cryptography with AES, 3DES, and Blowfish algorithms provides several advantages. Firstly, it ensures a multi-layered approach to encryption, enhancing the overall security of the file storage system. The combination of different algorithms adds complexity and makes it more challenging for attackers to decrypt the files. Additionally, by selecting the encryption algorithm based on file size, the methodology optimizes both security and performance. It allows for efficient encryption of smaller files using Blowfish while providing stronger protection for larger files with 3DES. The file segmentation aspect further enhances scalability and flexibility, enabling easy integration with existing storage infrastructure. Overall, this proposed methodology offers a comprehensive and secure file storage option appropriate for various storage platforms.

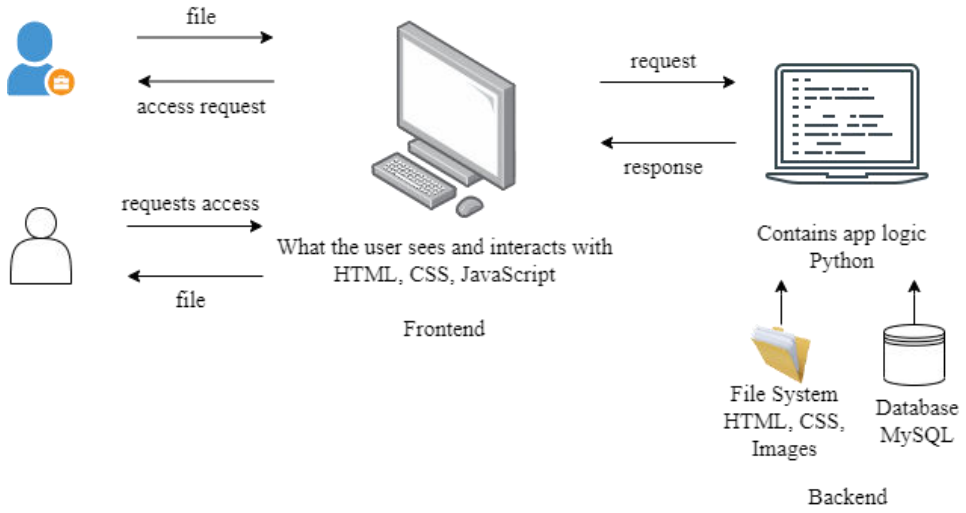

Fig. 1. Architecture Diagram for A Secure File Storage using Hybrid Cryptography

IV. CONCLUSION

In conclusion, the study seeks to answer the crucial need for secure and reliable file storage systems. By implementing hybrid cryptography techniques, which combine the strengths of multiple symmetric algorithms, the project offers a robust solution to prevent unauthorized access to critical data. The development process involves the creation and execution of a secure file storage system that ensures confidentiality, integrity, and authenticity of stored files. By employing advanced encryption methods and incorporating secure key management practices, this project presents a viable approach to safeguarding sensitive information, thereby enhancing data security in various domains.

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 8, August 2023 ||

| DOI:10.15680/IJIRSET.2023.1208015 |

REFERENCES

[1] Bharathi, P., Annam, G., Kandi, J. B., Duggana, V. K., & Anjali, T. (2021, July). Secure File Storage using Hybrid Cryptography. In Proceedings of the 6th International Conference on Communication and Electronics Systems (ICCES) (pp. 1-6). IEEE.

[2] Chinnasamy, P., Padmavathi, S., Swathy, R., & Rakesh, S. (2021). Efficient Data Security Using Hybrid Cryptography on Cloud Computing. In P. V. Veena, G. Sudha, M. Rajeshwari, & R. Anitha (Eds.), Inventive Communication and Computational Technologies: Proceedings of ICICCT 2020 (pp. 537-547). Springer Singapore.

[3] Seth, B., Dalal, S., Le, D. N., Jaglan, V., Dahiya, N., Agrawal, A., ... & Verma, K. D. (2021). Secure Cloud Data Storage System Using Hybrid Paillier–Blowfish Algorithm. CMC-Computers Materials & Continua, 67(1), 779-798.

[4] Viswanath, G., & Krishna, P. V. (2021). Hybrid encryption framework for securing big data storage in multi-cloud environment. Evolutionary Intelligence, 14, 691-698.

[5] Ahmad, S. A., & Garko, A. B. (2019, December). Hybrid Cryptography Algorithms in Cloud Computing: A Review. In Proceedings of the 15th International Conference on Electronics, Computer and Computation (ICECCO) (pp. 1-6). IEEE.

[6] Sajay, K. R., Babu, S. S., & Vijayalakshmi, Y. (2019). Enhancing the security of cloud data using hybrid encryption algorithm. Journal of Ambient Intelligence and Humanized Computing, 1-10.

[7] Bala, B., Kamboj, L., & Luthra, P. (2018). Secure file Storage in Cloud Computing using Hybrid Cryptography algorithm. International Journal of Advanced Research in Computer Science, 9(2).

[8] Taha, A. A., Elminaam, D. S. A., & Hosny, K. M. (2018). An improved Security Schema for Mobile Cloud Computing using Hybrid Cryptographic algorithms. Far East Journal of Electronics and Communications, 18(4), 521-546.

[9] Maitri, P. V., & Verma, A. (2016, March). Secure file storage in cloud computing using hybrid cryptography algorithm. In International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET) (pp. 1635-1638). IEEE.

[10] Anjali, D. V., & Chandrashekara, D. S. (2016). Design and Implementation of Secure Cloud Storage System using Hybrid Cryptography Algorithms with Role based Access Control Model. International Journal of Engineering and Technical Research (IJETR).

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details