INTERNATIONAL JOURNAL OF ADVANCED INNOVATIVE TECHNOLOGY IN ENGINEERING

Published by Global Advanced Research Publication House Journal

Home page: www.ijaite.co.in

Secure File Storage on Cloud using Hybrid Cryptography with Triple Encryption

[1]Shilpa Burade, [2]Prof. Jayant Adhikari, [3]Prof. Nilesh Mhaiskar, [4]Prof. Mukesh Trone

[1,2,3]Department of Computer Science and Engineering T.G.P.C.E.T. Nagpur, Maharashtra, India

[4]Department of Electronics Engineering Computer Science and Information Technology, Deori, Maharashtra, India

[1]shilpaburade93@gmail.com, [2]jayent.cse@tgpcet.com, [3]nilesh.cse@tgpcet.com, [4]mmtrone23@gmail.com.

Article History

Received on: 10 Feb. 2025
Revised on: 28 Feb. 2025
Accepted on: 30 March 2025

Keywords: Hybrid Cryptography, Integrity Confidentiality, Storage, Security, Data Protection, Elliptic Curve Cryptography.

e-ISSN: 2455-6491

DOI: 10.5281/zenodo.15433621

Production and hosted by
www.garph.org

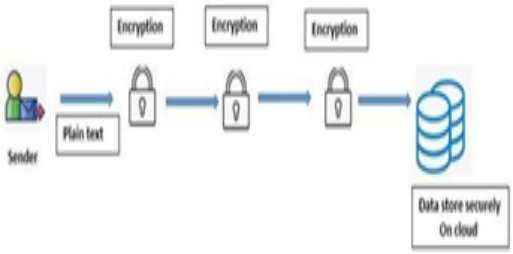
ABSTRACT

In today's digital age, cloud computing has become the backbone of data storage for both individuals and organizations. The adoption of cloud-based solutions offers scalability, flexibility, and cost-efficiency, enabling users to store and access vast amounts of data remotely. However, with the growing volume of sensitive information being stored in the cloud, the need for robust security measures has never been more critical. Data breaches, cyber-attacks, and unauthorized access remain constant threats to the integrity and privacy of cloud-stored data.

1. INTRODUCTION

To provide a more secure, effective, and scalable encryption system, hybrid cryptography blends the advantages of symmetric and asymmetric encryption. While symmetric encryption Blowfish is selected due to Asymmetric Encryption Techniques: Alongside Blowfish, other encryption methods such as AES**,** RC6, and 3DES, RSA or ECC (Elliptic Curve Cryptography) can be applied to encrypt the keys used by Blowfish. This ensures that the keys are securely stored and transmitted. Triple Encryption to achieve high-security levels, documents are encrypted using three distinct encryption methods [2]. This layered approach makes unauthorized decryption

incredibly difficult, enhancing security, especially when data is transmitted over the internet [4]. Unlike older systems that often rely on a single encryption method (either symmetric or asymmetric), our system combines Blowfish (a fast symmetric encryption algorithm) with AES, RC6, and 3DES, RSA or ECC (asymmetric encryption) to secure both data and the keys used for encryption [3]**.** Numerous benefits, including scalability, flexibility, cost effectiveness, and speed, have been brought about by the quick adoption of cloud computing [5]. However, data security is one of the main issues with cloud storage.



.

Figure1: Encryption Method

2. PROSPECTIVE APPLICATION

The research paper aims to improve cloud storage security using hybrid cryptography with multiple inscription technique. In this scheme, there is the use of symmetric key cryptography and Asymmetric key cryptography this paper's symmetric encryption various strong algorithms are selected due to its efficiency and speed content is highly focused on the security of files in the cloud as well as increasing the speed of data storing and retrieving on cloud. The data of the above algorithm is collected from various sources or another platform of a research paper. The above techniques and algorithms are a suitable method for protecting files from social platforms and the cloud.

3. METHDOLOGY

This project focuses on developing a File Storage System using Hybrid Cryptography with Triple Encryption to achieve the following objectives:

Enhanced Data Security: Protect data through multiple layers of encryption, significantly reducing the risk of unauthorized access or data breaches. Ensuring that only authorized parties can decrypt data.

Scalability and Performance: Design the system to be scalable and efficient, ensuring that the encryption process does not impede the performance or usability of the cloud storage.

Compliance and Regulatory Adherence: Develop a solution that ensures compliance with data protection laws and standards, making it suitable for industries with strict regulatory requirements.

User Accessibility and Control: Provide a user-friendly interface that allows easy file upload, encryption, storage, and decryption, while ensuring that the underlying encryption mechanisms remain transparent to the user.

In the current secure file storage system the current system uses symmetric key cryptography and steganography techniques. Symmetric key algorithms like AES, blowfish, RC6 algorithms are used to provide block-wise security to data in the files. Each file is split chunks and every block is encrypted using a different algorithm. Using LSB steganography keys are inserted into cover images and then cover images are shared with the user via email. The existing system only focuses on confidentiality and does not consider integrity and authentication. Updated Secure Cloud Storage Using Hybrid Cryptography Enhanced Features in the Proposed System.

- Files are divided into smaller chunks (configurable size). Each chunk is encrypted using AES-256-GCM for confidentiality and integrity in one step.
- Keys for each chunk, encrypted using the recipient's public key (asymmetric cryptography).
- A hash (SHA-256/SHA-3) of the entire file for integrity checks. The metadata is signed using the owner's private key to ensure authentication.
- A secure Public Key Infrastructure (PKI) system manages public and private keys.
- Encrypted file chunks are stored in the cloud storage.
- A trusted center stores and distributes public keys using protocols like HTTPS and Certificate Transparency Logs for validation.
- Key Revocation.
- Supports key revocation and updates via Online Certificate Status Protocol (OCSP).
- The user downloads the encrypted file chunks and metadata.

- Using their private key, the user decrypts the metadata to retrieve the AES keys for the file chunks.
- File chunks are decrypted locally using these AES keys.
- Integrity Check: The file hash is recalculated and compared with the hash stored in table.

Table 1: Summary of previous research work of hybrid encryption based on cloud

Author	Algorithm Used	Purpose Of System	Limitation
A. Ashok Kumar1, Santhosha 1, A.Jagan	DES & RSA /STENOGRAPHY	A hybrid Cryptography based plan for safe cloud data storage is put out in this study. To encrypt and decrypt the data, the suggested	Brute force attacks are a risk. Forward secrecy is not provided by DES or RSA. Brute force attacks are a risk. Forward secrecy is not provided by DES or RSA.
A. Poduvall, Doke, H. Nemade, and R. Nikam(2019)	DES, AES, and RC2	This system's goal is to create an encryption method for safe file storage in wireless communications, virtual private networks (VPNs), multi-cloud storage, and other electronic data.	The suggested system had a number of security flaws.

4. CHALLENGES AND FUTURE SCOPE

Cloud storage recognition has gained a lot of interest these days, but the main focus has shifted to the security that are not posed or that are spontaneous. So, the very first problem that is being faced recently is unavailability of the databases security having the spontaneous encryption and creating such database and storing data securely is one of the major challenges. As per the conclusion if the subjects have prior knowledge chances of error are also very high. An expertise is required on the coder part as well as on the observer part. To avoid the problems with labeling of data semi-supervised learning techniques could be used because they allow the use of labeled data along with the unlabeled data. There are some systems that are not fully automatic, they require some manual actions during processing, like some systems need fiducial points to be marked on the face manually during the initialization. So, the challenge here is to make a system that is fully automatic and does not require any manual interference. Other factors that affect the expressions like: Subjects that they are being store data securely then the problem will not remain. The next problem is having these spontaneous encryption with big data. For this type of cases the approach of using the hybrid encryption technique. Labeling of data is a lengthy and a complicated process, it consumes a lot of time and the chances of error are also very high. An expertise is required on the coder part as well as on the observer part. To avoid the problems with labeling of data supervised learning techniques could be used because they allow the use of labeled data along with the unlabeled data. The rapid adoption of cloud computing has brought numerous benefits, such as increasing storage adding multiple user at same time, capacity , smooth, and cost efficiency, speed. However, one of the primary concerns in cloud storage is data security. Also in this project we can also change the algorithms according to our need also we providing the facility to select layer of encryption. In future we will work on load balancing as well as minimizing the speed of uploading and downloading the file from cloud belonging to different cultures like Asians, Europeans, age groups will have different expressions. A facial expression recognition system should be able to handle these problems. Angles of head and their rotations are also a big concern. A future extension of facial expressions analysis could be the analysis of micro expression. Nowadays only few training techniques are available that works for micro expressions. One more issue that may rise in automatic facial expression systems is recognizing the expressions of the subjects, who have lost their natural facial expressions because of the medical problems. There are 12 diseases that results in this

loss of the facial expressions namely: Facial Paralysis, Autistic Disorder, Asperger Syndrome, Hepatolenticular Degeneration, Depressive Disorders, Bell's Palsy, Depression, Facial Weakness, Major Depressive disorder.

CONCLUSION

In this project by using Hybrid Cryptography combines the power of multiple encryption technique to offer a more secure, efficient, and very good encryption system. While symmetric encryption Blowfish is selected due to its efficiency and speed, making it suitable for encrypting large files with minimal processing time. Asymmetric Encryption Techniques: Alongside Blowfish, other encryption methods such as AES, RC6, and 3DES, RSA or ECC (Elliptic Curve Cryptography) can be applied to encrypt the keys used by Blowfish. This ensures that the keys are securely stored and transmitted. Triple Encryption to achieve high-security levels, documents are encrypted using three distinct encryption methods. This layered approach makes unauthorized decryption incred applied to encrypt the keys used by Blowfish. This ensures that the keys are securely stored and transmitted. Triple Encryption to achieve high-security levels, documents are encrypted using three distinct encryption methods. This layered approach makes unauthorized decryption incredibly difficult, enhancing security, especially when data is transmitted over the internet. Unlike older systems that often rely on a single encryption method (either symmetric or asymmetric), our system combines Blowfish (a fast symmetric encryption algorithm) with AES, RC6, and 3DES, RSA or ECC (asymmetric encryption) to secure both data and the keys used for encryption. The rapid adoption of cloud computing has brought numerous benefits, such as increasing storage adding multiple user at same time, capacity , smooth, and cost efficiency, speed. However, one of the primary concerns in cloud storage is data security. Also in this project we can also change the algorithms according to our need also we

ACKNOWLEDGEMENT (OPTIONAL).

The author acknowledges the immense help received from the scholars whose articles re cited and included in references to this manuscript. The author is also grateful to authors/editors/publishers of all those articles, journals and books from where the literature for this article has been reviewed and discussed.

CONFLICT OF INTEREST

There in no conflict of interest

FUNDING SUPPORT

Government grants, corporate sponsorships, venture capital, academic financing, crowd funding, and nonprofit organizations are some of the sources of funding for projects like safe file storage on the cloud employing hybrid cryptography with triple encryption. Whether you're seeking research grants, commercial product investment, or financial support from privacy and security advocacy groups, each funding source will need a different strategy.

References

[1] HEQING SONG , JIFEI LI , AND HAOTENG LIA Cloud Secure Storage Mechanism Based on Data Dispersion and Encryption

[2] Bharat S. Rawal and 2 S. Sree VivekSecure Cloud Storage and File Sharing IEEE International Conference on Smart Cloud

[3] Sidra Aslam, Munam Ali Shah Load Balancing Algorithms in Cloud Computing: A Survey of Modern Techniques(NSEC 2015)

[4] Shrikanta Jogarl & Darshan S Handral. (2022). "Secure File Storage on Cloud Using HybridCryptography", International Journal of Advanced Research in Science, Communication and Technology (IJARSCT).

[5] Gajanan T, S. Jayde, H.Gaurkhede, R. Vaidya, A. Wankhade& V.Yelekar. (2021). "Secure File Storage on Cloud Using Hybrid Cryptography", International Research Journal of Engineering and Technology (IRJET). ISSN: 2395-0056.

[6] M.Naveetha Krishnan&T.Tamilarasan. (2021). "Secure File Storage on Cloud Using Hybrid Cryptography", International Journal of Advanced Research in Computer Science Engineering and Information Technology (IJARCSEIT).

[7] R. Calheiros et al., "CloudSim: A Toolkit for Modeling and Simulation of Cloud Computing Environments and Evaluation of Resource Provisioning Algorithms," Software: Practice and Experience, vol. 41, no. 1, pp. 23-50, Jan. 2011, doi: 10.1002/spe.995.

[8] Uttam Kumar, Mr. Jay Prakash (2020). "Secure File Storage On Cloud Using Hybrid Cryptography Algorithm", International Journal of Creative Research Thoughts (IJCRT). ISSN:- 2320-2882 [Base Paper]. [5]. Aditya Poduval, Abhijeet Doke, Hitesh Nemade& Rohan Nikam. (2019). "Secure File Storage on Cloud using Hybrid Cryptography", International Journal of Computer Sciences and Engineering (IJCSE) E-ISSN: 2347-2693.

[9] M. Malarvizhi, J. Angela Jennifa Sujana, T.Revathi (2014). "Secure File Sharing Using Cryptographic Techniques In Cloud", International Conference On Green Computing Communication And Electrical Engineering (ICGCCEE).

[10] Lowlesh Yadav and Asha Ambhaikar, "IOHT based Tele-Healthcare Support System for Feasibility and performance analysis," Journal of Electrical Systems, vol. 20, no. 3s, pp. 844– 850, Apr. 2024, doi: 10.52783/jes.1382.

[11] L. Yadav and A. Ambhaikar, "Feasibility and Deployment Challenges of Data Analysis in Tele-Healthcare System," 2023 International Conference on Artificial Intelligence for Innovations in Healthcare Industries (ICAIIHI), Raipur, India, 2023, pp. 1-5, doi: 10.1109/ICAIIHI57871.2023.10489389.

[12] L. Yadav and A. Ambhaikar, "Approach Towards Development of Portable Multi-Model Tele-Healthcare System," 2023 International Conference on Artificial Intelligence for Innovations in Healthcare Industries (ICAIIHI), Raipur, India, 2023, pp. 1-6, doi:10.1109/ICAIIHI57871.2023.10489468.

[13] Lowlesh Yadav and Asha Ambhaikar, Exploring Portable Multi-Modal Telehealth

[14] Solutions: A Development Approach. International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC), vol. 11, no. 10, pp. 873– 879, Mar. 2024.11(10), 873–879.

[15] Lowlesh Yadav, Predictive Acknowledgement using TRE System to reduce cost and

[16] Bandwidth, March 2019. International Journal of Research in Electronics and Computer Engineering (IJRECE), VOL. 7 ISSUE 1 (JANUARY- MARCH 2019) ISSN: 2393-9028 (PRINT) | ISSN: 2348-2281 (ONLINE)