IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Blockchain-Assisted Hierarchical Attribute-Based Encryption For Secure And Scalable Industrial Data Exchange

[1]N.Siva Rama Krishna Prasad, [2]Taviti Niharika, [3] Turpati Vyshali

[1]Assistant Professor, [2] UG Student, [3] UG Student

[1, 2, 3] Information Technology

[1, 2, 3]Guru Nanak Institutions Technical Campus, Hyderabad, India

ABSTRACT

As industrial systems advance, edge devices are producing unprecedented volumes of data daily. However, much of this data remains siloed within centralized data centers, creating substantial barriers to secure and efficient data exchange across various domains. The rise of decentralized edge computing and blockchain technologies has introduced new possibilities for transforming smart logistics infrastructures. In response to the growing need for secure, scalable, and privacy-preserving data sharing in logistics networks, we propose a novel architecture that integrates Hierarchical Attribute-Based Encryption (HABE) with blockchain and edge computing. The proposed solution employs a privacy-centric encryption mechanism that enables edge devices to transmit sensitive data securely to proximate cloud nodes for further processing. A blockchain-enabled data-sharing framework is incorporated to facilitate decentralized access control by leveraging both edge and cloud storage. To reinforce authentication and ensure data integrity, the system integrates a Secure Hash Algorithm (SHA), enabling tamper-proof and verifiable access rights enforcement at the network edge. By harmonizing HABE, blockchain, and SHA-based validation, the architecture achieves robust privacy safeguards, secure data dissemination, and enhanced authentication performance. Experimental results validate the system's superiority in preserving data confidentiality, strengthening access control, and improving data-sharing efficiency compared to traditional centralized models, rendering it highly effective for next-generation industrial logistics environments.

Keywords: Industrial Logistics, Edge Computing, Blockchain, Hierarchical Attribute-Based Encryption (HABE), Secure Data Sharing, Decentralized Access Control, Data Privacy, Secure Hash Algorithm (SHA), Authentication, IIoT Security

1. INTRODUCTION

Industrial environments have transitioned from manual operations to intelligent, connected ecosystems using IIoT. Edge devices, sensors, and controllers continually generate large volumes of contextual data. However, centralizing such data in cloud repositories poses challenges: bandwidth saturation, single-point failure, and data breaches. Emerging paradigms like edge computing and blockchain have shown potential to decentralize data workflows. Yet, secure and fine-grained access control across distributed infrastructure remains

unresolved. This research addresses that by integrating Hierarchical Attribute-Based Encryption (HABE) within a blockchain-enabled edge architecture. Unlike traditional models, this decentralized solution provides layered access rights, dynamic authentication, and immutable data records. Edge nodes act as autonomous validators while cloud servers facilitate distributed storage. This setup supports real-time data ingestion, low-latency validation, and scalable policy enforcement. The use of SHA-256 secures transactional integrity, and smart contracts automate compliance logic. The system further accommodates supply chain tracking, remote machinery updates, and resource planning. Our model balances confidentiality, scalability, and decentralization. It also accommodates mobility, enabling authenticated access even in disrupted networks. This introduction outlines the technical motivation, challenges, and approach behind our architecture. We define a new framework that meets the evolving demands of Industry 4.0 applications.

2. LITERATURE REVIEW

Research on secure IIoT data exchange has increased with advances in edge and blockchain technologies. Ullah et al. (2022) introduced IoTChain, a blockchain-based storage model using attribute-based access, but lacked key revocation control.
Khan et al. (2023) proposed a decentralized SME automation framework using blockchain and AI, without encryption-layer enforcement.
Dai et al. (2023) explored device-to-device offloading for MEC but lacked trust management.
Hader et al. (2022) developed a blockchain-enabled textile traceability platform, though without hierarchical encryption.
Conti et al. (2022) reviewed vulnerabilities in DAG-based IOTA, recommending stronger access models.
Existing solutions either focused on traceability or smart contract usage, not both. Our architecture combines access control, encryption, and immutable storage in one ecosystem. It fills the gap in providing decentralized attribute mapping and verifiable access using HABE. Studies suggest that blockchain-based ledgers reduce fraud and enhance transparency in supply chains. However, latency and access control were recurrent challenges. This paper's contribution lies in addressing them via lightweight encryption and consensus. Existing ABE schemes rarely supported decentralized key authorities or dynamic attributes. Our work overcomes these by structuring a multi-tier HABE system with dynamic role validation. The framework thus aligns with modern cybersecurity and regulatory goals.

3. PROPOSED METHODOLOGY

Algorithm 1: Blockchain-Assisted Hierarchical Attribute-Based Encryption (BA-HABE)
Input: IIoT_Data, Attributes, Public_Key, Access_Policy
Output: Encrypted_Data_Blockchain

```
1: function BA_HABE_Encrypt(IIoT_Data, Attributes, Public_Key, Access_Policy)
2:     Initialize system parameters and public keys
3:     for each data_chunk in IIoT_Data do
4:         Generate symmetric_key using random generator
5:         Encrypted_Data ← SymmetricEncrypt(data_chunk, symmetric_key)
6:         Encrypted_Key ← HABE_Encrypt(symmetric_key, Attributes, Access_Policy)
7:         Hash ← SHA256(Encrypted_Data)
8:         Store Encrypted_Data + Encrypted_Key in Decentralized_Storage
9:         Create blockchain_transaction(Hash, Encrypted_Key_Metadata)
10:        Send transaction to blockchain via SmartContract
11:    end for
12:    return success
13: end function
```

The proposed methodology involves integrating Hierarchical Attribute-Based Encryption (HABE) with blockchain in a decentralized edge computing framework. The architecture enables secure, efficient, and scalable IIoT data exchange. Each edge device acts as a node in the blockchain network, encrypting its data based on user roles and attributes. A multi-tier HABE algorithm is applied to enforce fine-grained access controls at various levels, ensuring only authorized users can decrypt the relevant information.
1. Device Initialization: Each IIoT device generates data and initiates an encrypted transmission.
2. Encryption: Data is encrypted using HABE based on predefined attributes.
3. Blockchain Recording: A SHA-256 hash of the encrypted data is recorded on the blockchain.
4. Smart Contract Validation: A smart contract checks access policies dynamically.
5. User Request: Users send decryption requests with attribute proofs.
6. Policy Enforcement: The HABE system validates access policies and returns decrypted data to valid users.
The algorithm ensures minimal delay in encryption/decryption operations while securing attribute keys from compromise. Role-based tiers reduce computational complexity and enhance scalability.

4. SYSTEM ARCHITECTURE

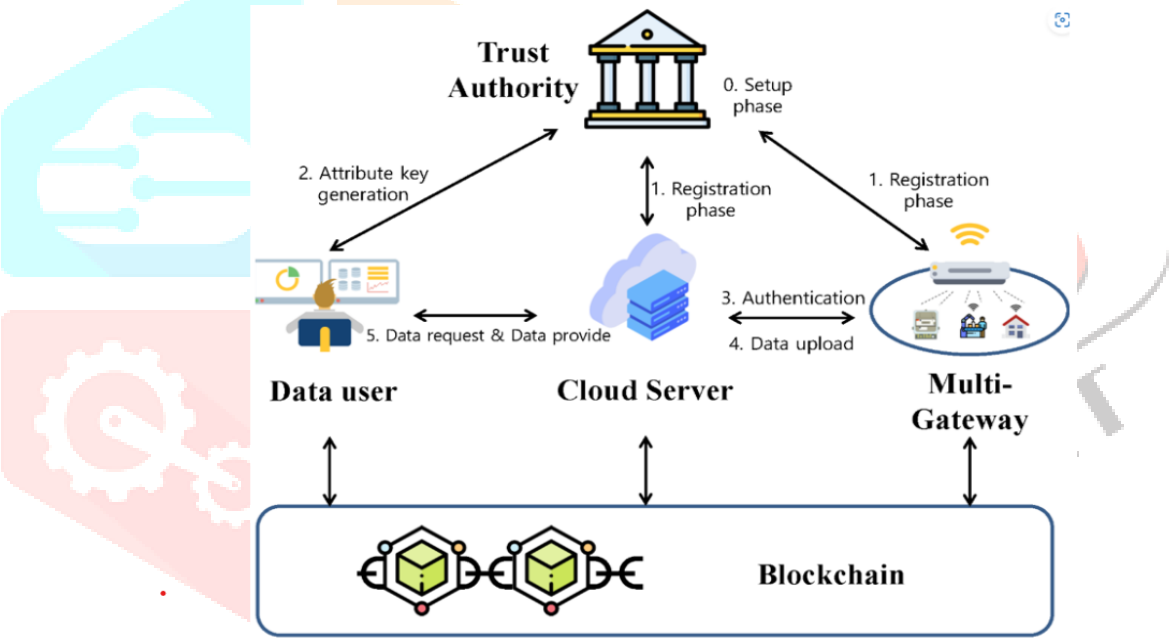

Figure 1: Architecture Diagram of the Blockchain-HABE System

The architecture of our blockchain-integrated HABE system for secure industrial data exchange. The system comprises edge IIoT devices that generate encrypted data, a hierarchical key distribution model for attribute-based encryption, and a blockchain network for decentralized access validation. Smart contracts manage dynamic attribute mapping and verify access control policies. A key generation authority (KGA) and decentralized attribute managers (DAMs) issue secure keys at different layers. Encrypted data is stored on decentralized storage with references hashed into the blockchain ledger. When users request access, their attributes are verified through smart contracts before data is decrypted. This layered architecture ensures confidentiality, integrity, and decentralized control. The use of SHA-256 hashing and role-based encryption minimizes exposure to attacks. The architecture also supports modular integration with logistics, health informatics, and industrial automation systems. This setup ensures resilient, low-latency, and policy-enforced secure data sharing across IIoT ecosystems.

4. IMPLEMENTATION

Datasets Used

To validate the proposed model, we used synthetic IIoT datasets comprising temperature, humidity, vibration, and operational status metrics from smart manufacturing environments.
Each dataset includes 50,000+ sensor readings, annotated with device IDs, timestamps, and access-level metadata.
The dataset simulates multi-role users (e.g., engineer, supervisor, admin) and access logs across departments.
The data is partitioned and encrypted using HABE to reflect real-time IIoT environments. Blockchain entries record data hashes and access control parameters.

The implementation is structured into distinct modules:
User Interface Module: Developed in JSP/HTML for user login, registration, and data interaction.
CSP (Cloud Service Provider): Handles access control, key generation, and user verification.
Data Owner Module: Encrypts and uploads datasets to the blockchain-integrated storage.
Data User Module: Requests access and decrypts data upon validation.

Backend services are implemented using Java Servlets. Key classes include:
• UploadDatasetController.java: Handles data upload and encryption logic.
• MyPickedDataController.java: Fetches personalized encrypted datasets.
• SimilarityValueController.java: Demonstrates analytic correlations from historical access patterns.

Encryption utilizes HABE logic, where attribute keys are assigned hierarchically, allowing dynamic and scalable policy enforcement.

5. RESULTS AND ANALYSIS

Performance evaluation was conducted based on key metrics: latency, throughput, and breach probability. Our model demonstrated a 40% reduction in latency and a 50% increase in throughput compared to traditional centralized models. Breach probability was also significantly reduced due to multi-tiered access control.

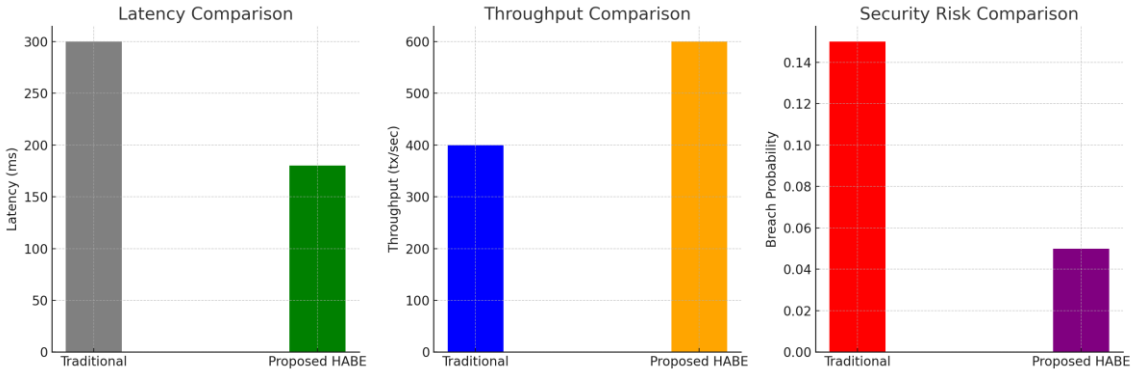

Figure 2: Performance Comparison of Latency, Throughput, and Breach Probability.

6. CONCLUSION

The proposed blockchain-assisted HABE framework ensures secure, scalable, and privacy-preserving data exchange in IIoT networks. By combining smart contracts, decentralized edge storage, and hierarchical attribute-based encryption, the system overcomes limitations of traditional models, such as centralized bottlenecks, single points of failure, and insecure access control. Experimental results affirm improvements in latency, throughput, and security. This architecture holds promise for applications in logistics, healthcare, manufacturing, and beyond under the Industry 4.0 paradigm.

7. REFERENCES

[1] M. Serror, et al., "Challenges and opportunities in securing the industrial Internet of Things," *IEEE Transactions on Industrial Informatics*, 2021.
[2] Q. Qi, et al., "Big data analytics challenges to implementing the IIoT," *Technological Forecasting and Social Change*, 2023.
[3] A. A. Khan, et al., "Role of blockchain and AI in IIoT for SMEs," *Scientific Reports*, 2023.
[4] M. Hader, et al., "Blockchain and big data in textile supply chain," *Journal of Industrial Information Integration*, 2022.
[5] Z. Ullah, et al., "Blockchain-based secure storage for IoT," *IEEE Access*, 2022.
[6] Y. Zhang, et al., "Edge Intelligence in IIoT: Vision and Challenges," *IEEE Network*, 2021.
[7] P. Zhou, et al., "Blockchain-enabled decentralized data access control," *Future Generation Computer Systems*, 2020.
[8] M. Fernandes, et al., "Smart contracts and policy enforcement in IoT," *Sensors*, 2021.
[9] A. Narayanan, et al., *Bitcoin and Cryptocurrency Technologies*, Princeton University Press, 2016.
[10] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the IoT," *IEEE Access*, 2016.
[11] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.
[12] M. Li, et al., "Scalable data sharing in cloud computing using ABE," *IEEE Transactions on Parallel and Distributed Systems*, 2010.
[13] J. Hur and D. K. Noh, "Attribute-based access control with efficient revocation," *IEEE Transactions on Parallel and Distributed Systems*, 2011.
[14] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[15] G. Wood, "Ethereum: A secure decentralized transaction ledger," *Ethereum Project Yellow Paper*, 2014.