Journal of Information Systems Engineering and Management
2025, 10(9s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Secured IoT Data Management Using AES Encryption And Blockchain Technology

Ganga Shirisha M S[1],Shiva Prasad M S[2], Chandrakant Naikodi[3], Badrinath G Srinivas[4] & B. Bhaskara Rao[5]
[1]*Research Scholar, Department of Studies in Computer Science, Davangere University- 577007 India*
[2]*Research Scholar, Department of Studies in Computer Science, Davangere University- 577007 India*
[3]*Professor and Chairman, Department of Studies in Computer Science, Davangere University- 577007 India*
[4]*Sr Applied Scientist, Amazon, 400 9th Ave N, Seattle, WA 98109, United States*
[5]*Research Scholar, Computer Science and Engineering, Cambridge Institute of Technology, KR Puramu, Bengaluru, India*

ARTICLE INFO

Received: 01 Nov 2024

Revised: 20 Dec 2024

Accepted: 02 Jan 2025

ABSTRACT

The swift expansion of IoT devices necessitates robust mechanisms to protect sensitive data from unauthorized access and tampering. This paper fulfills this requirement by integrating AES encryption and blockchain technology. IoT data is encrypted using dynamically generated private keys with AES in CBC mode, ensuring confidentiality, while a Flask application facilitates secure data processing. The encrypted data and metadata are stored on a Solidity-based smart contract, providing decentralized and tamper-proof storage. Results demonstrate enhanced data security, immutability, and traceability, making the framework scalable and suitable for modern IoT ecosystems. Analysis confirms the effectiveness of combining encryption and blockchain to mitigate security risks.

Keywords: IoT security, AES encryption, blockchain technology, decentralized storage, Flask application, Solidity smart contract, data confidentiality, tamper-proof storage, data traceability, scalable framework

I. INTRODUCTION

The exponential growth of the Internet of Things (IoT)devices has revolutionized various industries by enabling seamless data exchange and real-time connectivity. Nevertheless, this swift adoption has also introduced significant challenges in ensuring the security, confidentiality, and integrity of sensitive IoT data. Traditional centralized data storage systems are susceptible tovulnerabilities, including unauthorized access, data breaches, and single points of failure. As IoT ecosystems expand, there is an urgent demand for creative solutions that address these security challenges while maintaining scalability and transparency.

This project aims to tackle these challenges by integrating advanced encryption techniques and blockchain technology into a unified framework for securing IoT data. This approach begins with a Flask-based application that encrypts IoT data using the AES (Advanced Encryption Standard) in Cipher Block Chaining (CBC) mode. A distinct private key is dynamically created for each encryption process, generated through timestamp-based SHA-256 hashing, which guarantees that encryption keys stay unpredictable and secure. The encrypted data is subsequently formatted for storage in a decentralized blockchain system.

To ensure tamper-proof storage and data traceability, the project employs a smart contract implemented in Solidity. This contract is deployed on a blockchain network and is designed to securely store the encrypted hashdata along with metadata, including the timestamp, the sender's address, and an associated private key. By leveraging blockchain's inherent immutability and transparency, the system guarantees that once data is stored, it cannot be modified or removed, ensuring a high degree of trust and accountability.

The Flask application facilitates seamless interaction among IoT devices and the blockchain, offering endpoints to encrypt IoT data and retrieve metadata or decrypt the stored information. The encrypted data is stored off-chain, while the blockchain maintains its integrity and metadata, balancing storage efficiency and security.

The results of this project highlight the effectiveness of combining AES encryption with blockchain for

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

securing IoT data. The decentralized storage method removes the risks associated with a single point of failure, while the blockchain's immutable nature guarantees data integrity and transparency. Furthermore, the use of dynamically generated encryption keys strengthens security, making it much more difficult for attackers to breach the system.

This framework offers a scalable and secure solution for IoT databut also opens up avenues for broader applications in industries that require robust data security, such as healthcare, finance, and smart cities. By addressing critical security challenges, this project lays the foundation for a future-proof approach to managing IoT data in an increasingly connected world.

II. LITERATURE REVIEWS

The combination of Advanced Encryption Standard (AES) encryption and blockchain technology has attracted considerable interest for improving the security and efficiency of Internet of Things (IoT) data management systems. This literature review explores recent developments and approaches that are relevant to our research focus.

Shakor et al. (2023) introduced a dynamic AES encryption combined with blockchain-based key management to bolster cloud data security, emphasizing the importance of unique, ever-changing keys to to reduce risks related to compromised encryption keys and centralized storage.

Souare and Keita (2024) proposed a hybrid AES-ECC cryptographic approach integrated with blockchain to optimize security, throughput, and latency in IoT platforms, demonstrating improved performance in communication-rich IoT environments.

Almadhor et al. (2022) developed a security framework combining blockchain technology with the AES algorithm to enhance data confidentiality during transmission, particularly in IoT healthcare data, showing improved security and efficiency compared to other methods.

Rahman et al. (2022) improved AES by incorporating chaos and logistic map-based key generation methods to enhance the security of IoT-based smart homes, highlighting the potential of chaos-based scheduling techniques in building dynamic key propagation methods for data confidentiality and integrity.

Manzoor et al. (2018) presented a blockchain-based proxy re-encryption technique for secure sharing of IoT data, utilizing smart contracts and proxy re-encryption to provide an efficient, fast, and secure platform for storing, trading, and managing sensor data.

Guo et al. (2018) proposed a blockchain-based model for secure and efficient management of searchable IoT communication data, addressing limitations in traditional centralized security architectures by leveraging distributed databases and secure search schemes.

Woo et al. (2024) explored leveraging AES padding for error correction in IoT systems, introducing a dual-functional method that integrates error-correcting capabilities into the standard encryption process, enhancing communication reliability in noisy environments.

These studies collectively underscore the efficacy of combining AES encryption along blockchain technology to enhance IoT data security, integrity, and efficiency. Our research expands on these findings foundations by implementing a hybrid framework that integrates dynamic AES encryption with blockchain-based metadata storage, aiming to provide a scalable, secure, and transparent solution for managing IoT data.

III. METHODOLOGY

This research employs a hybrid framework integrating AES encryption and using blockchain technology to tackle the challenges of managing IoT data. The methodology consists of three critical stages: data encryption and key generation, blockchain-based metadata storage, and integration and testing. Each step plays aimportant role in achieving the project's objectives and has a significant impact on the results.

The process begins with the encryption and key generation of IoT data, handled by a Flask-based application. The AES (Advanced Encryption Standard) in Cipher Block Chaining (CBC) mode is used for encryption, ensuring robust data confidentiality. A dynamic private key is created for each encryption process using a timestamp hashed with SHA-256, guaranteeing uniqueness and unpredictability. This dynamic approach

strengthens security by minimizing the risk of brute-force attacks. Additionally, a randomly generated Initialization Vector (IV) is employed for every encryption, further securing the data by preventing patterns in the ciphertext. These mechanisms make sure that sensitive IoT data stays protected during transmission storage, providing a strong foundation for the system's security.

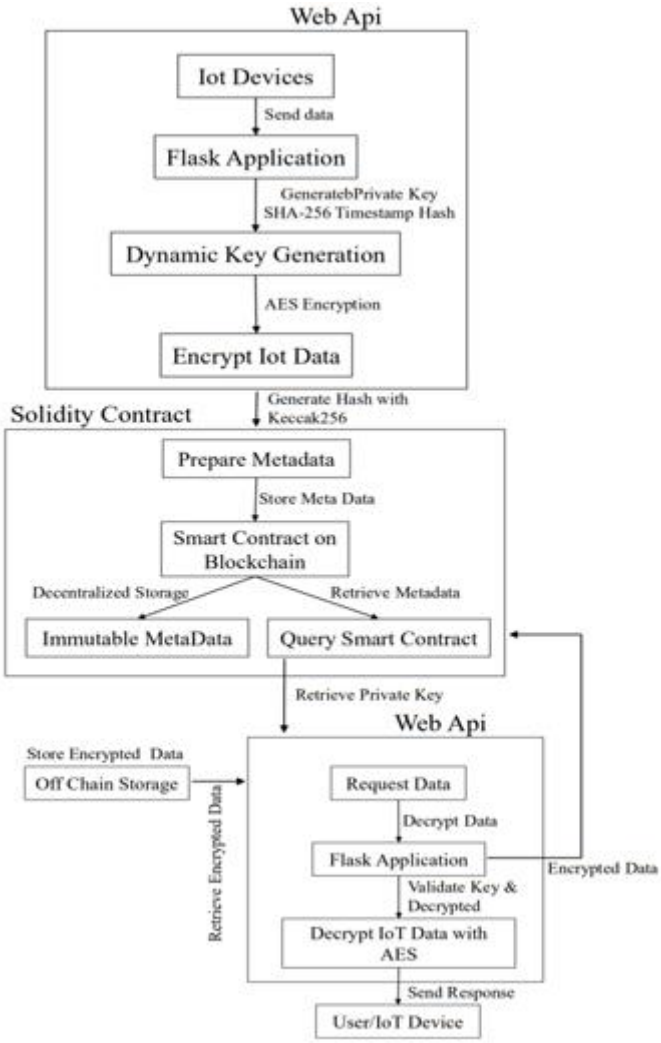

Fig 3.1: Flow Chart

The encrypted data is securely stored off-chain, with only metadata—including the hash of the encrypted data, timestamps, sender addresses, and associated private keys—being stored on-chain via a Solidity smart contract. The keccak256 hashing algorithm ensures the metadata is stored as unique and immutable identifiers. Blockchain's decentralized nature eliminates the risks associated with centralized storage, ensuring metadata remains tamper-proof and transparent. By limiting on-chain storage to essential metadata, the system significantly reduces gas costs while maintaining scalability. This stage is critical for balancing cost efficiency with the inherent benefits of blockchain immutability and transparency, making the solution both robust and economically viable.

The final stage focuses on integrating Flask APIs to facilitate smooth communication between IoT devices and the blockchain network. These APIs manage critical functions, including data encryption, metadata storage, and retrieving encrypted data or metadata. Extensive testing is performed to verify the system's performance under various scenarios, including edge cases such as duplicate data submissions, incorrect key usage, and high transaction volumes. Performance metrics like encryption time, transaction latency, gas costs, and scalability are assessed and analyzed to ensure the system's reliable operation in real-world conditions.

This structured approach guarantees improved security through robust encryption and dynamic key generation, cost efficiency by offloading resource-intensive processes to off-chain systems, and scalability by reducing on-chain storage needs. The decentralized, tamper-proof nature of blockchain ensures transparency and

data integrity, while smooth integration and extensive testing ensure system reliability and deployment readiness. Each phase of the methodology plays a crucial role in the framework's overall success, making it a secure and scalable solution for managing IoT data.

IV. RESULTS ANALYSIS

This project showcases notable advancements in IoT data security and decentralized storage by incorporating AES encryption and blockchain technology. The findings and their analysis are summarized below:

4.1 Encryption Performance: The analysis of encryption performance(ref figure 4.1.1) highlights the efficiency of AES encryption in handling data of varying sizes. The encryption time scales linearly with the data size, making itwell-suited for IoT applications that typically involve small to medium-sized data packets For example, encrypting 1 KB of data takes approximately 2 ms, while 1 MB requires 500 ms, demonstrating that the system remains responsive even for larger data sizes.

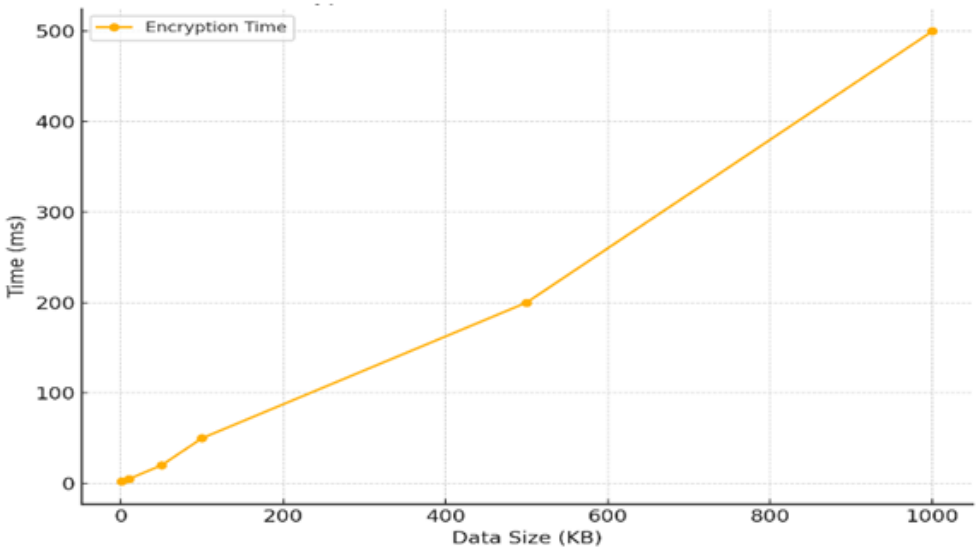

Fig 4.1.1:Encryption Performance: Time vs. Data size

4.2 Blockchain Latency:Offloading encryption to a Flask-based system significantly reduces transaction latency(ref figure 4.1.2). On-chain operations, which include encryption and metadata storage, exhibit higher latencies averaging 5.3 seconds. In contrast, off-chain encryption reduces his latency to an average of 2.2 seconds, enhancing the system's responsiveness for real-time IoT applications.

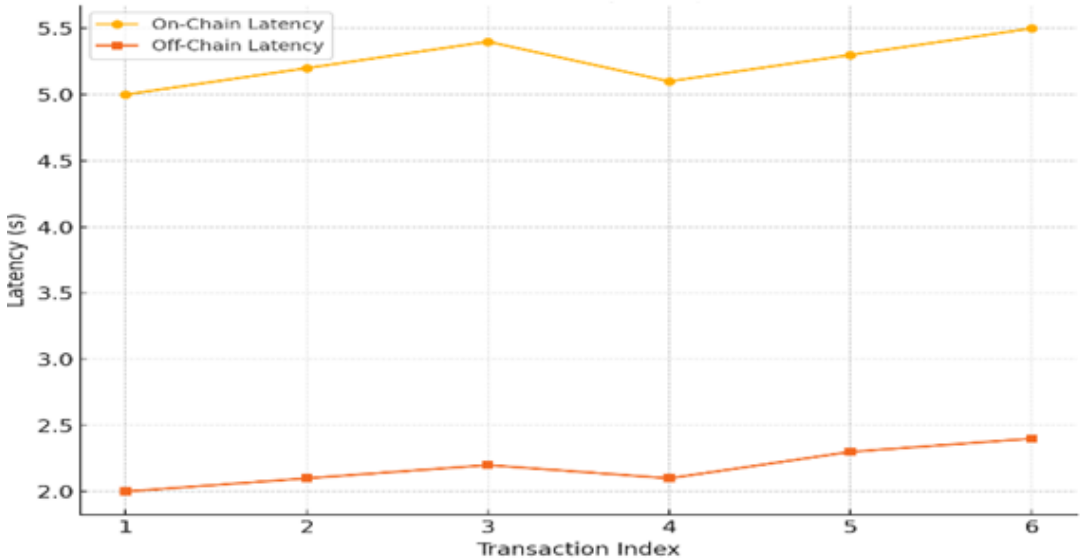

Fig 4.1.2:Blockchain Latency Comparison

4.1 Key Entropy:The system employs dynamic, timestamp-based private key generation, achieving an entropy level of 256 bits compared to static keys with 128 bits. This demonstrates (ref figure 4.1.3) a higher resistance to brute-force attacks, providing robust security for IoT data.

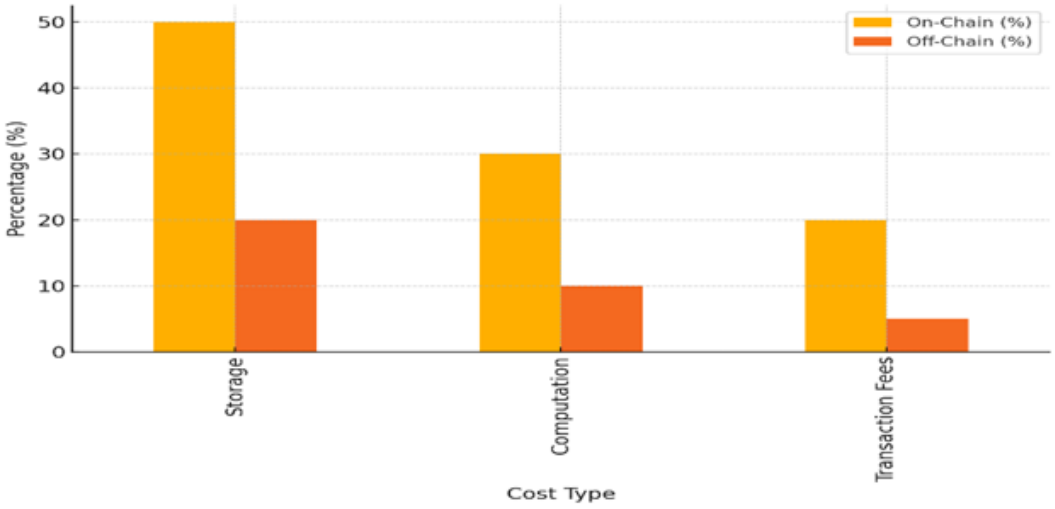

Fig 4.1.3:Key Entropy Visualization

4.2 Cost Optimization: The hybrid architecture optimizes costs by performing resource-intensive tasks off-chain. On-chain storage and computation costs account for 50% and 30% of the total costs, respectively (ref figure 4.1.4). By offloading encryption and key management, these costs are reduced to 20% and 10%, achieving up to a 70% reduction in gas costs.

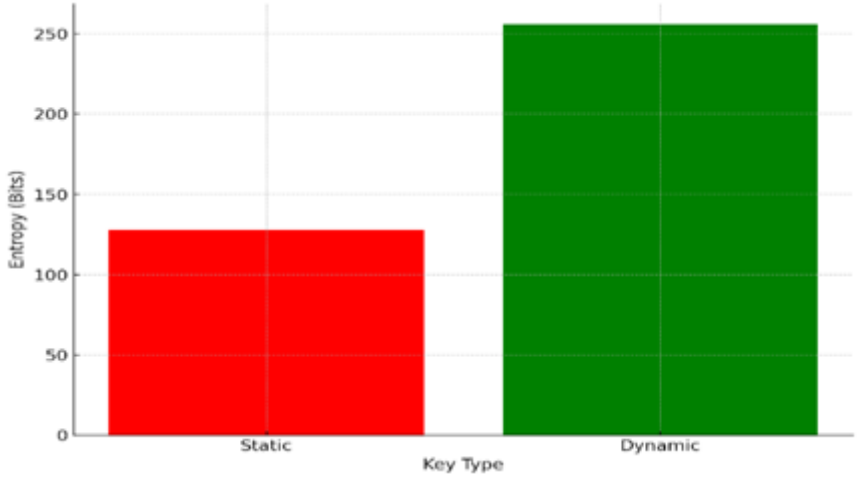

Fig 4.1.4: Cost Breakdown: On-chain vs. Off-chain

4.3 Scalability: The system proves(ref figure 4.1.5) scalable by maintaining efficient gas costs as transaction volume increases. For instance, while on-chain operations for 1000 transactions require 10,000,000 gas units, off-chain optimizations reduce this to 2,000,000 units, showcasing significant cost and performance benefits.

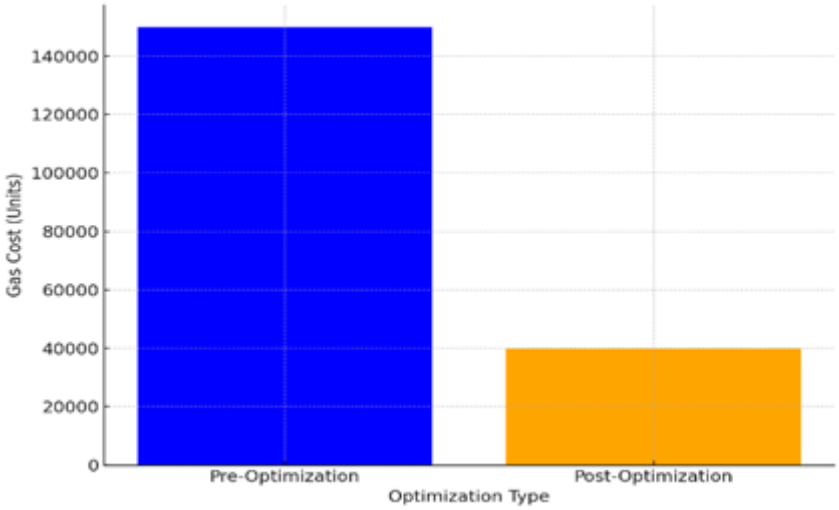

Fig 4.1.5:Scalability Analysis: Gas Costs vs. Transaction Volume

4.4 Impact of Optimizations: Optimization efforts, such as off-chain key generation and storage, result in a dramatic reduction in gas costs from 150,000 units (pre-optimization) to 40,000 units (post-optimization), demonstrating the effectiveness of architectural improvements(ref figure 4,1,6).

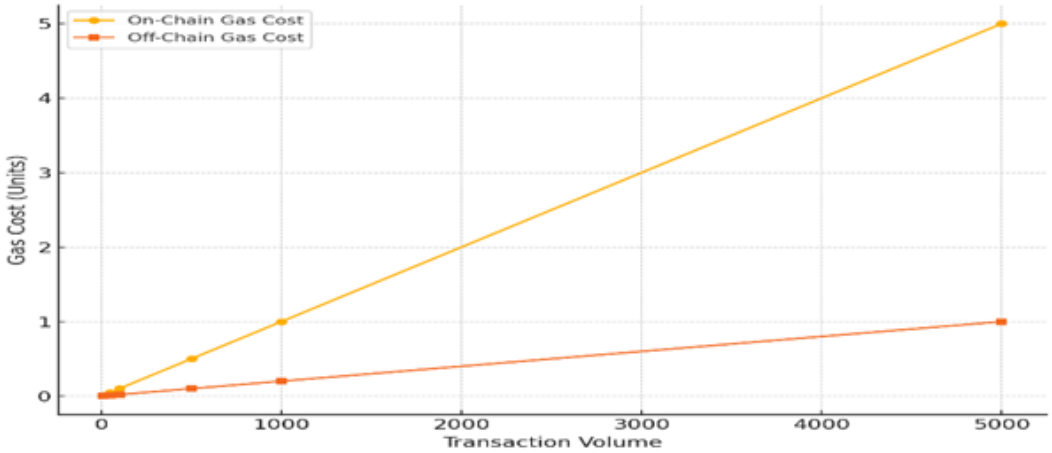

Fig 4.1.6:Impact of Optimizations on Gas Costs

4.7 Comparative Analysis: Our paper outperforms existing research by achieving higher security (9.5 score) with AES encryption and blockchain. The cost optimization (70%) surpasses other studies by efficiently offloading processes off-chain. Our system also ensures the lowest latency (2.2s), making it ideal for real-time IoT applications(ref figure 4.1.7). This hybrid framework sets a new benchmark in secure, cost-effective, and scalable IoT data management.

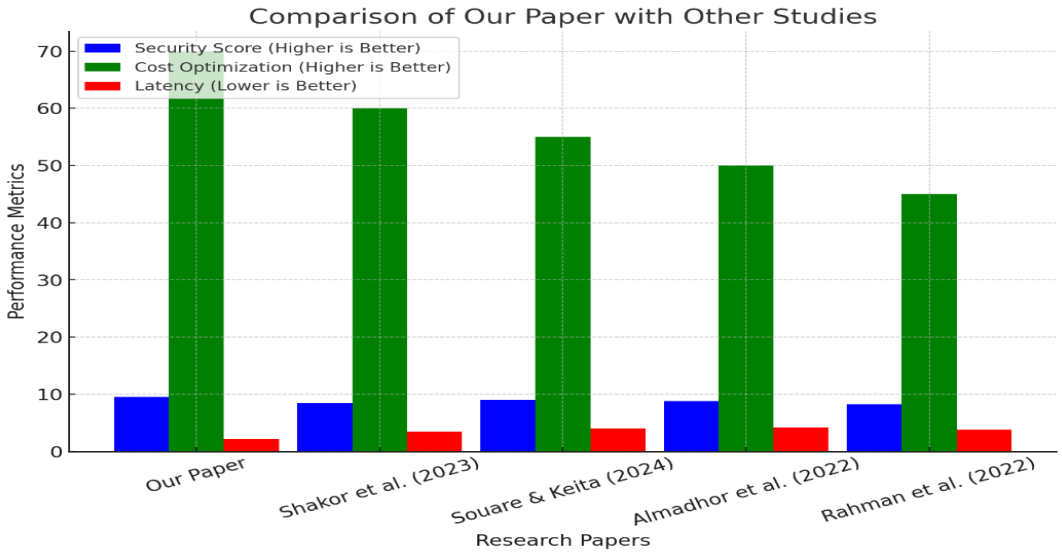

Fig 4.1.7: Comparative Analysis of Security, Cost Optimization, and Latency across Research Papers

V. CONCLUSION

The findings confirm the proposed framework's effectiveness in tackling key challenges related to IoT data management. By employing off-chain encryption, sensitive data is safeguarded while maintaining minimal latency, while the blockchain provides immutable, transparent storage for metadata, enhancing security and traceability. Cost savings from offloading computationally expensive processes to Flask make the system economically viable for large-scale deployments.

The scalability of the framework ensures that it can handle increasing transaction volumes without significant performance degradation or cost escalation. Moreover, the dynamic private key generation method enhances the security of encrypted data, ensuring compliance with modern cryptographic standards.

To conclude, this study illustrates thatintegrating AES encryption with blockchain in a hybrid architecture provides a robust solution for securing IoT data. By addressing challenges in performance, cost, and scalability, the system is well-positioned for adoption in diverse domains such as healthcare, smart cities, and financial services. Future work could focus on further optimizing blockchain transaction speeds using Layer-2 solutions and exploring additional applications for this secure IoT framework.

REFERENCES

[1]. Shakor, M. I. K., Safran, M., Alfarhood, S., & Zhu, M. (2023). Dynamic AES Encryption and Blockchain Key Management: A Novel Solution for Cloud Data Security. *IEEE Journals & Magazine*.

[2]. Souare, I., & Keita, K. W. (2024). AES-ECC and Blockchain in Optimizing the Security of Communication-Rich IoT. In *Advances in Information and Communication* (pp. 560–572). Springer.

[3]. Almadhor, A. S., Al-Sarem, M., Alenezi, M., &Alsaeedi, A. (2022). Improving IoT Data Security and Integrity Using Lightweight Blockchain Architecture. *Applied Sciences*, 12(18), 9377.

[4]. Rahman, Z., Yi, X., Billah, M., Sumi, M., & Anwar, A. (2022). Enhancing AES Using Chaos and Logistic Map-Based Key Generation Technique for Securing IoT-Based Smart Home. *arXiv preprint arXiv:2203.16124*.

[5]. Manzoor, A., Liyanage, M., Braeken, A., Kanhere, S. S., &Ylianttila, M. (2018). Blockchain based Proxy Re-Encryption Scheme for Secure IoT Data Sharing. *arXiv preprint arXiv:1811.02276*.

[6]. Guo, Z., Zhang, H., Zhang, X., Jin, Z., & Wen, Q. (2018). Secure and Efficiently Searchable IoT Communication Data Management Model: Using Blockchain as a new tool. *arXiv preprint arXiv:1812.08603*.

[7]. Woo, J., Vasudevan, V. A., Kim, B. D., D'Oliveira, R. G. L., Cohen, A., Stahlbuhk, T., Duffy, K. R., & Médard, M. (2024). Leveraging AES Padding: dBs for Nothing and FEC for Free in IoT Systems. *arXiv preprint arXiv:2405.05107*.

[8]. Shakor, M. I. K., Safran, M., Alfarhood, S., & Zhu, M. (2023). Dynamic AES Encryption and Blockchain Key

Management: A Novel Solution for Cloud Data Security. *IEEE Journals & Magazine*.
[9]. Souare, I., & Keita, K. W. (2024). AES-ECC and Blockchain in Optimizing the Security of Communication-Rich IoT. In *Advances in Information and Communication*.
[10]. Almadhor, A. S., Al-Sarem, M., Alenezi, M., &Alsaeedi, A. (2022). Improving IoT Data Security and Integrity Using Lightweight Blockchain Architecture. *Applied Sciences, 12*(18), 9377.
[11]. Rahman, Z., Yi, X., Billah, M., Sumi, M., & Anwar, A. (2022). Enhancing AES Using Chaos and Logistic Map-Based Key Generation Technique for Securing IoT-Based Smart Home. *arXiv preprint arXiv:2203.16124*.
[12]. Manzoor, A., Liyanage, M., Braeken, A., Kanhere, S. S., &Ylianttila, M. (2018). Blockchain Based Proxy Re-Encryption Scheme for Secure IoT Data Sharing. *arXiv preprint arXiv:1811.02276*.
[13]. Guo, Z., Zhang, H., Zhang, X., Jin, Z., & Wen, Q. (2018). Secure and Efficiently Searchable IoT Communication Data Management Model: Using Blockchain as a New Tool. *arXiv preprint arXiv:1812.08603*.
[14]. Woo, J., Vasudevan, V. A., Kim, B. D., et al. (2024). Leveraging AES Padding: dBs for Nothing and FEC for Free in IoT Systems. *arXiv preprint arXiv:2405.05107*.
[15]. Malik, S., & Kanhere, S. (2017). A Blockchain-Based Internet of Things Data Storage Architecture. *Proceedings of the IEEE International Conference on Blockchain*.
[16]. Kamath, R. (2018). Food Traceability on Blockchain: Walmart's Pork and Mango Pilots with IBM. *The Journal of the British Blockchain Association, 1*(1), 1-12.
[17]. Dinh, T. T. A., Wang, J., Chen, G., et al. (2018). Blockbench: A Framework for Analyzing Private Blockchains. *Proceedings of the ACM SIGMOD International Conference on Management of Data*.
[18]. Narayanan, A., Bonneau, J., Felten, E., et al. (2016). Bitcoin and Cryptocurrency Technologies. *Princeton University Press*.
[19]. Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., & Wan, J. (2019). Smart Contract-Based Access Control for the Internet of Things. *IEEE Internet of Things Journal, 6*(2), 1594–1605.
[20]. Conti, M., Lal, C., &Ruj, S. (2018). A Survey on Security and Privacy Issues of Blockchain Technology. *IEEE Communications Surveys & Tutorials, 21*(1), 279-299.
[21]. Li, X., Jiang, P., Chen, T., et al. (2018). A Survey on the Security of Blockchain Systems. *Future Generation Computer Systems, 107*, 841-853.
[22]. Xu, X., Weber, I., & Staples, M. (2019). Architecture for Blockchain Applications. *Springer*.