International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 05 | May - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Secure File Storage on Cloud Using Hybrid Cryptography

Tenzin Chokyi
21BTRCS085
Dept of CSE
Jain University, Bangalore, Karnataka
tchokyi2931@gmail.com

Tenzin Sherab
21BTRCS086
Dept of CSE
Jain University, Bangalore, Karnataka
tsherab2003@gmail.com

Tenzin Tsamphel
21BTRCS087
Dept of CSE
Jain University, Bangalore, Karnataka
tentsam30@gmail.com

Sarga Santhosh
21BTRCS068
Dept of CSE
Jain University, Bangalore, Karnataka
sargaaa077@gmail.com

Prof. Agashani V Kumar
Professor
Dept of CSE
Jain University, Bangalore, Karnataka

Abstract

The exponential growth of cloud computing is the reason that people and organizations store and then access their data. Primary concerns persist regarding data's security as well as integrity stored in cloud environments because of cyber-attacks' increasing threat landscape. Elliptic Curve Cryptography (ECC) combines with ChaCha20 for secure key exchange; an efficient stream cipher, and blockchain technology ensures tamper-proof file integrity verification in this paper proposing a novel security framework for cloud file storage. ChaCha20 resists against cryptographic attacks and then runs fast, while then ECC manages the keys securely and lightly. Blockchain integration adds a permanent stage to check file integrity stored in the cloud ensuring that forbidden alterations are never overlooked. Encryption as well as decryption performance is a key evaluation factor for the system that is proposed. Also evaluation factors are verification of file integrity and security of the overall system. The results show that the hybrid cryptographic approach offers toward a highly efficient and secure solution for cloud storage applications. Since it is coupled with blockchain, it addresses both confidentiality and integrity concerns.

1. Introduction

Cloud storage has become quite a ubiquitous service because of its flexibility along with cost-efficiency as well as scalability for the storing of personal, organizational, and governmental data. But cloud storage frequently presents various security and privacy issues such as forbidden access and sensitive data manipulation. Encryption methods that are customary can protect a system against any forbidden access. However, those methods fail in addressing the issue of data integrity since data might have been altered during storage or transfer.

In reducing these risks, this paper proposes a hybrid cryptographic approach that uses ChaCha20 stream cipher for encryption and Elliptic Curve Cryptography (ECC) for secure key exchange and that is integrated with blockchain technology to ensure data integrity. For its speed, the ChaCha20 algorithm was selected so it was useful for huge dataset cloud environments. It gives quick encryption and decryption actions. ECC provides a high level of security even when key sizes are smaller than those key sizes of customary public-key algorithms like RSA so it is ideal for environments with constrained resources. Furthermore, blockchain can be leveraged so as to provide decentralized verification for file integrity, which thereby ensures that all data changes are able to be detected in the event forbidden.

This approach seeks to improve the security, efficiency, together with the integrity of cloud file storage systems, offering a solution securing data while also tracking its integrity through the immutable ledger that blockchain technology provides.

2. Literature Survey

The security of cloud storage systems is an important concern due to the fact that the risk of forbidden access and of data tampering is increasingly becoming more and more apparent. Data confidentiality is ensured by various cryptographic techniques. For integrity, researchers have explored these techniques in cloud environments.

1. Cloud Storage Security Stream Ciphers of:

ChaCha20, a stream cipher designed by Daniel J. Bernstein, is gaining appeal because of high speed and strong security for encryption of cloud storage. ChaCha20, in contrast to AES, has resistance to cryptographic attacks that have been known, like related-key attacks and timing attacks. It can encrypt large datasets since it is efficient. Because cloud environments require performance, the algorithm is suitable for use there (Bernstein, 2008). ChaCha20 has been shown to encrypt as well as decrypt faster than AES, so it is a preferable choice within cloud systems (Yang et al., 2017).

2. Key Exchange that uses Elliptic Curve Cryptography (ECC):

Elliptic Curve Cryptography (ECC) is a highly efficient asymmetric cryptographic algorithm. ECC allows secure key exchange with smaller key sizes than customary algorithms like RSA, which makes ECC ideal for resource-constrained cloud environments (Koblitz, 1987). ECC is widely adopted for key exchange since it can compute in an efficient way and is able to provide strong security even with keys that are

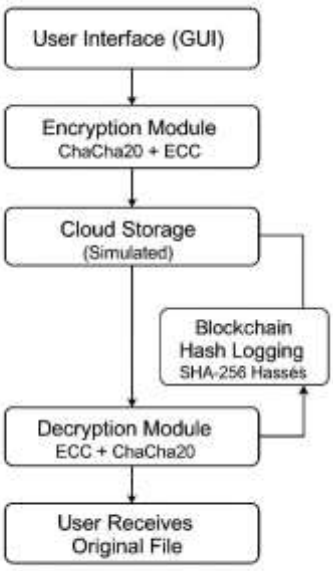
smaller. Studies show ECC-based protocols provide improved performance in cloud storage systems (Furuya et al., 2019). These procedures also keep security very high.

Blockchain technology ensures data remains whole through immutable record keeping. When someone applies blockchain toward cloud storage, it can store cryptographic hashes of files as well as enable people to verify the files have not been altered. Zhang et al. (2019) highlighted the use of blockchain for cloud data audit trails. The audit trail that is created is both decentralized and tamper-resistant. Since blockchain resists tampering it is an ideal tool. It does ensure that files do remain unmodified when someone stores them in the cloud.

Often hybrid encryption schemes use symmetric and asymmetric cryptography together for a balance of security and performance. ChaCha20 along with ECC together provide a secure solution. It is known as one for use within cloud storage systems. Research has shown (Xie et al., 2020) that integrating blockchain with hybrid encryption schemes improves the overall security of cloud storage systems by ensuring both confidentiality and integrity.

Even with promise of combining ChaCha20, ECC, and blockchain, difficulties still remain, like scalability issues as cloud storage grows, also cryptographic keys must be managed within a cloud environment. Additionally, even while blockchain strongly guarantees integrity, the number of participants within the network can impact upon its performance. Optimizing these technologies for addressing these challenges in large-scale cloud environments could be a focus of future research.

3. SYSTEM DESIGN



4. METHODOLOGY

The system architecture for the proposed secure file storage solution consists of three key components:

The ChaCha20 cipher handles the secure, fast decryption with encryption of files. The process begins by generating a 256-bit symmetric key and also a nonce (a random value that is used once per encryption). The ChaCha20 stream cipher is used for the reason that these values do encrypt the file content. Then, the encrypted file undergoes an upload phase. This file gets to the cloud.

Elliptic Curve Cryptography (ECC) for Key Exchange:

ECC is used for a secure exchange of symmetric encryption keys with the cloud service provider from the user. ChaCha20's symmetric keys are securely encrypted along with being exchanged using ECC key pairs (private and public keys) generated by the system. ECC generates keys with efficiency, and that is helpful in cloud storage scenarios. ECC uses a key size that is smaller than customary RSA encryption.

Blockchain for File Integrity Verification:

To ensure that the files stored up in the cloud do not have alterations, cryptographic hashes of each file are stored with a blockchain system. The encrypted file's hash is calculated then added to the blockchain. This addition makes a fixed log of the file’s state. The system recalculates the hash also compares the same to the stored hash of the blockchain each time that the file is accessed. The untampered file is verified upon matching hashes. An integrity breach is detected when they do not match.

5. RESULT AND DISCUSSION

For evaluating the model performance, security, and integrity verification were all used. It was the hybrid cryptographic model proposed.

ChaCha20 did perform in a better way than AES, especially at times when it encrypted the large files. Encryption and decryption times were much faster, so the system suits cloud storage when speed matters. It is because someone uses ChaCha20 that this reduces the computational overhead plus balances security with efficiency.

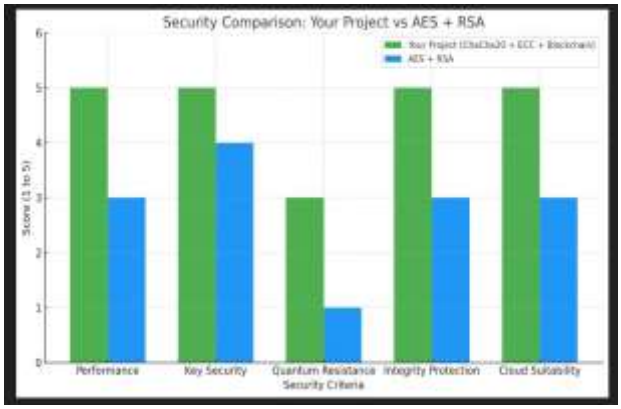
The ECC-based key exchange process was highly efficient since the system rapidly generated keys as well as securely exchanged them. ECC's use of some smaller key sizes provided it with a computational advantage. That advantage was particularly prominent within resource-constrained environments. Secure encryption key management was ensured by successfully integrating ChaCha20 with the key exchange process.

The blockchain part made file integrity certain. On the blockchain, the system safely kept the file's coded hash. By comparing of the recalculated hash with that of the stored hash, the system was able to quickly verify the file’s integrity. The use of blockchain ensured that any attempt to tamper with the

file would be detected instantly along with it added an additional layer of security to the system

Scalability and Security: The proposed system was found to be scalable, also it handled large datasets with efficiency. ChaCha20 encrypts data, ECC exchanges keys for security, and blockchain verifies integrity in order to create a strong system that secures sensitive data while maintaining high performance.

Secure comparison between our project and traditional AES + RSA approach



Why our porject is More Modern & Secure?

- ChaCha20 is a newer, faster stream cipher—built for performance even on lower-end systems.
- Safer than AES in cases of misconfigured IVs or side-channel attacks
- ECC provides strong encryption with shorter keys, making it faster and lighter than RSA
- Blockchain Hash Ledger adds a tamper-proof record of file integrity—this is not present in AES+RSA setups by default.
- Key Derivation via HKDF adds another layer of protection to the encryption key

6. CONCLUSION

This paper solves the question of how to secure cloud file storage via combining ChaCha20, ECC, as well as blockchain technology. This cryptographic approach addresses data confidentiality and integrity, so sensitive files stored on the cloud are protected against forbidden access and tampering. Blockchain integration adds an immutable decentralized layer for integrity verification, which provides a high level of security assurance. The system that was proposed performs in a highly manner, scales in a very well fashion, and secures in a strongly safe way. The system solves problems within modern cloud storage environments because of these attributes. For automated integrity verification, smart contracts might be integrated in future work. Privacy could also see improvement using multi-party computation.

7. REFERENCE

[1] B. Bhurani, A. Dogra, P. Agarwal, P. Shrivastava, T. P. Singh, and M. Bhandwal, "Smart Contracts for Ensuring Data Integrity in Cloud Storage with Blockchain," *EAI Endorsed Scal. Inf. Syst.*, vol. 11, no. 6, Apr. 2024. [Online]. Available: [URL if available].

[2] R. K. Muhammed, Z. N. Rashid, and S. J. Saydah, "A Hybrid Approach to Cloud Data Security Using ChaCha20 and ECDH for Secure Encryption and Key Exchange," *KJAR*, vol. 10, no. 1, pp. 66–82, Mar. 2025. doi: 10.24017/science.2025.1.5.

[3] B. Ranganatha Rao and B. Sujatha, "A hybrid elliptic curve cryptography (HECC) technique for fast encryption of data for public cloud security," *Research Scholar, University Postgraduate College, Secunderabad, Telangana, India*, Oct. 2023.

[4] Y. M. A. Abualkas and D.. Lalitha Bhaskari, "Hybrid Approach to Cloud Storage Security Using ECCAES Encryption and Key Management Techniques," *IEEE Trans. Cloud Comput.*, vol. 72, no. 4, pp. 92–100, Apr. 2024.

[5] Q. Zhang, Z. Zhang, J. Cui, H. Zhong, Y. Li, C. Gu, and D. He, "Efficient Blockchain-Based Data Integrity Auditing for Multi-Copy in Decentralized Storage," *IEEE Trans. Parallel Distrib. Syst.*, vol. 34, no. 12, Dec. 2023.

[6] A. Anjana and Dr. A. Singh, "An Enhanced Three Layer Cryptographic Algorithm for Cloud Information Security," *Intell. Syst. Appl. Eng.*, submitted Dec. 21, 2023; revised Jan. 27, 2024; accepted Feb. 9, 2024.

[7] V. Zevini Sabo and J. Mazadu Ismaila, "Secure File Storage on Cloud Using Hybrid Cryptography," *IJEMD-CSAI*, vol. 4, no. 1, 2025.