WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Survey on Integration of Dynamic AES Encryption with Blockchain Key Management

Aparna R[1], Prof. Smitha Karunan[2]

[1]Department of Computer Science and Engineering Government Engineering College, Wayanad Kerala, India aparnageth@gmail.com
[2]Department of Computer Science and Engineering Government Engineering College, Wayanad Kerala, India smithakarunan@gecwyd.ac.in

ABSTRACT—

Cloud computing offers scalability, cost- effectiveness, and accessibility but poses significant security challenges related to data confidentiality, integrity, and access control. Traditional encryption and centralized key management systems often fall short, leaving data vulnerable to unauthorized access and tampering. This survey explores innovative solutions combining advanced encryption technologies with blockchain- based key management to address these issues.

Specifically, it investigates dynamic AES methods for adaptive, file-specific encryption and blockchain's decentralized, transparent framework for secure key handling. Current cloud security techniques, such as hybrid encryption, Attribute- Based Encryption (ABE), and blockchain-based solutions, are evaluated for scalability, efficiency, and resilience. The survey also highlights emerging trends, including quantum-resistant encryption, real-time key rotation, and blockchain integration in resource-constrained environments. By synthesizing these advancements, it offers insights into creating more secure and scalable cloud systems.

Index Terms- Dynamic AES Encryption, Blockchain Key Management, Attribute-Based Encryption (ABE), Decentralized Key Storage, Access Control, Key Rotation

I. Introduction

Cloud computing has changed how organizations and individuals store, handle, and retrieve data. By providing on- demand resources and scalable infrastructures, it has emerged as a key technology in numerous sectors, such as healthcare, finance, education, and entertainment. It's capacity to enhance resource use, lower expenses, and offer remote access has resulted in extensive adoption. Nonetheless, in addition to these benefits, cloud computing poses serious security issues that undermine user trust and restrict wider acceptance. Primary concerns involve maintaining the confidentiality, integrity, and accessibility of sensitive information given to external service providers.

One of the primary challenges in cloud security lies in protecting data from unauthorized access and tampering during storage and transmission. Traditional encryption methods, while crucial, often rely on static keys and centralized management systems. These approaches are vulnerable to single points of failure, exposing data to risks such as key compromise, insider threats, and man-in-the-middle attacks.

Additionally, centralized key management systems lack transparency, making it difficult for users to monitor and audit access to their data effectively. The dynamic nature of cloud environments, coupled with the increasing sophistication of cyberattacks, necessitates innovative security solutions.

To address these challenges, it proposes a hybrid approach that integrates Dynamic Advanced Encryption Standard (AES) encryption with blockchain-based key management. Dynamic AES introduces file-specific encryption by generating unique and adaptable keys for each data instance, significantly reducing the risks associated with key compromise. Periodic key rotation further strengthens the system's resilience against attacks. Blockchain technology, on the other hand, offers a decentralized and tamper-proof framework for managing encryption keys. Its immutable ledger ensures secure key storage, auditability, and resistance to unauthorized modifications, thereby eliminating the vulnerabilities associated with centralized systems. By combining these technologies, the hybrid framework ensures robust data security, fine-grained access control, and enhanced trust in cloud systems.

The survey aims to explore existing techniques in cloud security, including traditional encryption methods, blockchain- based solutions, and hybrid models. It evaluates the strengths and limitations concerning key metrics such as scalability, computational efficiency, and resistance to emerging threats. Furthermore, it contextualizes the proposed hybrid approach within the current research landscape, demonstrating its po- tential to address existing gaps and advance the state of cloud security. By providing a comprehensive review and analysis, it seeks to guide researchers and practitioners in developing scalable, efficient, and secure solutions for modern cloud environments.

II. LITERATURE REVIEW

Many research efforts in cloud security investigate sophisticated encryption and key management methods, with each making a distinct contribution to the domain. Nonetheless, these methods frequently encounter issues concerning scalability, computational effectiveness, or versatility. The suggested hybrid approach—combining Dynamic AES Encryption with Blockchain-Based Key Management—successfully tackles these shortcomings, offering a strong and scalable solution for contemporary cloud settings. An analysis and comparison of various existing methods with the proposed approach is done as follows.

[1] One approach involves the use of Dynamic AES Encryption alongside blockchain and Elliptic Curve Cryptography (ECC). This method guarantees encryption specific to each file and distributed key storage, improving data privacy and key administration. Nonetheless, it experiences computational burden and delays as a result of combining various technologies. The suggested approach enhances this by flexibly modifying AES encryption according to data sensitivity and integrating blockchain mainly for key management, thereby lowering computational complexity while ensuring strong security.

[2]A different study investigates Optimized Encryption for Multi-Cloud Containers, combining hybrid AES-RSA and AES-ECC techniques to protect data while migrating containers. Although the method effectively balances security and resource consumption, its scalability in multi-cloud settings is still restricted. The suggested approach, utilizing a permissioned blockchain and Dynamic AES, attains improved scalability and adaptability for various cloud infrastructures.

[3] Another studies on End-to-End Encryption (E2EE) for Cloud Storage offering formal cryptographic frameworks to protect data from server breaches. Although it provides robust confidentiality assurances, it encounters difficulties in executing sophisticated features such as metadata safeguarding and session administration. The suggested approach, utilizing blockchain’s unalterable ledger and Attribute-Based Encryption (ABE), guarantees secure key administration and precise access control, enhancing its practicality for real-world scenarios.

[4]A hybrid method is used which merges Encryption and Compression thus aims to minimize data volume while maintaining privacy. This approach shows notable enhancements in both processing durations and space efficiency. Nonetheless, it is mainly designed for text-oriented data and is not suitable for multimedia material. The suggested approach’s adaptability in managing various data types and varying encryption strength offers a broader solution.

[5]A Modified AES (MAES) algorithm incorporates extra cryptographic layers to enhance encryption speed and ensure data integrity. Although it provides improved computational efficiency, it does not have decentralized key management, which renders it susceptible to single points of failure. The suggested approach addresses this limitation by incorporating blockchain for secure and decentralized key storage, thereby ensuring enhanced robustness.

[6] An additional study integrates ABE with Federated Learning and Blockchain to protect medical data in healthcare. Although it performs exceptionally in maintaining privacy and decentralized learning, its computational requirements are substantial, particularly during encryption. The suggested approach efficiently utilizes ABE for access management, paired with blockchain for key administration, minimizing overhead while providing comparable privacy and security advantages.

[7] Investigations that combine Blockchain and Searchable Encryption enable precise access control and safe keyword searching. While it reduces dependence on centralized systems, the computational expense of multi-keyword searches on blockchain continues to be significant. The suggested approach lowers these costs by emphasizing key management while providing efficient and secure access via ABE.

[8]A new Blockchain-GAN-Based System improves inventory management security through the combination of machine learning and cryptography. Although useful for particular industrial uses, the intricacy of integrating GANs and blockchain may result in latency problems. The suggested approach attains comparable data integrity and access control via a more straightforward, efficient structure, enhancing its scalability and versatility.

[9] Next approach is an innovative Blockchain-Based e-KYC System securing customer identity data using CP- ABE and smart contracts. While excelling in privacy and compliance, it is primarily focused on financial applications and lacks versatility for broader cloud scenarios. The proposed method, with its scalable and dynamic architecture, can address diverse use cases beyond financial systems.

[10] Finally, a Hybrid Encryption Model that combines Homomorphic Encryption and Blowfish for enhanced data security. While it ensures confidentiality and efficient processing, the lack of decentralized key management makes it less robust against insider threats. The proposed method’s use of blockchain addresses this, ensuring tamper-proof key management alongside efficient encryption.

III. Proposed Model

The proposed method uniquely combines encryption, blockchain, and Attribute-Based Encryption (ABE) to address critical shortcomings in existing cloud security approaches. Its dynamic adaptability ensures optimal encryption based on the sensitivity of the data. Unlike static systems that apply a uniform encryption level, the proposed method dynamically adjusts encryption strength, providing robust security for sensitive data while optimizing performance for less critical information. This adaptability reduces unnecessary computational strain, striking a balance between security and efficiency.

The solution also excels in scalability, leveraging permissioned blockchain technology for key management. Traditional systems often struggle to scale in multi-tenant or distributed environments due to centralized bottlenecks or excessive resource demands. The decentralized nature of the proposed blockchain implementation ensures seamless scalability, enabling secure key management and data access across large, distributed cloud systems without performance degradation.

Another key strength lies in its fine-grained access control achieved through ABE. Unlike conventional access control systems that rely on predefined roles or broad permissions, ABE allows data owners to define flexible policies tailored to specific user attributes, such as roles, departments, or clearance levels. This ensures that sensitive data is only accessible to authorized users, significantly enhancing privacy and compliance with security regulations.

Finally, the proposed method demonstrates reduced overhead compared to systems that combine complex encryption algorithms and resource-intensive processes. By focusing blockchain usage on key management and employing dynamic AES for data encryption, the approach minimizes latency and computational demands while maintaining robust security. This balance makes it more efficient and practical for real-world applications where performance and security are equally critical.

By addressing these limitations in existing methods, the proposed solution emerges as a comprehensive framework for secure, efficient, and adaptable cloud data protection. Its ability to dynamically adjust to varying security needs, scale effectively, enforce precise access control, and reduce resource consumption positions it as a highly versatile and practical solution for modern cloud environments.

IV. CONCLUSION

Cloud computing has emerged as an essential element of modern digital environments, providing scalability, efficiency and accessibility. Nonetheless, it poses considerable security issues, such as safeguarding sensitive information and handling encryption keys. The study examined current approaches in cloud security, concentrating on encryption innovations, blockchain incorporation, and hybrid frameworks. Although these methods tackle important concerns such as data confidentiality and access control, they frequently encounter challenges related to scalability, computational efficiency, and adaptability to changing environments.

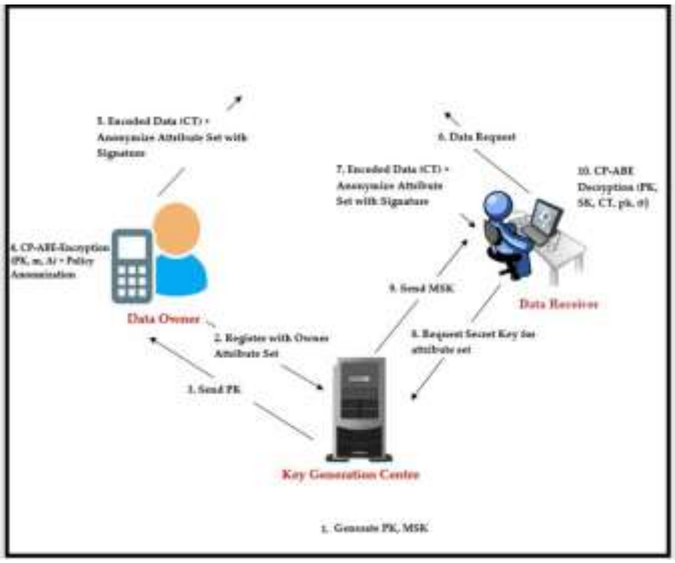
5. Encoded Data (CT) + Anonymize Attribute Set with Signature
6. Data Request
7. Encoded Data (CT) + Anonymize Attribute Set with Signature
10. CP-ABE Decryption (PK, SK, CT, pk, σ)
4. CP-ABE-Encryption (PK, m, A) + Policy Anonymization
Data Owner
9. Send MSK
Data Receiver
2. Register with Owner Attribute Set
8. Request Secret Key for attribute set
3. Send PK
Key Generation Centre
1. Generate PK, MSK

Fig. 1. System Architecture

The hybrid approach merging Dynamic AES Encryption with Blockchain Enabled Key Managementsuccessfully connects these gaps. Dynamic AES offers flexible, file-oriented encryption, whereas blockchain guarantees decentralized, immutable key management. Incorporating Attribute-Based Encryption (ABE) improves access control, rendering the framework appropriate for sensitive settings and multi-tenant situations. This all-encompassing strategy harmonizes security, scalability, and efficiency, exceeding the performance of conventional methods.

Future studies need to concentrate on improving scalability, incorporating quantum-resistant encryption, and utilizing AI for better key management. Moreover, initiatives aimed at enhancing energy efficiency and interoperability will bolster the practical relevance of this framework. By tackling these issues, the suggested solution opens the door for safe, scalable, and effective cloud systems, enhancing trust and uptake across sectors.

References

[1] Mohammed Y Shakor, Mustafa Ibrahim Khaleel, Mejdl Safran, Sultan Alfarhood, and Michelle Zhu. Dynamic aes encryption and blockchain key management: A novel solution for cloud data security. *IEEE Access*, 2024.

[2] Mohammad A Altahat, Tariq Daradkeh, and Anjali Agarwal. Optimized encryption-integrated strategy for containers scheduling and secure migration in multi-cloud data centers. *IEEE Access*, 2024.

[3] Matilda Backendal, Hannah Davis, Felix Gu¨nther, Miro Haller, and Kenneth G. Paterson. A formal treatment of end-to-end encrypted cloud storage. Cryptology ePrint Archive, Paper 2024/989, 2024.

[4] A Abdo, Taghreed S Karamany, and Ahmed Yakoub. A hybrid approach to secure and compress data streams in cloud computing environment. *Journal of King Saud University-Computer and Information Sciences*, 36(3):101999, 2024.

[5] Md Sadi Arman, Shamim Al Mamun, and Nuray Jannat. A modified aes based approach for data integrity and data origin authentication. In *2024 3rd International Conference on Advancement in Electrical and Electronic Engineering (ICAEEE)*, pages 1–6. IEEE, 2024.

[6] Atul B Kathole, Kapil Netaji Vhatkar, Ankur Goyal, Shivkant Kaushik, Amita Sanjiv Mirge, Prince Jain, Mohamed S Soliman, and Mohammad Tariqul Islam. Secure federated cloud storage protection strategy using hybrid heuristic attribute-based encryption with permissioned blockchain. *IEEE Access*, 2024.

[7] Reyazur Rashid Irshad, Zakir Hussain, Ihtisham Hussain, Shahid Hus- sain, Ehtisham Asghar, Ibrahim M Alwayle, Khaled M Alalayah, Adil Yousif, and Awad Ali. Enhancing cloud-based inventory management: A hybrid blockchain approach with generative adversarial network and elliptic curve diffie helman techniques. *IEEE Access*, 12:25917–25932, 2024.

[8] Liang Yan, Lina Ge, Zhe Wang, Guifen Zhang, Jingya Xu, and Zheng Hu. Access control scheme based on blockchain and attribute-based searchable encryption in cloud environment. *Journal of Cloud Comput- ing*, 12(1):61, 2023.

[9] Somchart Fugkeaw. Enabling trust and privacy-preserving e-kyc system using blockchain. *IEEE Access*, 10:49028–49039, 2022.

[10] KR Sajay, Suvanam Sasidhar Babu, and Yellepeddi Vijayalakshmi. Enhancing the security of cloud data using hybrid encryption algorithm.

[11] *Journal of Ambient Intelligence and Humanized Computing*, pages 1–10, 2019.