2025 International Conference on Intelligent Communication Networks and Computational Techniques (ICICNCT)

Blockchain based on Encryption Scheme for Internet of Things Environment

1st Kumar. M P
Department of Computer Science
VELS Institute of Science, Technology and Advanced Studies(VISTAS)
Pallavaram, India
kumarmp.mca@gmail.com

2nd Akila. A
Department of Computer Science and Information Technology
VELS Institute of Science, Technology and Advanced Studies(VISTAS)
Pallavaram, India
akila.scs@velsuniv.ac.in

***Abstract*—In recent years, Internet of Things (IoT) technology has been widely used, especially in fields involving smart fitness and smart vehicles. IoT devices continuously generate real-time information and transmit it over the internet. IoT systems use a centralized design for statistical storage and processing within modern IoT processes. However, with the rapid development of network technologies, IoT environments have grown exponentially, ranging from military surveillance to e-smart health, traffic monitoring, and industrial control. Despite their numerous applications, improving IoT security remains a major concern. The reliance on third-party involvement in typical IoT systems to safeguard sensitive data during transmission has increased complex and significant concerns. Blockchain technology offers a modern solution for reducing third-party dependency in IoT environments and is essential for addressing security challenges. To address the aforementioned challenges, this study applies various approaches such as authorization, encryption, and validation, utilizing a blockchain-based encryption scheme within the IoT environment. The parameters considered in this study are storage cost, computation cost, throughput, latency, and correlation coefficient.**

Keywords—authorization, blockchain, encryption scheme, internet of things (IoT), privacy and security.

I. INTRODUCTION

The Internet of Things (IoT) has grown to be one of the most promising technologies, with devices such as smart physical systems, vehicles, and appliances anonymously collecting data, enabling connectivity, and facilitating data sharing [1]. It has been widely adopted in industrial management, traffic monitoring, smart healthcare, military surveillance, and other domains due to its wide applicability. Wireless connectivity, computation, sensing, and the generation of large-scale distributed records are among the core technologies where IoT devices are utilized. It not only improves living standards but also contributes significantly to the global economy [2]. However, the conventional cloud-based infrastructure is experiencing several management challenges due to the continuously growing volume of IoT data, including concerns related to data privacy, response delay, bandwidth limitations, and storage potential [3]. Moreover, a decentralized, dynamic and large-scale distributed IoT architecture is gradually taking shape. Each subnet within this structure operates as an independent domain, incorporating a wide range of communication protocols, subordinate devices, and autonomous management systems [4]. Due to the extensive deployment of IoT gadgets and the rapid development of related services and solutions in recent years, numerous vulnerabilities and security issues have emerged in IoT environments. Key vulnerabilities include unauthorized access for device console hijacking, manipulation of code execution flow within devices, and interference during the firmware update process [5]. These structures enable the independent addition of numerous values while preserving private data and safeguarding against information manipulation [6]. Unauthorized access to IoT devices can result in serious consequences, significantly threatening privacy, safety, functionality, and data confidentiality. This is because IoT devices frequently handle sensitive information and play a vital role in specific operations. Securing IoT systems is essential for enforcing appropriate access controls [7]. Encrypting data before transmission to the cloud is an effective technique. When conventional security measures fail, attackers can access only the encrypted form of the data. To ensure the security of shared information, all data should be encrypted at the source and decrypted only by authorized users. A privacy protection scheme was implemented for data revocation and domain-based encryption in high-dimensional attributes [8]. Blockchain technology is a peer-to-peer approach in which all users collaboratively manage the network, offering advantages such as traceability, data integrity, scalability, and interoperability [9]. Blockchain is a traceable, distributed, and tamper-resistant ledger that relies on collaborative maintenance and data sharing, and uses consensus mechanisms to ensure data consistency. Furthermore, due to its temporal ordering capabilities, blockchain currently outperforms conventional databases and cloud systems in terms of chronological sequencing, privacy protection, and tamper-proofing [10].

The Related works on blockchain based on encryption schemes for IoT environments are discussed in Section 2. A taxonomy of encryption scheme based blockchains is presented in Section 3. A comparative analysis of the various approaches is presented in Section 4. Section 5 presents the problem statement and Section 6 presents a summary of the paper.

The remainder of this paper is organized as follows: The related, blockchain-based conventional encryption schemes for IoT environments are discussed in Section 2, while the taxonomy of encryption scheme-based blockchains are discussed in Section 3. The comparative analysis of these approaches is presented in Section 4, Section 5 presents the problem statement and finally, Section 6 presents the summary of this study.

II. TAXONOMY OF ENCRYPTION SCHEME-BASED BLOCKCHAIN

This section discusses the taxonomy of existing blockchain-based encryption schemes that utilize authorization, encryption, and validation techniques. These approaches employ numerous algorithms within blockchain techniques. Blockchain-based encryption schemes play a

979-8-3315-8623-2/25/$31.00 ©2025 IEEE

crucial role in securing IoT environments, ensuring data integrity and protecting privacy. Fig. 1 illustrates a taxonomy diagram of the encryption scheme based on blockchain for the IoT environment.

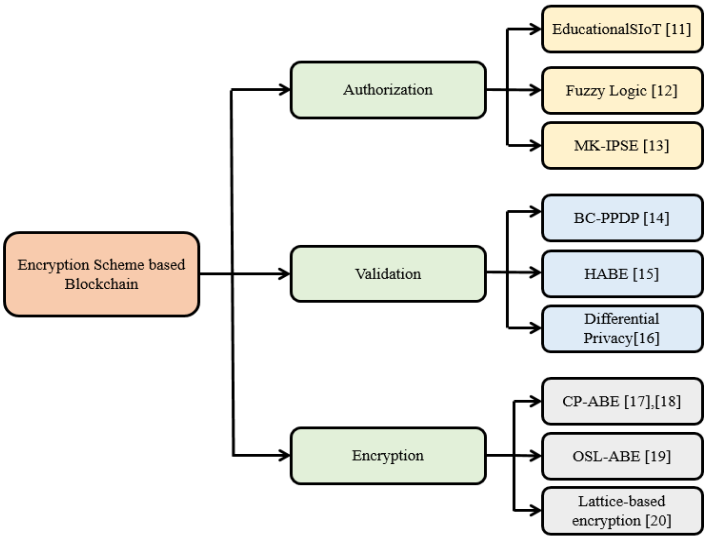

Fig. 1. Taxonomy Diagram of Blockchain based on Encryption Scheme for IoT

A. Authorization

Authorization in blockchain-based total-encryption strategies for IoT is vital for ensuring secure and effective communication across the IoT environment. IoT devices operate in dynamic and distributed environments, and access permissions may vary due to the diversity of shared IoT devices. A large array of networked devices complicates identification and access management. Various approaches to authorization, such as MK-IPSE and SM-ARM, are utilized. These approaches are briefly described as follows.

Dallel et al. [11] developed a blockchain-based authorization mechanism for the Educational Social Internet of Things (EducationalSIoT). EducationalSIoT supported service exchange, context-awareness, and secure access control, building social relationships between devices based on educational interactions. The extensible Access Control Markup Language (XACML) policy was extended to include social constraints that enabled fine-grained access control decisions matching academic interactions. Policy evaluation enhancements ensured that higher-priority relationships and delegation policies enabled secure and flexible authorization across academic devices. However, the existing access control mechanisms in SIoT were not designed for specific applications such as education, which reduced the accuracy of access decisions in educational environments.

Alqbaishi and Ahmed [12] introduced fuzzy logic to enhance decision-making in blockchain-based access control in an IoT environment. Fuzzy reputation computed a quantitative reputation score for each IoT device, incorporating multiple dynamic variables such as access request rate and request frequency. The decay algorithm was used to reduce the influence of previous behavior, and the calculated reputation score determined access permissions through smart contracts implemented in a hybrid blockchain using Geth and Hyperledger Fabric. However, the complexity of the fuzzy logic system made it more difficult for users to understand the reasoning behind reputation values, resulting in a trade-off between precise evaluation for IoT users.

Liu et al. [13] developed a blockchain-assisted privacy-preserving medical data-sharing approach for e-healthcare systems. This methodology provided a fully blockchain-based MK-IPSE aimed at ensuring complete privacy preservation and ciphertext retrieval for electronic medical records (EMRs). Internal product encryption (IPE) allowed the specification of access rights for permissions, ensured that only eligible clients with matching attributes were granted access to corresponding files, and allowed coverage masking. In addition, the proposed approach integrated Searchable Encryption (SE) with a Federated Blockchain (FB) to enable an intuitive and robust multi-keyword search function.

B. Validation

Data validation in simple blockchain-based IoT encryption systems is a major task for ensuring data integrity and trustworthiness. Any node in the blockchain network authenticates and verifies the use of a reliable consensus mechanism before any transactions are completed. The distributed nature of the blockchain conveys comprehensive data integrity information and high anti-tampering capability, thereby ensuring that the information is not changed. Data validation is separated from the principal blockchain and then transferred for processing, reducing processing overhead while ensuring data security. Some validation approaches, such as BC-PPDP and Hybrid Attribute-Based Encryption (HABE), are used and are described as follows.

Wang et al. [14] introduced a personal-privacy data protection scheme for the encryption and revocation of high-dimensional attribute domains. This model developed a novel approach for personal privacy data protection based on a blockchain technology called Blockchain-based Personal Privacy Data Protection (BC-PPDP). The BC-PPDP model was constructed using two main components: the Fast High-dimensional attribute Domain-based Message Encryption (HAD-FME) and Attribute Revocation Mechanism based on Sentry Mode SM-ARM. The model ensured that data subjects maintained a control over private information stored in the blockchain through smart contracts. With HAD-FME key technology in BC-PPDP, it was used for secure data storage and transfer. Additionally, to achieve an efficient attribute revocation mechanism, HAD-FME introduced a timestamp attribute into the data profile of each individual.

Sasikumar et al. [15] presented a blockchain-aided HABE for secure data sharing in IoT. Initially, a data encryption mechanism was introduced for enabling IoT devices to securely transmit data to nearby cloud networks while preserving privacy. In addition, a blockchain-integrated data-sharing scheme was established to facilitate data exchange through both facet and cloud storage systems. Notably, this model was characterized by an encryption-based authentication mechanism integrated into IoT devices to decentralize the verification of user access privileges within the community network. Using HABE, this approach provided a blockchain-enabled framework that user privacy protection. The proposed strategy integrated area and cloud network paradigms with HABE, making it well-suited for applications such as smart logistics.

Kashif and Kalkan [16] developed a differential privacy-preserving framework using the blockchain of IoT networks with a large volume of data generated from interconnected devices. This framework enabled differential privacy techniques based on Laplace and Gaussian noise to ensure privacy protection across various levels. A lightweight cryptographic mechanism and fast convergence consensus protocol were utilized for blockchain privacy preservation, enhancing data privacy and securing IoT data handling within blockchain environments. However, this framework faced scalability issues due to high computational and storage requirements during the processing of private IoT data on the blockchain, thereby deteriorating performance and impeding long-term data storage.

C. Encryption

In blockchain-based encryption schemes for IoT, encryption plays a crucial role in ensuring stable and privacy-protection data transmission. These techniques enable reliable searches and access to databases based on keywords, in addition to mechanisms for secure key revocation and policy updates. The integration of blockchain technology with robust encryption mechanisms protects IoT data and supports decentralized applications across various domains. Different encryption schemes, such as CES Blocks, HAD-FME, and BFR-SE, are employed, and these approaches are explained as follows.

Yang et al. [17] introduced an attribute-based access control using blockchain technology for IoT data protection. Attribute-Based Encryption (ABE) was used to enforce fine-grained access control, and a decentralized blockchain framework was used to improve traceability and policy privacy. The optimized ABE scheme handled large attribute universes efficiently and prevented replay attacks, which reduced system parameter size and algorithmic efficiency. The overall approach outperformed other approaches in terms of security, expressive policy, and policy hiding. However, the ABE scheme eliminated centralization and optimized encryption, which posed challenges in handling large-scale IoT environments, owing to the computational demands of the blockchain network.

Xie et al. [18] developed a blockchain-enabled data sharing for IoT environments based on a lightweight, secure, and searchable scheme. Searchable encryption and smart contracts enabled privacy-preserving and verifiable search operations on encrypted data, without the need for a central server. Instead of relying on central servers, a smart contract for executing ciphertext retrieval provided more accurate search results. The ABE algorithm reduced computational cost and maintained constant encryption and decryption workloads. However, in smart contract execution, the number of files and keyword indexes increased, leading to scalability and cost efficiency challenges in large IoT deployments.

Vinnarasi and Dayana [19] developed an Optimal Secure and Lightweight (OSL) ABE method for blockchain enabled IoT based healthcare. The ABE enabled fine-grained access control over sensitive data in IoT applications. The Modified Sandpiper Optimization (MSO) algorithm enabled privacy-preserving key generation and included an Enhanced Gravitational search (EGS) algorithm to support secure and efficient key revocation mechanisms. A single short broadcast message helped maintain confidentiality of the IoT system. However, the framework faced scaling issues in the presence of a large number of IoT devices and huge data volumes.

Prajapat et al. [20] presented a quantum-safe blockchain-assisted data encryption protocol for IoT networks. The model included lattice-based cryptography to provide post-quantum security breach for ensured robustness against both polynomial-time and probabilistic polynomial time adversaries. This approach employed blockchain consensus nodes as proxy services for data encryption and aggregate translated ciphertext, which supported multi-authority key management for achieving collision resistance, significantly reducing encryption and decryption processing overhead. However, the model faced certain setbacks such as restricted computing resources and slow transaction speed in IoT environments. Additionally, several connected sensors and nodes lacked the required memory and processing power.

III. Comparative Analysis

Blockchain-based encryption schemes are comparatively analyzed against existing approaches to performance evaluation within IoT environments. The comparative analysis considers the employed methodologies, advantages, limitations, and performance metrics of each approach. This comparison aims to identify the most efficient methods for improving model development and optimizing performance. Table 1 presents a comparative analysis of the existing techniques.

TABLE I. Comparative Analysis of Existing Methods

Authors	Methodology	Advantages	Disadvantages	Performance Metrics
Dallel et al. [11]	EducationalSIoT	Policy evaluation enhancements ensured high priority relationships and delegation policies for secure and flexible authorization across academic devices.	Access control mechanisms in SIoT were not designed for specific uses like education, which reduced the accuracy of access decisions made by the framework in such environments.	Policy Evaluation Time, Request Execution Time
Alqbaishi and Ahmed [12]	Fuzzy Logic	Decay algorithm was enabled to reduce the influence of previous behavior, calculating reputation score to determine access permissions through smart contract.	The complexity of fuzzy logic systems made if challenging for users to reason out the chosen reputation values.	Reputation Analysis, Access Request Rate, Comparative Analysis, Security Analysis

Liu et al. [13]	MK-IPSE	This model supported secure access permission control and hidden policy, accelerating the progress of medical systems and improving security.	The implemented MK-IPSE method used in healthcare systems faced difficulties with a large number of transactions, resulting in lower processing speed.	Storage cost, computation cost
Wang et al. [14]	HAD-FME, SM-ARM, BC-PPDP	The model addressed challenges such as low protection, massive computational overhead, and excessive characteristic retrieval cost demand with existing schemes in high-dimensional attribute domains.	The implemented method faced scalability issues when dealing with a large number of attributes.	Transaction throughput, transaction latency
Sasikumar et al. [15]	HABE	The data-sharing approach performed well on blockchains, allowing for faster data retrieval.	The developed approach was required to enhance secure real-time transport monitoring and data management using the blockchain-integrated edge computing approach.	Memory utilization, data retrieval latency and average throughput
Kashif and Kalkan [16]	Differential Privacy	A lightweight cryptographic mechanism and a fast-convergence consensus protocol were utilized to maintain blockchain privacy preservation, which enhanced data privacy.	The framework faced scalability issues due to high computational and storage demands when processing private IoT data on the blockchain, which reduced performance.	Throughput, Latency
Yang et al. [17]	ABE	Optimized ABE scheme was enabled for handling large attribute universes efficiently and to prevent replay attacks, reducing system parameter sizes smaller and improving algorithm efficiency.	The ABE scheme eliminated centralization and optimized encryption, which posed challenges in handling large-scale IoT environments, owing to the computational demands of the blockchain network.	Encryption Time, Decryption Time
Xie et al. [18]	ABE	ABE algorithm enabled reduced computation cost with a constant encryption and decryption workload management.	In smart contract execution, the number of files and keyword indexes increased, leading to scalability and cost efficiency challenges in large IoT deployments.	Computational costs
Vinnarasi and Dayana [19]	OSL-ABE	A single short broadcast message helped maintain confidentiality of the IoT system.	The framework faced scaling issues in the presence of a large number of IoT devices and huge data volumes.	NPCR, Information Entropy
Prajapat et al. [20]	Lattice based Encryption	This approach employed blockchain consensus nodes as proxy services for data encryption and aggregate translated ciphertext, which supported multi-authority key management for achieving collision resistance.	The model faced certain setbacks such as restricted computing resources and slow transaction speed in IoT environments.	Computational and Communication costs

IV. Problem Statement

Table 2 below presents the problem statements of existing methods introduced for blockchain-based on encryption scheme for the IoT environment.

TABLE II. Problem Statement for Existing Methods

Problem Statement	Description
Energy and channel issues	Due to limited energy resources in sensors and unreliable wireless channels, maintaining strong data confidentiality and privacy becomes challenging in IoT systems.
Medical image vulnerability	Existing encryption methods fail to fully protect the integrity and privacy of sensitive medical images on chain networks in the face of evolving cyber threats.
Blockchain based issues	Blockchain-based encryption schemes still suffer from issues like lack of transparency, inadequate trust mechanisms, and unresolved security vulnerabilities.

V. Conclusion

In recent years, IoT applications have proliferated in a wide range of industries, including transportation, logistics, cars, healthcare, wise environments, and commercial enterprise structures, with client electronics receiving substantial benefits. The growing adoption of IoT technologies, resulting in the generation of massive volumes of data, poses challenges to traditional centralized data management, particularly in terms of performance, privacy, and security. As most IoT devices have restricted storage capacity and produce large amounts of data, data owners increasingly rely on cloud storage services to reduce infrastructure costs and minimize local storage overhead. However, this data, especially that generated by specific IoT devices such as smart homes and smartwatches, often contains sensitive personal information. To address these challenges, an encryption scheme-based blockchain solution has emerged as a robust and practical approach for securing IoT data, enabling controlled access within specialized IoT environments while ensuring data privacy and security.

References

[1] Y. Meng, B. Wang, Q. Xing, X. Wang, J. Liu, and X. Xu, "BBAD: Blockchain-based data assured deletion and access control system for IoT," Peer-to-Peer Netw. Appl, vol. 18, p. 1, December 2024.

[2] N. A. Ismail, S. A. Khadra, G. M. Attiya, and S. E. S. E. Abdulrahman, "Optimizing SIKE for blockchain-based IoT ecosystems with resource constraints," J. Supercomput, vol. 81, p. 463, February 2025.

[3] A. Sasikumar, L. Ravi, M. Devarajan, A. Selvalakshmi, A. T. Almaktoom, A. S. Almazyad, G. Xiong, and A. W. Mohamed, "Blockchain-assisted hierarchical attribute-based encryption scheme for secure information sharing in industrial Internet of Things," IEEE Access, vol. 12, pp. 12586–12601, January 2024.

[4] G. Ganapathy, S. J. Anand, M. Jayaprakash, S. Lakshmi, V. B. Priya, and S. P. Pandi, "A blockchain-based federated deep learning model for secured data transmission in healthcare IoT networks," Meas.: Sens., vol. 33, p. 101176, June 2024.

[5] T. Nguyen, H. Nguyen, and T. N. Gia, "Exploring the integration of edge computing and blockchain IoT: Principles, architectures, security, and applications," J. Netw. Comput. Appl, vol. 226, p. 103884, June 2024.

[6] F. M. Alserhani, "Integrating deep learning and metaheuristics algorithms for blockchain-based reassurance data management in the detection of malicious IoT nodes," Peer-to-Peer Netw. Appl, vol. 17, pp. 3856–3882, September 2024.

[7] W. Wang, B. Yan, B. Chai, R. Shen, A. Dong, and J. Yu, “EBIAS: ECC-enabled blockchain-based identity authentication scheme for IoT device,” High-Confidence Comput, vol. 5, p. 100240, March 2025.

[8] X. Wang, H. Zhang, H. Wu, and H. Yu, “Dual-blockchain based multi-layer grouping federated learning scheme for heterogeneous data in industrial IoT,” Blockchain: Research and Applications, vol. 5, p. 100195, September 2024.

[9] N. Xiao, Z. Wang, X. Sun, and J. Miao, “A novel blockchain-based digital forensics framework for preserving evidence and enabling investigation in industrial Internet of Things,” Alex. Eng. J, vol. 86, pp. 631–643, January 2024.

[10] T. B. D. Cunha and K. Manjappa, “Private and consortium blockchain-based authentication protocol for IoT devices using PUF,” J. Commun. Netw, vol. 26, pp. 166–181, April 2024.

[11] O. Dallel, S. B. Ayed, and J. B. H. Tahar, “Blockchain-Based Authorization Mechanism for Educational Social Internet of Things,” IEEE Access, vol. 12, pp. 42888–42907, March 2024.

[12] A. A. Alqbaishi and A. E. S. Ahmed, “Reputation evaluation using fuzzy logic for Blockchain‐Based access control in an IoT environment,” IEEE Access, vol. 12, pp. 97386–97404, July 2024.

[13] J. Liu, Y. Fan, R. Sun, L. Liu, C. Wu, and S. Mumtaz, “Blockchain-aided privacy-preserving medical data sharing scheme for e-healthcare system,” IEEE Internet of Things J, vol. 10, pp. 21377–21388, June 2023.

[14] C. Wang, J. Lu, X. Li, P. Cao, Z. Zhou, and Q. Wen, “A Personal Privacy Data Protection Scheme for Encryption and Revocation of High-dimensional Attribute Domains,” IEEE Access, vol. 11, pp. 82989–83003, July 2023.

[15] A. Sasikumar, L. Ravi, M. Devarajan, A. Selvalakshmi, A. T. Almaktoom, A. S. Almazyad, G. Xiong, and A. W. Mohamed, “Blockchain-Assisted Hierarchical Attribute-Based Encryption Scheme for Secure Information Sharing in Industrial Internet of Things,” IEEE Access, vol. 12, pp. 12586–12601, January 2024.

[16] M. Kashif and K. Kalkan, “Differential privacy preserving based framework using blockchain for internet-of-things,” Peer-to-Peer Netw. Appl, vol. 18, p. 33, December 2024.

[17] Z. Yang, X. Chen, Y. He, L. Liu, Y. Che, X. Wang, K. Xiao, and G. Xu, “An attribute-based access control scheme using blockchain technology for IoT data protection,” High-Confid. Comput, vol. 4, p. 100199, September 2024.

[18] Q. Xie, F. Zhu, and X. Feng, “Blockchain-enabled data sharing for IoT: A lightweight, secure and searchable scheme,” J. Syst. Archit, vol. 154, p. 103230, September 2024.

[19] A. P. Vinnarasi and R. Dayana, “OSL-ABE: an optimal secure and lightweight attribute-based encryption method for blockchain-enabled IoT-based healthcare systems,” Neural Comput. Appl, vol. 37, pp. 123–148, November 2024.

[20] S. Prajapat, N. Kumar, A. K. Das, P. Kumar, and R. Ali, “Quantum-safe blockchain-assisted data encryption protocol for internet of things networks,” Cluster Comput, vol. 28, p. 5, October 2024.