ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

ISSN 2454-9940

www.ijasem.org

Vol 19, Issue 2, 2025

ENHANCING CLOUD DATA SECURITY WITH DYNAMIC AES ENCRYPTION AND BLOCKCHAIN-BASED KEY MANAGEMENT

Mr. R. Prapulla Kumar1, Shaik Heemsaleem2, Bandla Hushitha3, Chithukati Lakshman4, Vadem Chenchu Teja5

#1Assistant Professor in Department of CSE, PBR VISVODAYA INSTITUTE OF TECHNOLOGY AND SCIENCE, KAVALI.

#2#3#4 #5#6 B. Tech with Computer Science & Engineering, VISVODAYA ENGINEERING COLLEGE, KAVALI

Abstract: The article introduces a new way to secure data stored in the cloud by combining Dynamic AES encryption with Blockchain-based key management. The old-fashioned method of centrally storing keys leaves all encryption keys on a single server, making it easy to attack or manipulate. To solve these problems, AES encryption keys are stored safely on Blockchain due to its decentralised and tamper-proof nature. Each file is encrypted uniquely with dynamic AES keys since they are produced via an XOR operation on file and block hash codes. Elliptic Curve Cryptography (ECC) is another method that is used to encrypt files. Uniform BIT density in encrypted pictures improves security and sensitivity, according to experimental data. With the addition of the lightweight CHACHA20 algorithm, computational costs may be decreased and the method can be adjusted to work with any type of file.

Index terms - *Cloud Security, Dynamic AES Encryption, Blockchain, Key Management, Elliptic Curve Cryptography (ECC), CHACHA20, Decentralized Storage, Tamper-proof, File Encryption, Data Integrity, Secure File Sharing, Cryptographic Hash, Secure Cloud Storage.*

.INTRODUCTION

Cloud computing has become a foundational element of modern IT infrastructure due to its ability to offer services like virtualization, on-demand access, scalability, and cost-efficiency. It supports a wide range of applications, including business processes, educational platforms, and data storage. Cloud storage services provide benefits such as high availability, ease of access, and flexible data sharing. However, as more users rely on cloud platforms to store sensitive data, concerns regarding data privacy, integrity, and security have intensified. Users require strong assurance that their data is protected against unauthorized access and manipulation.

Traditional cloud security solutions use encryption to safeguard data, relying on symmetric and asymmetric cryptographic techniques. While effective, these models often depend on centralized servers to manage encryption keys. This centralized key management approach poses serious risks, including a single point of failure, vulnerability to insider threats, and limited tamper detection. If the key server is compromised, attackers can gain access to all encryption keys and thereby decrypt sensitive files, leading to massive data breaches.

To mitigate these challenges, this paper introduces an innovative approach that combines Dynamic AES encryption with Blockchain-based key management and Elliptic Curve Cryptography (ECC). Blockchain's decentralized and immutable nature ensures that encryption keys are securely stored and tamper-proof. Dynamic AES keys, generated by combining file hashes and block hashes, provide unique encryption for each file, further enhancing security. The inclusion of ECC adds an additional layer of encryption strength. Together, these technologies create a secure and transparent cloud environment that improves trust, ensures data confidentiality, and protects against both external and internal threats.

1. LITERATURE SURVEY

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

https://www.sciencedirect.com/science/article/abs/pii/S1874490723000514

ABSTRACT: The blockchain is a decentralised, publicly accessible record of all transactions. Finding a happy medium between data sharing's practicality and the need to safeguard individuals' privacy is no easy task. Furthermore, a difficult issue is the continual modification of blockchain data access permissions. In order to achieve this goal, this study proposes a proxy re-encryption-based blockchain data sharing system. An SM2-and-blockchain-based proxy re-encryption technique is first built. Businesses may benefit from blockchain data sharing by having a safe method to store and transfer data. Because there is no central authority controlling the flow of information on this network, and because data travels from node to node protected by an immutable cryptographic signature. Because of blockchain technology, data tampering and hacking become more difficult. Data security sharing and the privacy of transaction data are both ensured by the data-controlled sharing scheme's usage of proxy re-encryption. Second, we provide a system for user privileges that may be adjusted dynamically. To accomplish the determinism of user access rights, blockchain nodes split labour and independently maintain re-encryption key parameters. The transparency of financial transactions is changed on the fly. At last, the results of the performance and security tests show that this method is suitable for Controlled blockchain data sharing as it allows for the dynamic exchange of blockchain data while still protecting transaction privacy and has lower computational overhead. This study proposes a proxy re-encryption system based on blockchain technology for controlled data exchange. They are working on an SM2-based proxy re-encryption algorithm to achieve data access authority determination and completely protect transaction data privacy. The method will regulate the proxy re-encryption key settings. Users with restricted resources should be able to access previously encrypted information by using a hybrid attribute-based proxy re-encryption approach. This method allows the proxy server to turn attribute-encrypted cypher texts into identity-based encrypted cypher texts.

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

https://www.researchgate.net/publication/369039711_Dynamic_Multimedia_Encryption_Using_a_Parallel_File_System_Based_on_Multi-Core_Processors

ABSTRACT: Because multimedia files grow in size over time and security and privacy issues are common, protecting multimedia data on disc drives is a top priority. Current cryptography systems are sluggish to respond and have large processing overhead. As a result of constant, regular encounters, they also have restricted user flexibility and usefulness. By automatically managing all encryption procedures with little user involvement and a greater security level, dynamic encryption file systems can lessen the drawbacks of traditional encryption software. However, due to their architectural design's failure to take into account the special characteristics of multimedia data or the vulnerabilities associated with key management and multiuser file sharing, the majority of state-of-the-art cryptographic file systems do not offer the required performance. The recent shift to multi-core processor design has produced a practical way to maximise performance while lowering computational costs. In this work, we created ParallelFS, a parallel FUSE-based encrypted file system for disc storage of multimedia content. The created file system employs a hybrid encryption technique for symmetric and asymmetric cyphers and takes advantage of the parallelism of multi-core machines. When encryption, decryption, and key management are carried out in a way that is completely dynamic and visible to users, usability is greatly improved. According to experiments, the created ParallelFS outperforms the methods that use standard sequential encryption processing by around 35% and 22%, respectively, when it comes to reading and writing multimedia files.

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

https://link.springer.com/article/10.1007/s11042-022-14064-8

ABSTRACT: This article proposes a cryptographic encryption standard based on the same paradigm as the Rijndael Algorithm, which was developed by Joan Daemen and Vincent Rijmen. The change is in the cipher's architecture; rather than using the Extended Binary Galois Field (GF), we now employ the Inverse Property (IP) loop. Because of its broader key space, the suggested mathematical structure may produce arbitrary randomness and is more sophisticated than GF. Furthermore, in contrast to GF, IP loops are non-isomorphic and contain several Cayley table representations. This outcome demonstrates that mathematical structures are particularly resistant to cryptanalytic assaults. To support its multimedia applications, the whole S-box description, encryption, and decryption of this cryptographic system are measured and critically assessed.

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

https://link.springer.com/chapter/10.1007/978-981-99-3878-0_23

ABSTRACT: A fascinating new field of study that has the potential to significantly change how companies handle their data both now and in the future is the combination of blockchain technology and cloud computing. The benefits, drawbacks, and possible enhancements of integrating blockchain technology with cloud storage will be examined in this article. Combining the finest aspects of both technologies may lead to creative solutions that are clear, safe, efficient, and cost-effective. Use cases like digital identification, decentralised banking, and supply chain management that were previously unattainable are made viable by the marriage of blockchain technology and cloud computing. Issues that emerge from this system merger include scalability, interoperability, security, regulatory compliance, and technological complexity, all of which need to be addressed. The report emphasises that a successful rollout of blockchain-based cloud solutions requires planning and investment in both personnel and infrastructure. Overall, the combination of blockchain and cloud computing offers organisations a fantastic chance to adjust to the quick and erratic changes in the contemporary corporate environment.

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

https://www.sciencedirect.com/science/article/abs/pii/S1574013722000648

ABSTRACT: The latest and most sophisticated method of Elliptic Curve Cryptography (ECC) is Elliptic Curve (EC). EC is frequently used to increase the security of open communication networks and to grant access to the Modern Digital Era (MDE) to those individuals whose identities have been verified. MDE users utilise a wide range of technologies, including the cloud, social media, and the Internet of Things sector. The entire environment must be able to protect users' privacy and security regardless of the tool they are using.

Because insecure networks expose data transmission and information transfer to open channel attacks and data theft, studying cryptography is necessary. Because of this, learning cryptography is essential. Cryptography is the technique of utilising keys to encrypt documents and communications so that only the people who are supposed to receive them can decode and process them. In addition to mathematical operations to determine the signature, the address of the sender and the recipient is necessary for a digital signature, cryptographic data integrity, and authentication technique. To demonstrate the distinctions between the two procedures, the solution that was offered and the method that ECDSA is now using are contrasted during the signature and verification process.

This complete examination of EC aims to fully explore a wide range of scientific ideas, cutting-edge, creative approaches, and applications. Scholars who are interested in further in-depth examination will find this material helpful. Compared to RSA and Diffie-Hellman schemes, the use and development of EC-based techniques for cloud computing, e-health, and e-voting is more secure. According to this thorough analysis, there are major advantages to using EC techniques in asynchronous networking and distributed computing as well as interdependent networking.

2. METHODOLOGY

i) Proposed Work:

The proposed system aims to enhance cloud data security by integrating Dynamic AES encryption with Blockchain-based key management and Elliptic Curve Cryptography (ECC). Instead of relying on a centralized key server, which is vulnerable to attacks and internal misuse, the system employs Blockchain to store and manage encryption keys in a decentralized and tamper-proof manner. Dynamic AES keys are generated uniquely for each file using a combination of file hash and Blockchain block hash (XORED), ensuring high security and resistance to brute-force attacks. ECC is then used to encrypt the file contents, providing lightweight yet strong encryption suitable for secure cloud environments.

In addition to encryption, the system offers a user-friendly key management interface, allowing users to upload, share, and access files securely. When a file is uploaded, the dynamic key is generated and encrypted with ECC, then securely stored on the Blockchain. Authorized users can retrieve and decrypt files by securely obtaining the key from the Blockchain. The system also includes a performance comparison module, where encryption times and sensitivity are measured using AES, ECC, and CHACHA20 algorithms. This not only validates the improved performance and security of the proposed method but also highlights its adaptability to various file types with reduced computational overhead.

ii) System Architecture:

The system architecture is designed to provide a secure and decentralized cloud storage solution by combining Dynamic AES encryption, Blockchain-based key management, and Elliptic Curve Cryptography (ECC). It begins with the user registration process, where all user details are securely recorded on the Blockchain to ensure authenticity and transparency. Once logged in, users can upload any type of file to the cloud. During file upload, a dynamic AES key is generated by XORing the file's hash with a block hash from the Blockchain. This dynamic key ensures that every file has a unique encryption pattern, enhancing data security. The generated AES key is then stored securely on the Blockchain, making it tamper-proof and decentralized.

For accessing shared files, authorized users request the file, and the system retrieves the corresponding AES dynamic key from the Blockchain. The encrypted file is then decrypted using the AES key and ECC algorithm. This dual-layer encryption ensures both key and data-level security. Additionally, the system includes a performance analysis module that compares encryption time and sensitivity between traditional AES, ECC, and lightweight CHACHA20 algorithms. This architecture not only strengthens data protection but also improves efficiency, trust, and usability in cloud-based storage environments.

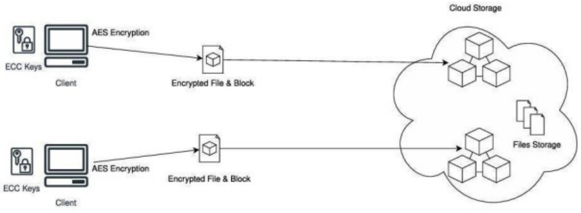


Fig 1 Proposed architecture

iii) Modules:

a. **User Sign-Up:**

New users can register into the system. All user registration details are securely stored on the Blockchain to prevent identity fraud and ensure secure authentication.

b. User Login:

Registered users can log in using their credentials. The system validates the user against the Blockchain-based registry to maintain authentication integrity.

c. Upload File:

Users can upload any type of file to the cloud. A dynamic AES key is generated using a combination of file hash and Blockchain block hash. The file is then encrypted using this key and the ECC algorithm for added security.

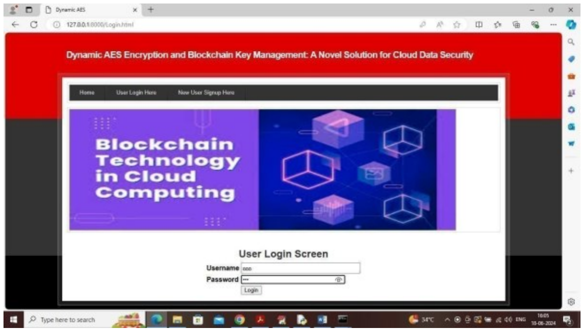
d. Access File from Cloud:

Shared users can view a list of files available in the cloud. When accessing a file, the system fetches the AES dynamic key from the Blockchain and uses the ECC algorithm to decrypt and deliver the file securely.

e. Comparison Graph:

This module encrypts a sample image using AES + ECC and also with the CHACHA20 algorithm. It compares computation time and sensitivity values to demonstrate the proposed system's efficiency and security.

3. EXPERIMENTAL RESULTS


Dynamic AES
127.0.0.1:8000/Login.html
Dynamic AES Encryption and Blockchain Key Management: A Novel Solution for Cloud Data Security
Home
User Login Here
New User Signup Here
Blockchain Technology in Cloud Computing
Type here to search

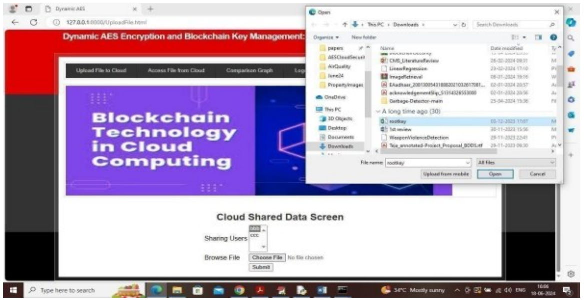
User Login Screen

Username ooo

Password ···

Login

Fig 2. user Login page



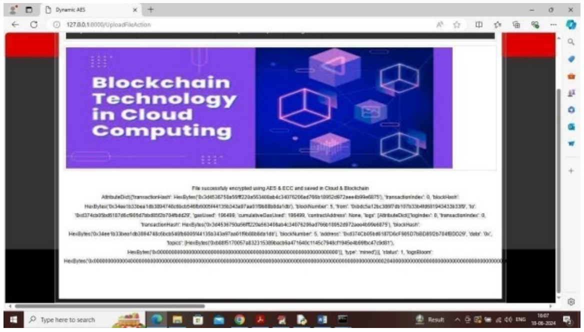
Cloud Shared Data Screen

Sharing Users

Browse File Choose File No file chosen

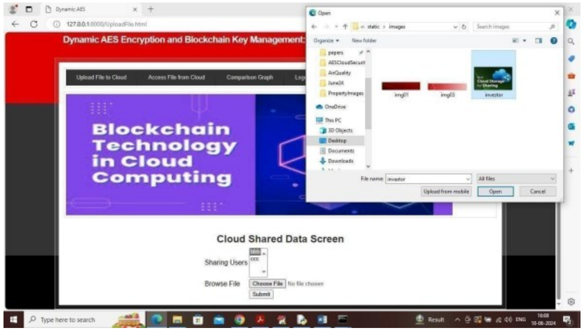
Submit

Fig 3. Upload file to cloud


Dynamic AES
127.0.0.1:8000/UploadFileAction
Blockchain Technology in Cloud Computing
Type here to search
Result

```
File successfully encrypted using AES & ECC and saved in Cloud & Blockchain
AttributeDict({'transactionHash': HexBytes('0x3d4536750a56ff220a563408ab4c34076206ad766b18952d972aee4b99e6875'), 'transactionIndex': 0, 'blockHash':
HexBytes('0x34ee1b33bea1db3894748c6bcb546fb6005f44135b343a97aa01f9b88b8da1db'), 'blockNumber': 5, 'from': '0xbdc5a12bc386f7db107b33b4fd681943433b33f9', 'to':
'0xd374cb05bd6187d6cf905d7bbd85f2b704fbdd29', 'gasUsed': 106499, 'cumulativeGasUsed': 106499, 'contractAddress': None, 'logs': [AttributeDict({'logIndex': 0, 'transactionIndex': 0,
'transactionHash': HexBytes('0x3d4536750a56ff220a563408ab4c34076206ad766b18952d972aee4b99e6875'), 'blockHash':
HexBytes('0x34ee1b33bea1db3894748c6bcb546fb6005f44135b343a97aa01f9b88b8da1db'), 'blockNumber': 5, 'address': '0xd374Cb05bd6187D6cF905D7bBD85f2b704fBDD29', 'data': '0x',
'topics': [HexBytes('0xb88f5170057a832315389bacb6a471640c1145c7948cf1945e4b66fbc47c9d81'),
HexBytes('0x0000000000000000000000000000000000000000000000000000000000000000')], 'type': 'mined'})], 'status': 1, 'logsBloom':
HexBytes('0x0000000000004000000000000000000000000000000000000000000000000000000000000000000000000000000000000000002040000000000000000000000000000
```

Fig 4. File saved in cloud page



File name investor

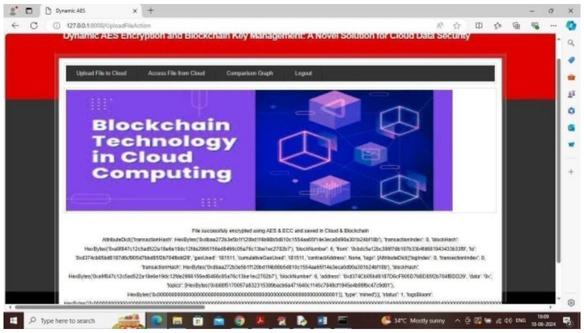
Cloud Shared Data Screen

Sharing Users

Browse File Choose File No file chosen

Submit

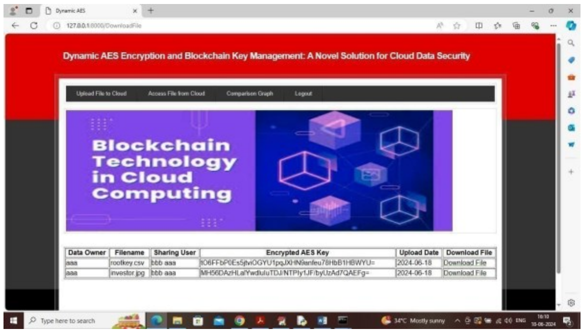
Fig 5. Upload image


Dynamic AES Encryption and Blockchain Key Management: A Novel Solution for Cloud Data Security
Upload File to Cloud
Access File from Cloud
Comparison Graph
Logout
Blockchain Technology in Cloud Computing

File successfully encrypted using AES & ECC and saved in Cloud & Blockchain

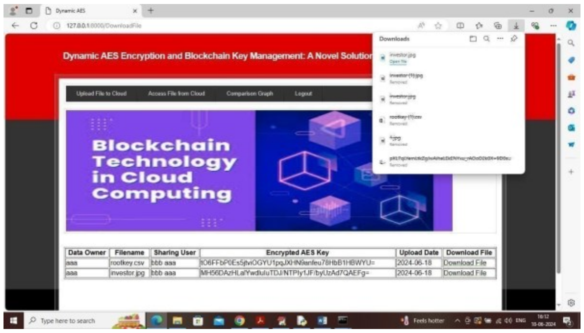
AttributeDict({'transactionHash': HexBytes('[illegible]'), 'transactionIndex': 0, 'blockHash': HexBytes('[illegible]'), 'blockNumber': 6, 'from': '[illegible]', 'to': '[illegible]', 'gasUsed': 101511, 'cumulativeGasUsed': 101511, 'contractAddress': None, 'logs': [AttributeDict({'logIndex': 0, 'transactionIndex': 0, 'transactionHash': HexBytes('[illegible]'), 'blockHash': HexBytes('[illegible]'), 'blockNumber': 6, 'address': '[illegible]', 'data': '0x', 'topics': [HexBytes('[illegible]')], 'type': 'mined'})], 'status': 1, 'logsBloom': HexBytes('[illegible]

Fig 6. Image File saved in cloud page


Dynamic AES Encryption and Blockchain Key Management: A Novel Solution for Cloud Data Security
Upload File to Cloud
Access File from Cloud
Comparison Graph
Logout
Blockchain Technology in Cloud Computing

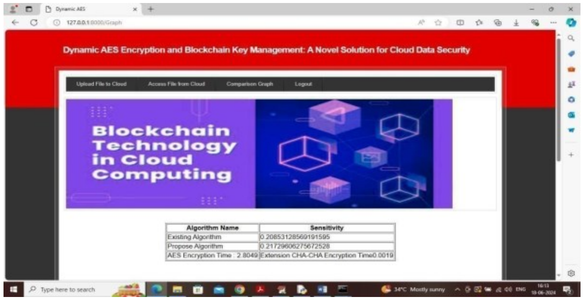
Data Owner	Filename	Sharing User	Encrypted AES Key	Upload Date	Download File
aaa	rootkey.csv	bbb aaa	fO6FFbP0Es5jtviOGYU1pqJXHN9anfeu78HbB1HBWYU=	2024-06-18	Download File
aaa	investor.jpg	bbb aaa	MH56DAzHLalYwdluluTDJ/NTPly1JF/byUzAd7QAEFg=	2024-06-18	Download File

Fig7. all file details page


Dynamic AES Encryption and Blockchain Key Management: A Novel Solution
Upload File to Cloud
Access File from Cloud
Comparison Graph
Logout
Downloads
Blockchain Technology in Cloud Computing

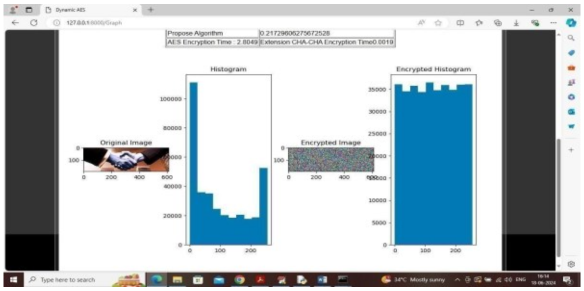
Data Owner	Filename	Sharing User	Encrypted AES Key	Upload Date	Download File
aaa	rootkey.csv	bbb aaa	fO6FFbP0Es5jtviOGYU1pqJXHN9anfeu78HbB1HBWYU=	2024-06-18	Download File
aaa	investor.jpg	bbb aaa	MH56DAzHLalYwdluluTDJ/NTPly1JF/byUzAd7QAEFg=	2024-06-18	Download File

Fig 8. Download file


Dynamic AES Encryption and Blockchain Key Management: A Novel Solution for Cloud Data Security
Upload File to Cloud
Access File from Cloud
Comparison Graph
Logout
Blockchain Technology in Cloud Computing

Algorithm Name	Sensitivity
Existing Algorithm	0.20853128569191595
Propose Algorithm	0.21729606275672528
AES Encryption Time : 2.8049	Extension CHA-CHA Encryption Time0.0019

Fig.9 encryption sensitivity



Propose Algorithm	0.21729606275672528
AES Encryption Time : 2.8049	Extension CHA-CHA Encryption Time0.0019

Fig.9 image encryption

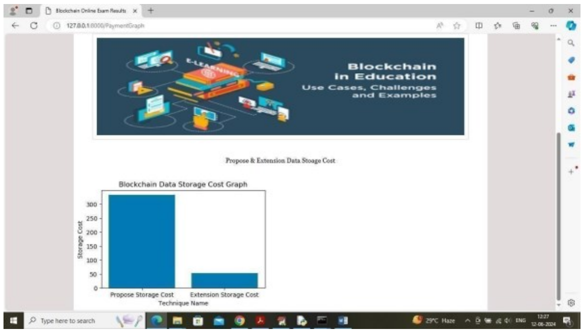


Fig7. Storage Cost

4. CONCLUSION

This study presents a thorough and creative approach to solving important security issues in cloud computing settings. The recommended strategy makes use of a hybrid dynamic encryption method that combines ECC, AES, and Blockchain. This multi-layered defensive mechanism guarantees a high level of protection for sensitive data. In the process, well-known security problems with cloud computing have been clarified, including the need for privacy reinforcement and the lack of centralised key management. The two-stage solution that has been suggested is a good fit for the issues that have been identified. To ensure that every file is encrypted uniquely and often, dynamic AES keys are initially generated. By reducing the chance of compromise, this dynamic key generation significantly improves file-level security. The second stage presents blockchain technology, which offers a decentralised, unchangeable record for safely storing encryption keys. We guarantee that unwanted access is successfully avoided during transmission and storage by encrypting these blocks using ECC public keys. These elements work together to increase consumer confidence while strengthening the security of data stored in the cloud. While service providers gain from decentralised key management, users may safely handle a variety of files with different encryption keys using a single key saved on their device. To put it simply, the recommended approach creates a robust and adaptable security framework that fits the evolving demands of cloud computing. It is effective in resolving cloud security issues. While satisfying the various needs of users or service providers, it ensures that the data is secure and confidential.

5. FUTURE SCOPE

The goal of this study is to increase the system's efficiency and capacities in the future. The algorithm's application across a wider range of businesses will be increased by expanding it to provide encryption of all file formats, not only photos. Additionally, investigating lightweight encryption techniques like CHACHA20, which may drastically lower resource needs without sacrificing security, might further optimise the system's computational performance. In the future, this approach may potentially be integrated with real-time cloud-sharing apps to give consumers safe, easy file sharing and storage options. Blockchain technology has the potential to improve its fault tolerance and scalability as it develops, providing improved defence against widespread assaults. Enhancing system performance and security in dynamic cloud environments may also be possible with research into automated key management and real-time encryption status monitoring.

REFERENCES

[1] I. Keshta, Y. Aoudni, M. Sandhu, A. Singh, P. A. Xalikovich, A. Rizwan, M. Soni, and S.

Lalar, ‘‘Blockchain aware proxy re-encryption algorithmbased data sharing scheme,’’ Phys.

Commun., vol. 58, Jun. 2024, Art. no. 102048.

[2]O.A.Khashan,N.M.Khafajah,W.Alomoush,M.Alshinwan,Alamri,S.Atawneh,andM.K.Alsmadi,‘‘Dynamicmultimediaencryptionusingaparallelfile system based on multi-core processors,’’ Cryptography, vol. 7, no. 1, p. 12, Mar. 2023.

[3] S. Hussain, T. Shah, and A. Javeed, ‘‘Modified advanced encryption standard (MAES) based on non-associative inverse property loop,’’ Multimedia Tools Appl., vol. 82, no. 11, pp. 16237–16256, May 2023.

[4] M. Rashmi, P. William, N. Yogeesh, and D. K. Girija, ‘‘Blockchain based cloud storage using secure and decentralised solution,’’ in Proc.Int. Conf. Data Anal. Insights (ICDAI), in Lecture Notes in Networks and Systems, vol. 727, N. Chaki, N. D. Roy, P. Debnath, and K. Saeed, Eds. Singapore: Springer, 2023. [Online]. Available: https://link.springer. com/chapter/10.1007/978981-99-3878-0_23, doi: 10.1007/978-981-993878-0_23.

[5] S. Ullah, J. Zheng, N. Din, M. T. Hussain, F. Ullah, and M. Yousaf, ‘‘Elliptic curve cryptography; applications, challenges, recent advances, and future

trends: A comprehensive survey,'' Comput. Sci. Rev., vol. 47, Feb. 2023, Art. no. 100530.

[6] K.Bhalla, D. Koundal, S. Bhatia, M. Khalid ImamRahmani, andM.Tahir, ''Dynamic encryption and secure transmission of terminal data files,'' Comput., Mater. Continua, vol. 71, no. 1, pp. 1221–1232, 2022.

[7] 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.

[8] F. Thabit, O. Can, S. Alhomdy, G. H. Al-Gaphari, and S. Jagtap, ''A novel effective lightweight homomorphic cryptographic algorithm for data security in cloud computing,'' Int. J. Intell. Netw., vol. 3, pp. 16–30, 2022.

[9] G. Habib, S. Sharma, S. Ibrahim, I. Ahmad, S. Qureshi, and M. Ishfaq, ''Blockchain technology: Benefits, challenges, applications, and integration of blockchain technology with cloud computing,'' Future Internet, vol. 14, no. 11, p. 341, Nov. 2022.

[10] P. Sharma, R. Jindal, and M. D. Borah, ''A review of blockchain based applications and challenges,'' Wireless Pers. Commun., vol. 123, pp. 1201–1243, 2022. [Online]. Available: https://link.springer.com/ article/10.1007/s11277-021-09176-7, doi: 10.1007/s11277021091767

[11] 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

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

[13] S. N. G.Gourisetti, Ü. Cali, K.-K.-R. Choo, E. Escobar, C. Gorog, A. Lee, C. Lima, M. Mylrea, M.Pasetti, F. Rahimi, R. Reddi, and A. S. Sani, ''Standardization of the distributed ledger technology cybersecurity stack for power and energy applications,'' Sustain. Energy, Grids Netw., vol. 28, Dec. 2021, Art. no. 100553.

[14] S. Banani, S. Thiemjarus, K. Wongthavarawat, and N. Ounanong, ''A dynamic light-weight symmetric encryption algorithm for secure data transmission via BLE beacons,'' J. Sensor Actuator Netw., vol. 11, no. 1,p. 2, Dec. 2021.

[15] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, ''Integration of blockchain and cloud of things: Architecture, applications and challenges,'' IEEE Commun. Surveys Tuts., vol. 22, no. 4, pp. 2521–2549,4th Quart., 2020.

[16] X. Liu, R. Zhang, and M. Zhao, ''A robust authentication scheme with dynamic password for wireless body area networks,'' Comput. Netw., vol. 161, pp. 220–234, Oct. 2019.

[17] M. Yousefpoor and H. Barati, ''Dynamic key management algorithms in wireless sensor networks: A survey,'' Comput. Commun., vol. 134,pp. 52–69, Jan. 2019.

[18] R. K. Chaurasiya, B. Acharya, and P. Singh, ''A comparative survey on lightweight block ciphers

for resource constrained applications,'' Int. J. High Perform. Syst. Archit., vol. 8, no. 4, p. 250, 2019

[19] 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.

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

Author's Profiles

Mr. Rondla Prapulla Kumar is currently working as an Assistant Professor in the Department of Computer Science and Engineering at Parvatha Reddy Babul Reddy Visvodaya Institute Technology and Science, Kavali, SPSR Nellore, Andhra Pradesh, India. He has 6 years of academic experience. He earned Masters of Technology in Computer Science and Engineering and is currently pursuing his Doctor of Philosophy.

Email: prapul2229@gmail.com

I am Shaik Heema Saleem, currently pursuing B. Tech in Computer Science and Engineering at Visvodaya Engineering College, Kavali. My areas of interest include Java and Python. I have earned certifications such as NPTEL's 'Cloud Computing' and social innovation in industry 4.0. I have also completed a Web Development internship at Navodita InfoTech, and python programming Internship at CodeTech It solutions and Javafullstack Certificate from EXCELR. Additionally, I have knowledge about various AI tools I am passionate about building scalable applications and solving real- world problems through technology.

I am Bandla Hushitha, currently pursuing a B. Tech in computer science and engineering at Visvodaya Engineering College, Kavali. My areas of interest include Python, Java and Web development. I have earned certifications such as NPTEL's "Municipal Solid waste management". I have also completed python programming and Web development internships. Additionally, I have knowledge about various AI tools I am passionate about building scalable applications and solving real-world problems through technology.

I am Chithukati lakshman, currently pursuing a B. Tech in Computer Science and Engineering at Visvodaya Engineering College, Kavali, SPSR Nellore, Andhra Pradesh, India. My areas of interest include Python, HTML, CSS. I have earned certificate 'Dotnet Certificate' from Wipro. I have completed a Python internship at 'Codtech IT Solutions Pvt.Ltd', ‘Young Professional from TCS iON Career Edge’, ’Communication and Team Work' from edX, I have also completed a python development internship at Cognifyz Technology Pvt. Ltd. where I gained hands-on experience in efficient code, and implementing some projects, am a proficient developer with expertise in HTML, CSS, and Python, capable of building responsive and dynamic web applications.

I am Vadem Chenchu Teja, currently pursuing a B. Tech in Computer Science and Engineering at Visvodaya Engineering College, Kavali, SPSR Nellore, Andhra Pradesh, India. My areas of interest include Java, SQL HTML, CSS and Artificial Intelligence. I have earned certifications such as 'Full Stack Development ', 'Build Your Own Generative AI Model'. ‘Young Professional from TCS iON Career Edge’, ’Communication and Team Work' from edX. I have also completed a Python internship at Pantech e learning Pvt. Ltd, 'Java programming' internship at Codtech It Solution Pvt. Ltd. and 'Java Development' at Cognifyz Technologies Pvt. Ltd. I have gained valuable experience and skills through internships and certifications, enhancing their technical expertise in computer science and engineering.