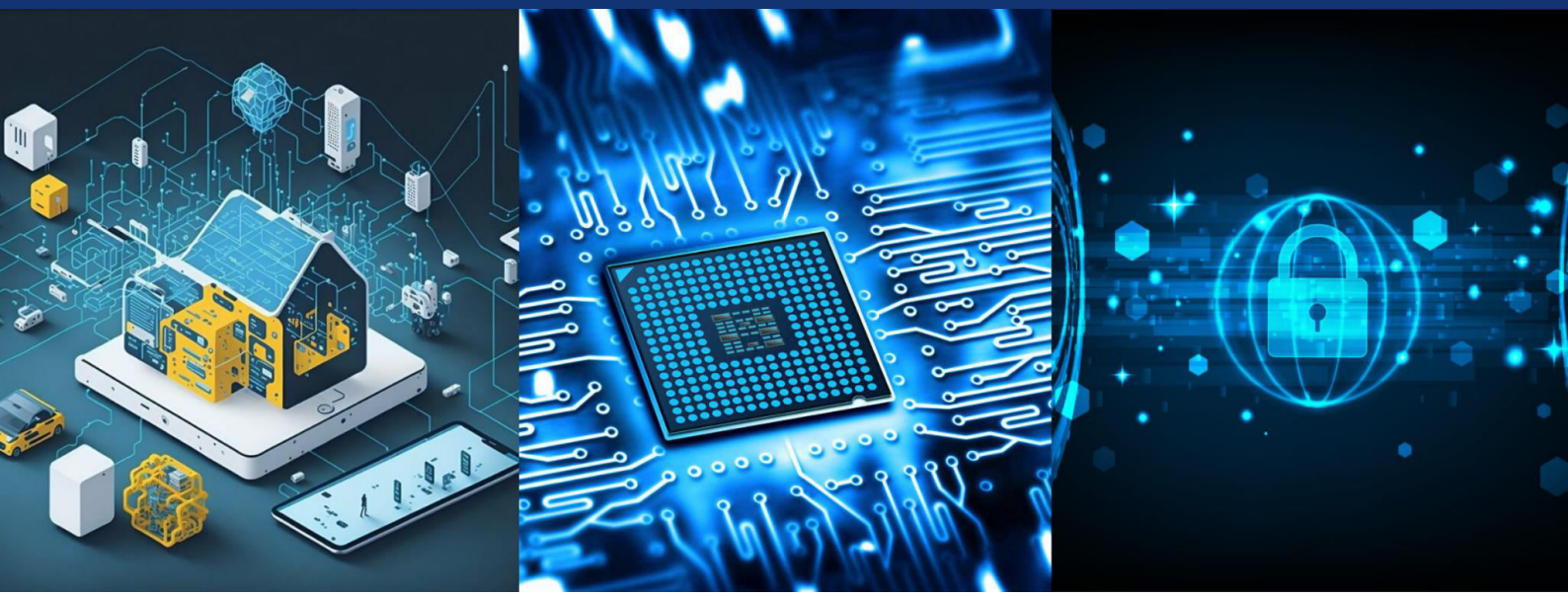
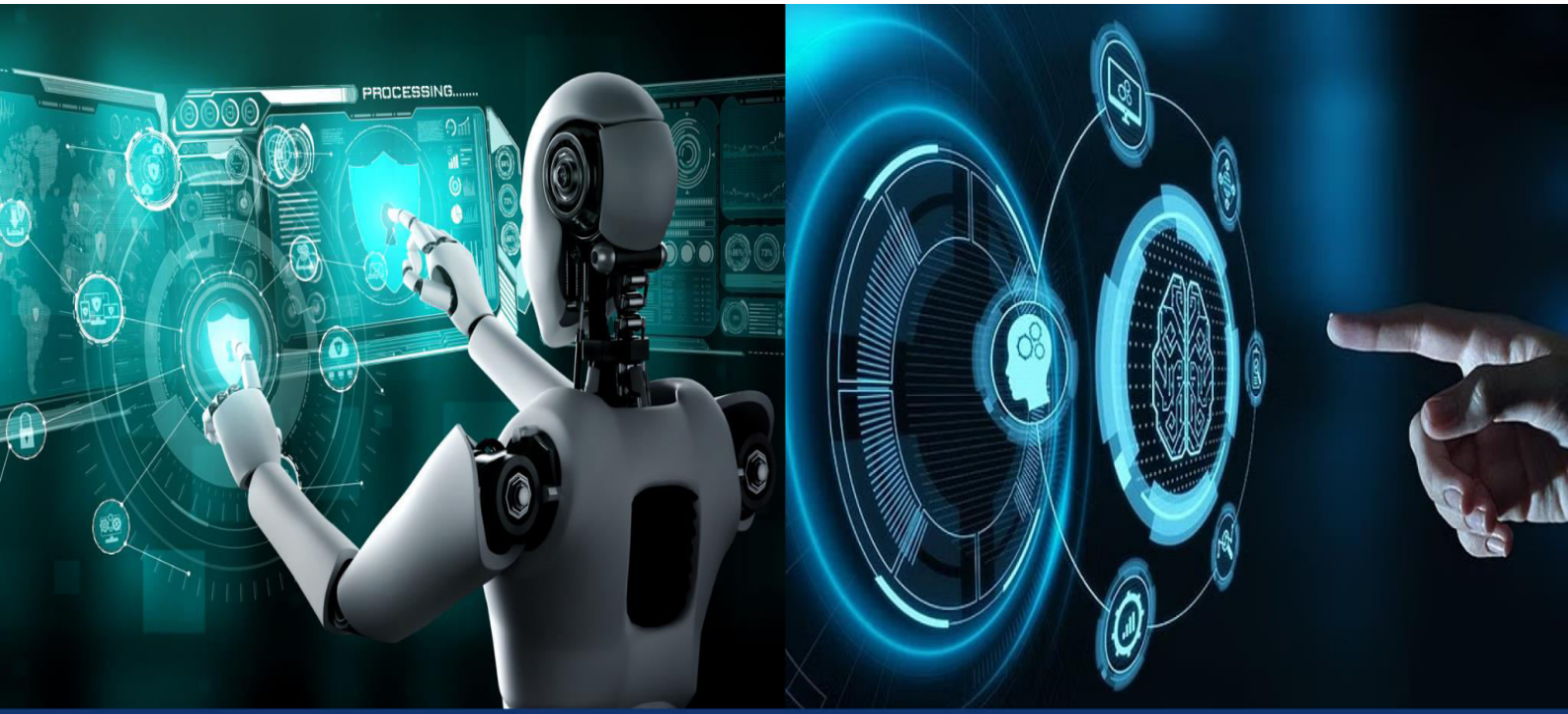
ISSN(O): 2320-9801
ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.771 **Volume 13, Issue 5, May 2025**

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI:10.15680/IJIRCCE.2025.1305266

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Dynamic AES Encryption and Blockchain Key Management: A Novel Solution for Cloud Data Security

Gowthami M, Bada Chandana, Kunukuntla Tejeswara Reddy

UG Students, Dept. of CSE, R L Jalappa Institute of Technology, Bengaluru, India

Prof. G M Anand Reddy

Associate professor Dept. of CSE, R L Jalappa Institute of Technology, Bengaluru, India

ABSTRACT: This project presents an advanced approach to securing cloud storage by integrating Blockchain technology for decentralized and tamper-resistant management of AES encryption keys. It introduces a novel technique for generating dynamic AES keys using a combination of file and block hash values, ensuring each file is encrypted with a unique and highly secure key. To further enhance the security of key exchanges, the system incorporates Elliptic Curve Cryptography (ECC), leveraging asymmetric encryption for added protection. For improved computational efficiency, the lightweight CHACHA20 algorithm is employed as an alternative to AES and ECC, maintaining strong security while boosting performance. The proposed encryption framework is designed to support a wide range of file types, increasing its applicability beyond image files. Overall, the project aims to deliver a robust and efficient cloud security solution by combining dynamic encryption, decentralized key management, and optimized cryptographic algorithms to safeguard sensitive data and ensure reliable system performance.

KEYWORDS: Cloud Security, AES Encryption, Dynamic Key Generation, Blockchain, Decentralized Key Management

I. INTRODUCTION

Cloud storage has become an integral part of modern data management, offering scalability, accessibility, and cost efficiency. However, traditional cloud architectures often rely on centralized servers for managing encryption keys—a practice that, while administratively convenient, introduces critical security risks. A single breach of the centralized key management server can potentially expose all encrypted data, threatening the integrity, confidentiality, and availability of sensitive information. This vulnerability becomes especially concerning for users, businesses, and organizations that store confidential or sensitive data on the cloud. To overcome these challenges, the integration of Blockchain technology presents a promising solution. With its decentralized and tamper-proof architecture, Blockchain enables the secure distribution of encryption keys across multiple nodes, effectively eliminating the risk of a single point of failure. This project builds on that concept by proposing a system that combines Blockchain with dynamic AES encryption, wherein encryption keys are uniquely generated for each file using a combination of file and block hash values. This approach enhances unpredictability and security, making it more resilient to attacks. The system further aims to improve computational efficiency by exploring alternative encryption algorithms and validating the performance benefits through experimentation. By addressing the limitations of centralized key management and introducing dynamic, decentralized key generation, the proposed solution not only strengthens data protection but also fosters greater trust and reliability in cloud storage systems. This comprehensive strategy is designed to ensure that sensitive data remains secure from unauthorized access, ultimately contributing to a safer cloud computing environment.

1.1 Problem Statement

Cloud storage systems relying on centralized AES key management are vulnerable to breaches, risking unauthorized access and data compromise. The lack of decentralized control creates a single point of failure, making sensitive information susceptible to theft, privacy violations, and reputational damage.

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI:10.15680/IJIRCCE.2025.1305266

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

1.2 Objective

This project aims to enhance cloud data security by integrating Blockchain-based decentralized key management with dynamic AES encryption. It seeks to ensure unique, tamper-proof key generation for each file while improving efficiency through optimized cryptographic algorithms.

II. RELATED WORK

Cloud data security has become a critical research area due to increasing concerns over data privacy, integrity, and trust in cloud environments. Several studies have proposed innovative solutions to tackle these issues from various perspectives. In the work by Sahoo et al. (2022), a **Hyperchaotic Image Encryption Framework** was developed to secure sensitive medical data in cloud-based e-Health applications. The framework dynamically selects between different chaos-based encryption and image scrambling techniques based on the attack intensity, offering a robust and adaptive solution for protecting image data. Simulation results demonstrated its effectiveness in resisting both known and unknown attacks, particularly in the sensitive domain of health information systems.

A **Systematic Literature Review** by Almorsy et al. (2021) analyzed security threats and mitigation strategies in cloud computing by reviewing 80 selected research papers. The study identified seven major threats, with data tampering and leakage as the most prevalent. The review emphasized the importance of data confidentiality, integrity, and availability, recommending Blockchain as a promising technology to mitigate these security challenges.

In another significant contribution, a **Survey on Centric Data Protection Methods** by Muthukumaran and colleagues (2022) highlighted the persistent vulnerabilities in cloud storage, such as eavesdropping, data tampering, and identity theft. The study pointed out trust issues between cloud service providers and clients, underlining the need for advanced data protection mechanisms and policy frameworks.

Lastly, Das et al. (2022) proposed a **Lightweight Homomorphic Cryptographic Algorithm** that combines symmetric and asymmetric encryption to ensure high-level security in cloud data transmission and storage. Their dual-layer approach using a new lightweight algorithm and multiplicative homomorphic schemes demonstrated promising performance metrics in securing cloud environments.
These studies collectively emphasize the urgent need for dynamic, efficient, and decentralized approaches to secure cloud data, motivating the integration of Blockchain and dynamic encryption techniques in this project.

III. PROPOSED SYSTEM

The proposed system introduces a secure and decentralized approach to encryption key management by integrating **Blockchain technology** with **dynamic AES encryption** and **Elliptic Curve Cryptography (ECC)**. Blockchain, a distributed ledger system, organizes data into sequentially linked blocks, each protected by a unique cryptographic hash. This inherent immutability and transparency make Blockchain an ideal solution for securely storing AES encryption keys.

In this framework, AES keys are not stored centrally; instead, they are distributed across the Blockchain network, with each key embedded in a separate block. This decentralized model eliminates the vulnerability of a single point of failure, significantly reducing the risk of large-scale data breaches. Furthermore, the system employs **dynamic key generation**, where AES keys are uniquely generated for each file using a combination of the file's hash and the corresponding block hash. This method ensures enhanced unpredictability and security for every encryption instance.
To further strengthen the encryption process, the system incorporates **Elliptic Curve Cryptography (ECC)**, which offers strong encryption with smaller key sizes compared to traditional public-key algorithms. ECC is used to secure the transmission and access of AES keys, thus adding an additional layer of protection without compromising performance.

Advantages of the Proposed System

- **Decentralized Key Management:** Distributing AES keys across Blockchain blocks eliminates single points of failure, making unauthorized access considerably more difficult.
- **Tamper Resistance:** Each block's unique hash ensures the integrity of stored keys, as any unauthorized modification is immediately detectable.

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI:10.15680/IJIRCCE.2025.1305266

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

- **Enhanced Security and Efficiency:** The combined use of AES for data encryption and ECC for secure key exchange provides a robust, scalable, and performance-optimized security solution.

IV. PSEUDOCODE

```
START

DISPLAY "Cloud Data Security System Ready"

 WHILE system is running:

 // Step 1: Upload file for encryption
  file = get file input from user
  DISPLAY "File received for encryption"

  // Step 2: Generate file hash
  file_hash = generate hash of the file

  // Step 3: Get latest block hash from Blockchain
  block_hash = retrieve latest block hash from Blockchain

  // Step 4: Dynamically generate AES key
  aes_key = derive AES key using file_hash and block_hash

  // Step 5: Encrypt file using AES key
  encrypted_file = AES_encrypt(file, aes_key)
  DISPLAY "File encrypted successfully"

  // Step 6: Encrypt AES key using Elliptic Curve Cryptography (ECC)
  encrypted_aes_key = ECC_encrypt(aes_key, receiver_public_key)

  // Step 7: Store encrypted AES key in a new Blockchain block
  create new block in Blockchain with:
     - transaction: store encrypted_aes_key
     - hash = compute new block hash
     - previous_hash = hash of last block
  append block to Blockchain
  DISPLAY "Encrypted AES key stored in Blockchain"

  // Step 8: Upload encrypted file to cloud storage
  upload encrypted_file to cloud
  DISPLAY "Encrypted file uploaded to cloud"

  // Optional Step 9: User retrieves file for decryption
  IF user requests file download THEN
     encrypted_file = download from cloud
     encrypted_aes_key = retrieve from Blockchain
     aes_key = ECC_decrypt(encrypted_aes_key, user_private_key)
     decrypted_file = AES_decrypt(encrypted_file, aes_key)
     DISPLAY "File decrypted successfully"

 END WHILE
```

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI:10.15680/IJIRCCE.2025.1305266

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

V. SIMULATION RESULTS

The simulation results, displayed via the Django web interface, compare the performance of the existing and proposed encryption algorithms. The proposed system demonstrates significantly higher sensitivity in detecting and securing data against threats. Notably, in the final comparison rows, the AES algorithm took **2.80 seconds** for key generation and encryption, while the **CHACHA20 extension algorithm** completed the same task in only **0.0019 seconds**, highlighting its lightweight and efficient nature. These results validate that the proposed approach not only enhances data security using dynamic AES and Blockchain integration but also optimizes performance through the CHACHA20 extension.

Figure 1: Algorithm and sensitivity

In above screen can see encryption sensitivity of both existing and propose algorithm and can see propose algorithm has high sensitivity and then in last rows can see AES took 2.80 seconds for key generation and encryption and CHACHA20 extension took only 0.0019 seconds so extension algorithm is much lighter. Scroll down above output screen to get below page

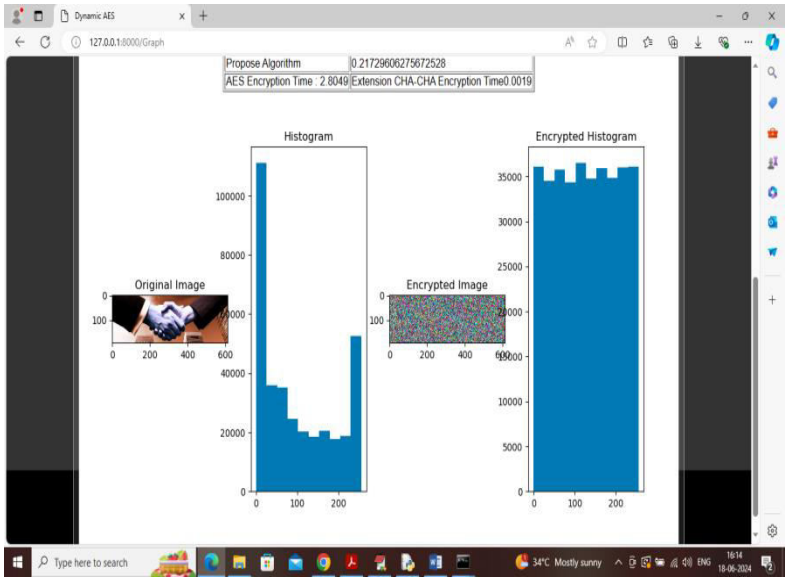


Figure 2: performance comparison

In above screen first image is the original image and then histogram of original image has very much un-uniform values as bars have too much up and down and then can encrypted image and then can see histogram of encrypted image which has uniform values as all bars are equal shape with minor gap.So by using propose paper concept we can provide decentralized security to cloud data by saving keys at multiple Blockchain nodes.

V. CONCLUSION AND FUTURE WORK

This project successfully presents a robust cloud data security solution by integrating Blockchain technology with dynamic AES encryption and Elliptic Curve Cryptography. The decentralized key management approach effectively eliminates the vulnerabilities associated with traditional centralized systems, enhancing the confidentiality and integrity of sensitive data. The dynamic generation of AES keys based on file and block hashes ensures unique encryption for each file, significantly improving security. Additionally, the inclusion of the lightweight CHACHA20 algorithm as an extension demonstrates notable improvements in computational efficiency without compromising security. Simulation results validate the proposed system's superior sensitivity and performance compared to existing methods, making it a practical choice for secure cloud storage.

For future work, the system can be expanded to support a wider range of cryptographic algorithms, allowing dynamic selection based on specific use cases or threat levels. Incorporating machine learning models could further improve threat detection and automatic adjustment of encryption parameters. Moreover, enhancing the system's scalability and interoperability with various cloud platforms will broaden its applicability. Investigating quantum-resistant encryption methods may also prepare the system for emerging security challenges posed by quantum computing. Finally, user-friendly interfaces and real-time monitoring tools can be developed to facilitate easier adoption and management of the system in real-world environments.

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,andM.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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] I. Keshta, Y. Aoudni, M. Sandhu, A. Singh, P. A. Xalikovich, A. Rizwan, M. Soni, and S. Lalar, ''Blockchain aware proxy re-encryption algorithm based data sharing scheme,'' Phys. Commun., vol. 58, Jun. 2023, Art. no. 102048.

[11] O. A. Khashan, N. M. Khafajah, W. Alomoush, M. Alshinwan, S. Alamri, S. Atawneh,andM.K.Alsmadi,''Dynamicmultimediaencryptionusinga parallel file system based on multi-core processors,'' Cryptography, vol. 7, no. 1, p. 12, Mar. 2023.

[12] 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.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

[13] 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.
[14] M. Yousefpoor and H. Barati, ''Dynamic key management algorithms in wireless sensor networks: A survey,'' Comput. Commun., vol. 134, pp. 52–69, Jan. 2019.
[15] 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.
[16] 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.
[17] 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.
[18] 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.
[19] 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/10.1007/978-981-99-3878-0_23,doi:10.1007/978-981-99 3878-0_23.
[20] 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/s11277-021-09176-7.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details