International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Peer Reviewed, Referred & Indexed Journal

Research Paper

Secure and Scalable Cloud Storage with Dynamic AES and Blockchain-Based Key Management with CHACHA20 Optimization

Y.Nagamalleswararao [1],K.Pavani[2],K.Akanksha Sai[3]

#1 Assistant Professor in the Department Of MCA, SRK Institute Of Technology,Vijayawada.

#2 Assistant Professor & Head of Department of MCA, SRK Institute of Technology, Vijayawada.

#3 Student in the Department of MCA, SRK Institute of Technology, Vijayawada

Abstract: This study proposes an advanced cloud data security solution that combines blockchain-based decentralized key management, dynamic AES encryption, and CHACHA20 optimization. Unlike traditional systems, encryption keys are generated dynamically using XOR operations on file hashes and blockchain block hash values, ensuring unique and incredibly secure encryption for each file. By offering distributed, tamper-proof encryption key storage, blockchain technology removes insider threats and single-point failure. Additionally, the suggested modification improves computational speed and enables compatibility for all file formats by substituting the lightweight CHACHA20 algorithm for AES and ECC. Because testing results demonstrate enhanced security strength, reduced encryption time, better scalability, and superior performance in resource-constrained scenarios, the method is suitable for real-world cloud applications.

Index terms **-** *Cloud Security, Dynamic AES Encryption, Blockchain Key Management, CHACHA20 Algorithm, Decentralized Storage, Data Encryption, Cryptography, Secure Cloud Storage, Key Generation, Data Integrity, Lightweight Encryption, Scalability*

.

1. INTRODUCTION

Because of its scalability, flexibility, and affordability, cloud computing has emerged as a key technology for data exchange and storage. However, the quick expansion of cloud services has raised significant security issues, especially with regard to safeguarding private information from insider threats, illegal access, and data breaches. Conventional cloud security techniques mostly rely on centralized key management systems, which hold encryption keys on a single server. Because all encrypted data might be exposed if the key server is compromised, this centralized solution poses a serious risk.

Cryptographic methods like Elliptic Curve Cryptography (ECC) and Advanced Encryption Standard (AES) are frequently used to secure cloud

data in order to overcome these problems. Although these techniques offer robust security, they have drawbacks such high processing costs and a lack of flexibility in dynamic cloud settings. Furthermore, many current systems are limited in their application in real-world settings involving a variety of file formats since they are built for particular data types, like photos.

Because blockchain technology is decentralized, unchangeable, and tamper-proof, it has become a viable option for improving data security in recent years. Blockchain reduces the possibility of single-point failure and guarantees the integrity of stored data by spreading data among several nodes and utilizing cryptographic hashing. By combining blockchain technology with cloud security, safe and transparent key management is made possible, making it extremely resilient to intrusions and illegal changes.

In order to provide safe and effective data protection, this study proposes a revolutionary cloud security architecture that integrates blockchain-based key management with dynamic AES encryption. To ensure that every file has a unique encryption, the system uses XOR operations on file hash and blockchain block hash values to dynamically create encryption keys. Additionally, by utilizing the lightweight CHACHA20 algorithm and supporting all file formats, the suggested extension improves the system's computational performance. This integrated method is appropriate for contemporary cloud storage applications because it offers enhanced security, scalability, and performance.

2. LITERATURE SURVEY

2.1 Blockchain aware proxy re-encryption algorithm-based data sharing scheme

ABSTRACT: All transactions are freely and decentralizedly stored on the blockchain. It's challenging to strike a balance between privacy and the usefulness of data sharing. Modifications to the permissions to access blockchain data are likewise problematic. This paper proposes a blockchain data sharing mechanism based on proxy re-encryption for this purpose. An SM2-and-blockchain proxy re-encryption technique is first developed. Businesses may safely store and transfer data thanks to blockchain data sharing. Since there is no central authority in this network, data is sent between nodes while being protected by an unchangeable cryptographic signature. Blockchain technology makes hacking and data manipulation more difficult. In the data-controlled sharing system, proxy re-encryption guarantees transaction data privacy and data security. We also provide dynamic user privileges. To guarantee user access rights, blockchain nodes divide up the work and independently control re-encryption key settings. Transparency in financial transactions is instantly altered. Lastly, because it permits dynamic blockchain data exchange while guaranteeing transaction privacy and having a lower computational cost, the performance and security tests show that this approach is appropriate for regulated blockchain data sharing. A blockchain-based proxy re-encryption method for controlled data sharing is presented in this study. To ascertain data access authorization and guarantee transaction data privacy, they are creating a proxy re-encryption method based on SM2. The method regulates the key parameters for proxy re-encryption. Limited users should be able to access encrypted data via a hybrid attribute-based proxy re-

encryption technique. This allows the proxy server to transform attribute-encrypted communications into identity-based ones.

2.2 Dynamic Multimedia Encryption Using a Parallel File System Based on Multi-Core Processors:

ABSTRACT: Growing file sizes and security and privacy issues make it essential to protect multimedia data on disk drives. The encryption technologies in use today are resource-intensive and sluggish. Because of their frequent interactions, they restrict the freedom and usefulness of users. By dynamically managing all encryption techniques with little user involvement and increased security, dynamic encryption file systems can lessen the drawbacks of conventional encryption software. The majority of cutting-edge cryptographic file systems fall short of performance standards because their architectural design overlooks the special features of multimedia data or weaknesses in key management and multiuser file sharing. Higher performance and lower computational costs are made possible by new multi-core CPUs. For multimedia disk storage, we created ParallelFS, an encrypted file system based on parallel FUSE. For both symmetric and asymmetric cyphers, the file system employs hybrid encryption and multi-core parallelism. When encryption, decryption, and key management are transparent and dynamic, usability is enhanced. Studies show that ParallelFS reads and writes multimedia files 35% and 22% quicker than sequential encryption processing.

2.3 Modified advanced encryption standard (MAES) based on non-associative inverse property loop:

ABSTRACT: The cryptographic encryption standard suggested in this article is similar to the Rijndael Algorithm, developed by Joan Daemen and Vincent Rijmen. The Extended Binary Galois Field (GF) loop has been replaced with the Inverse Property (IP) loop in the cipher's new design. Because of its broader key space, the suggested mathematical structure is more complicated than GF and might produce arbitrary randomness. Furthermore, unlike GF, IP loops are non-isomorphic and contain several Cayley table representations. This outcome demonstrates how resilient mathematical structures are to cryptanalytic assaults. To support its multimedia applications, this cryptographic system's encryption, decryption, and S-box description are all carefully measured and assessed.

2.4 Blockchain-Based Cloud Storage Using Secure and Decentralised Solution:

ABSTRACT: The combination of cloud computing with blockchain technology is a fascinating new area of study that might fundamentally change how companies manage their data in the present and the future. The benefits, drawbacks, and prospective enhancements of integrating blockchain technology with cloud storage will be examined in this article. The finest aspects of both technologies might be used to create creative, secure, practical, and affordable solutions. Digital identification, decentralized banking, and supply chain management are just a few of the previously unattainable use cases made available by the marriage of blockchain technology with cloud computing. This system merging raises a number of concerns that need to be addressed, including scalability, interoperability, security, regulatory compliance, and technological complexity. The study highlights that the successful deployment

of blockchain-based cloud solutions requires planning, infrastructure, and personnel expenditures. All things considered, businesses have a great chance to adjust to the quick and unpredictable changes in the contemporary business environment thanks to the combination of blockchain and cloud computing.

2.5 Elliptic Curve Cryptography; Applications, challenges, recent advances, and future trends: A comprehensive survey:

ABSTRACT: The most recent and sophisticated Elliptic Curve Cryptography (ECC) technique is called EC. In the Modern Digital Era (MDE), EC is frequently used to protect open communication networks and grant access to verified identities. Cloud, social media, and IoT technologies are utilized by MDE users. Regardless of the technology, the entire ecosystem must protect users' security and privacy.

Because insecure networks make data transmission and information transfer vulnerable to open channel assaults and data theft, cryptography must be explored. Thus, it is essential to understand cryptography. Cryptography encrypts messages and documents using keys so that only the intended receivers may read them. The source and destination addresses as well as mathematical techniques are required for digital signatures, cryptographic data integrity, and authentication. To illustrate the differences, the present ECDSA method and the suggested alternative are compared during signing and verification.

A wide range of scientific ideas, innovative, cutting-edge methods, and applications are examined in the thorough EC test. Scholars who wish to go deeper will find this material useful. EC-based techniques, which are more secure than RSA and Diffie-Hellman, are used in cloud computing, e-health, and e-voting. This thorough evaluation indicates that EC techniques offer significant advantages in distributed computing, interdependent networking, and asynchronous networking.

3. METHODOLOGY

i) Proposed Work:

The proposed work presents an improved architecture for cloud data security that combines blockchain-based decentralized key management with dynamic AES encryption. It is further expanded with CHACHA20 optimization. This technique ensures that every file is secured with a distinct key by dynamically generating encryption keys by an XOR operation between the file hash and the most recent blockchain block hash. While the encrypted data is kept in the cloud, these keys are safely kept on the blockchain, offering distributed and tamper-proof key management.

By providing compatibility for all file types—including documents, music, video, and images—the expansion enhances the system and increases its adaptability for practical uses. Additionally, the lightweight CHACHA20 algorithm is used as a substitute encryption technique to alleviate the high computational cost of AES and ECC. This speeds up processing and improves performance, particularly in settings with limited resources. When compared to conventional cloud security procedures, the suggested approach guarantees enhanced security, scalability, efficiency, and flexibility.

ii) System Architecture:

The user interface, encryption module, blockchain network, and cloud storage are the four primary parts of the suggested system design. A hash value of the file is created after the user uploads it using the interface. The most recent block hash is simultaneously obtained from the blockchain. A unique dynamic encryption key is created by combining these two hash values using an XOR technique. For further protection, the file is then encrypted using Elliptic Curve Cryptography (ECC) and Dynamic AES. To provide decentralized and impenetrable key management, the encrypted file is kept in the cloud while the matching encryption key is safely kept on the blockchain.

The system's adaptability is increased by the extensible architecture, which supports all file formats, including text, photos, audio, and video. In order to lower computational cost and boost processing speed, the CHACHA20 algorithm is also incorporated as a lightweight substitute for AES. Authorized users request access to the encrypted data from the cloud during file retrieval, and the matching key is safely retrieved from the blockchain. After that, the system uses the proper algorithm to decrypt the file, guaranteeing safe and effective data access. This design removes the dangers of centralized key management while improving security, scalability, and speed.

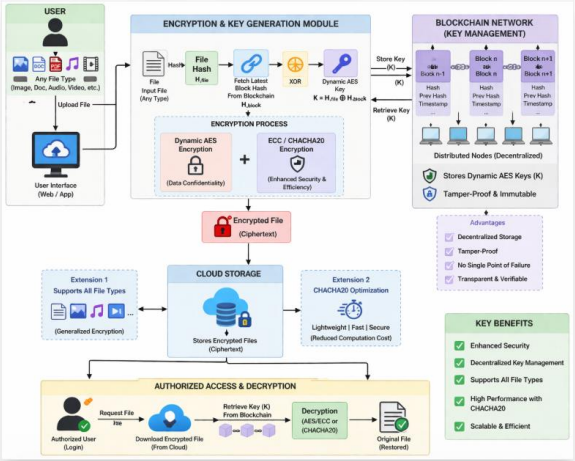

Fig 1 Proposed architecture

iii) Modules:

1. User Registration Module

enables new users to sign up for the system. For increased security, user credentials are safely kept and identity may be connected to blockchain.

2. User Authentication Module

allows for safe login using credentials. Upload, encryption, and decryption features are only accessible by authorized users.

3. File Upload Module

Any kind of file (picture, document, music, video) can be uploaded by users. The file is prepared by the system for hashing and encryption.

4. Dynamic Key Generation Module

uses the XOR technique on the file hash and blockchain block hash to create a unique AES key. guarantees that every file has a unique encryption key.

5. Encryption Module

uses Dynamic AES in conjunction with ECC or CHACHA20 (extension) to encrypt the file. offers robust data protection and confidentiality.

6. Blockchain Key Management Module

uses a decentralized blockchain network to store encryption keys. guarantees safe and impenetrable key storage without the need for a central authority.

7. Cloud Storage Module

safely keeps encrypted information on the cloud. To prevent unwanted access to the original data, only ciphertext is kept.

8. File Access & Decryption Module

Blockchain keys can be retrieved and encrypted files downloaded by authorized users. AES/ECC or CHACHA20 are used for decryption in order to recover the original data.

9. Performance Analysis Module

evaluates the encryption capabilities of CHACHA20, ECC, and AES. assesses increases in efficiency and calculation time.

iv) ALGORITHMS

1. Dynamic AES Key Generation

To improve security, this technique creates a distinct encryption key for every file. The uploaded file is first used as input, and a secure hash algorithm is used to calculate a hash value. Concurrently, the most recent block's hash is obtained from the blockchain. An XOR procedure is used to merge these two hash values to create a dynamic AES key. By ensuring that every file is encrypted with a unique key, this procedure lowers the possibility of key reuse and enhances data security overall.

2. AES + ECC Encryption

The process of encrypting files starts when the dynamic AES key is produced. The input file is optionally split into blocks, and the created key is used to encrypt each block using the AES technique. Elliptic Curve Cryptography (ECC) is used to process the AES-encrypted data in order to provide an extra degree of security. Confidentiality and secure key management are ensured by storing the finished encrypted file in the cloud and the matching encryption key safely on the blockchain.

3. CHACHA20 Encryption (Extension)

In order to increase computational efficiency, the CHACHA20 algorithm is included in the expanded system as a lightweight substitute for AES. The CHACHA20 encryption algorithm is applied straight to the file once the dynamic key is generated using the same XOR-based technique. This method preserves high security while drastically cutting down on encryption time. The linked key is kept on the blockchain, while the encrypted file is kept in the cloud. The system is now more suited for large-scale applications and situations with limited resources thanks to this enhancement.

4. EXPERIMENTAL RESULTS

The usefulness of the suggested solution in terms of security and computing efficiency was assessed using a variety of file kinds, such as photos and general data files. By guaranteeing consistent bit distribution and high sensitivity in encrypted outputs, the experimental findings show that dynamic AES

International Journal of Engineering Research and Science & Technology

encryption in conjunction with blockchain-based key management offers robust data security. By effectively removing the possibility of key tampering and single-point failure, blockchain technology for key storage improves overall system stability.

Additionally, a comparison between the CHACHA20-based extension and the conventional AES + ECC method was carried out. The results indicate that the CHACHA20 algorithm significantly reduces encryption and decryption time while maintaining a high level of security. Particularly for huge data and real-time applications, graphical comparisons demonstrate enhanced performance in terms of computing cost and processing speed. Additionally, by supporting various file formats, the expanded system exhibits improved scalability and flexibility. All things considered, the suggested solution performs better than traditional approaches in terms of security robustness, effectiveness, and usefulness in cloud contexts.

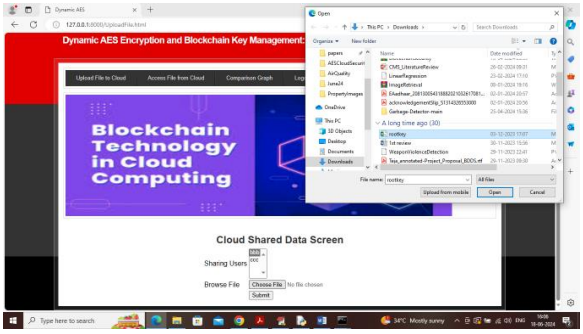

Fig 2. Upload file to cloud

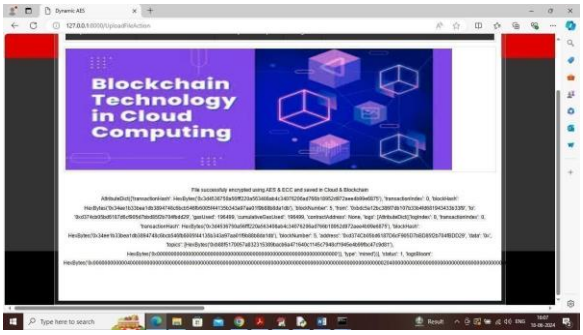

Fig 3. File saved in cloud page

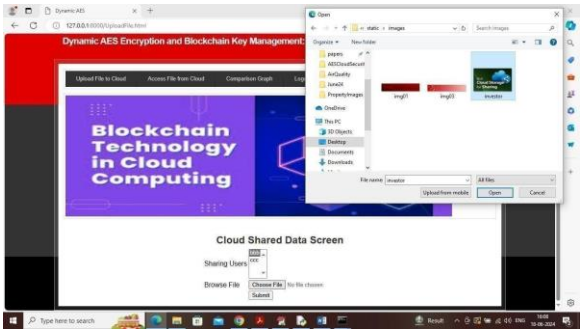

Fig 4. Upload image

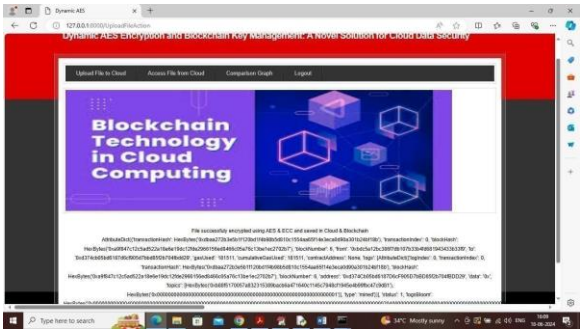

Fig 5. Image File saved in cloud page

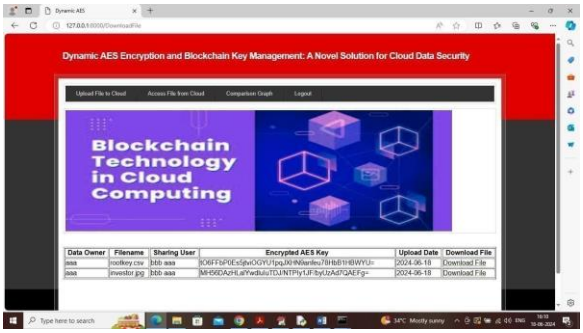

Fig6. all file details page

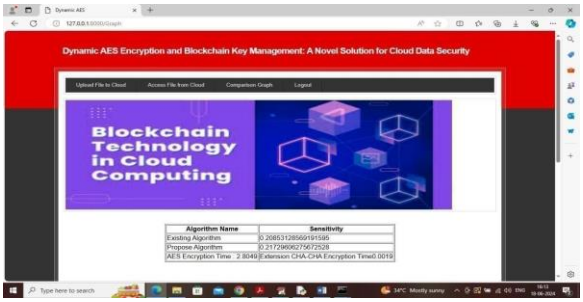

Fig.7 encryption sensitivity

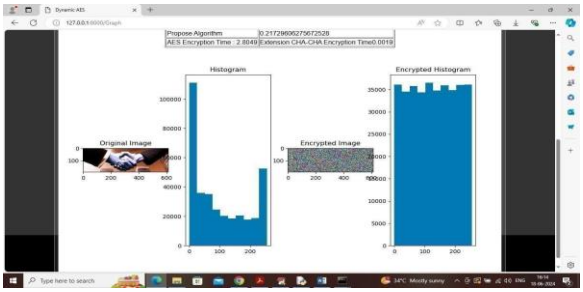

Fig.8 image encryption

Fig9. Storage Cost

5. CONCLUSION

By combining blockchain-based decentralized key management with dynamic AES encryption, the suggested approach effectively improves cloud data security while removing the dangers associated with centralized key storage. Each file is encrypted uniquely thanks to the use of dynamic key generation, and blockchain technology offers safe and impenetrable key storage. Additionally, the system's scalability and computational efficiency are enhanced by the CHACHA20-based modification, making it appropriate for practical cloud applications.

6. FUTURE SCOPE

Future work will concentrate on improving the suggested system's scalability, efficiency, and real-time applicability. To maximize efficiency in settings with limited resources, more study can examine sophisticated lightweight encryption methods beyond CHACHA20. Integration with IoT-based systems and real-time cloud sharing platforms can increase application areas and enhance usability. Additionally, latency and storage overhead can be decreased via advancements in blockchain scalability and consensus techniques. To offer intelligent and flexible cloud security solutions, the system may also be expanded with automated key management and AI-based threat detection.

REFERENCES

[1] R. Anandkumar, K. Dinesh, A. J. Obaid, P. Malik, R. Sharma, A. Dumka, R. Singh, and S. Khatak, ‘‘Securing e-health application of cloud computing using hyperchaotic image encryption framework,’’ Comput. Electr. Eng., vol. 100, May 2022, Art. no. 107860.

[2] Z. Bashir, T. Rashid, and S. Zafar, ‘‘Hyperchaotic dynamical system based image encryption scheme with time-varying delays,’’ Pacific Sci. Rev. A, Natural Sci. Eng., vol. 18, no. 3, pp. 254–260, Nov. 2016.

[3] W. Y. Chang, H. Abu-Amara, and J. F. Sanford, Transforming Enterprise Cloud Services. Berlin, Germany: Springer, 2010.

[4] B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami, and M. Ayaz, ‘‘A systematic literature review on cloud computing security: Threats and mitigation strategies,’’ IEEE Access, vol. 9, pp. 57792–57807, 2021.

[5] N. M. Sultana and K. Srinivas, ‘‘Survey on centric data protection method for cloud storage application,’’ in Proc. Int. Conf. Comput. Intell. Comput. Appl. (ICCICA), Nov. 2021, pp. 1–8.

Author profiles

Mr. Y. Nagamalleswararao completed his Master of Technology (M.Tech) from JNTUK, M.Sc (IS) from ANU, and BCA from ANU. He has expertise in System Administration, Network Administration, and Oracle Administration. He is also a Web Developer and Python Developer. Currently, he is working as an Assistant Professor in the Department of MCA at SRK Institute of Technology, Enikepadu, NTR District. His areas of interest include Artificial Intelligence and Machine Learning.

Ms. K. Pavani is working as an Assistant Professor and Head of the Department of MCA at SRK Institute of Technology, Vijayawada. She completed her M.Tech and MCA in Computer Science. She has 10 years of teaching experience at SRK Institute of Technology, Enikepadu, Vijayawada, NTR District. Her areas of interest include Machine Learning with Python and DBMS.

Mrs. ,K.Akanksha Sai[3] is an MCA student in the Department of Computer Applications (MCA) at SRK Institute of Technology, Enikepadu, Vijayawada, NTR District. He completed his degree in B.Sc. (Computers) from Sri Kakatiya Degree college, Vijayawada. His areas of interest include DBMS and Machine Learning with Python.