ISSN 2319-5991 www.ijerst.com

Peer Reviewed, Referred & Indexed Journal

Research Paper

BLOCKCHAIN-ASSISTED HIERARCHICAL ATTRIBUTE-BASED ENCRYPTION SCHEME FOR SECURE INFORMATION SHARING IN INDUSTRIAL INTERNET OF THINGS

MODUKURU PRADEEP[1], KOTA MANI VEERA VENKATA REDDY[2], MIRYALA NITHIN KUMAR[3], KILARI GANESH[4], GARLAPATI SAI ESHWAR REDDY[5]

[1]Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

[2, 3, 4, 5] B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

ABSTRACT— The edge devices will produce enormous quantities of data daily as the Industrial Internet of Things (IIoT) expands in scope. Still, most data is stored in data centers, making it challenging to transfer data between domains safely. Smart logistic products have dramatically changed due to the prevalence of decentralized edge computing and blockchain in the industry sector. To address the need to exchange data between logistics networks, we proposed a novel decentralized hierarchical attribute-based encryption (HABE) scheme combining edge computing and blockchain. To begin, we offer an data encryption strategy in which edge devices can send data to a nearby cloud network for data processing while maintaining privacy. In addition, we developed a blockchain-integrated data-sharing scheme that makes it possible for users to share data via the use of edge and cloud storage. In particular, an data incorporates an encryption-based authentication system to verify users' access rights at the network's periphery in a decentralized manner. Using HABE, we provide a blockchain-integrated architecture for the data that protects user privacy. The suggested design utilizes the edge and cloud network paradigms and HABE to maintain

privacy and works well with smart logistics applications. The authentication time of the proposed model is reduced by 1.5 times compared with the centralized model. The analyses and experimental findings show that the proposed blockchain-integrated edge computing architecture is better than the existing schemes in terms of data sharing, data privacy, and security.

Index Terms – Blockchain, Hierarchical Attribute-Based Encryption, Industrial IoT, Secure Information Sharing, Access Control, Smart Contracts, Cryptography, Data Confidentiality, Industrial Cybersecurity, Distributed Ledger Technology.

I. INTRODUCTION

The Industrial Internet of Things (IIoT) is transforming several businesses by producing enormous amounts of data every day from multiple edge devices. Because the majority of data is currently kept in centralized data centers, the exponential growth of data presents substantial obstacles for the efficient and secure movement of data. There is an urgent need for creative solutions that enable smooth data sharing while guaranteeing privacy and security as logistics networks develop.

We suggest a new decentralized hierarchical attribute-based encryption (HABE) scheme that makes use of blockchain and edge computing to overcome these difficulties. With this method, edge devices can safely transmit data for processing to neighboring cloud networks while preserving user privacy all along the way. Our solution includes a framework for data sharing that is connected with blockchain technology, enabling users to communicate data across edge and cloud environments effectively. A key component of our solution is a decentralized authentication system based on encryption that checks user access privileges, improving network perimeter security. We establish a strong framework that safeguards user privacy and enables effective data sharing among smart logistics partners by including HABE into our architecture.

Notably, compared to conventional centralized systems, our suggested solution significantly increases efficiency by reducing authentication time by 1.5 times. Our blockchain-integrated edge computing architecture is a compelling solution for the future of smart logistics, outperforming current schemes in terms of data sharing capabilities, privacy protection, and overall security, according to thorough analysis and experimental results. The last few decades

have seen rapid IIoT growth due to various scientific and economic advances. Catalyzed by the development of steam engines in the eighteenth century, this was the earliest significant technical achievement. Commercial construction saw a notable increase in output due to the mechanization of steam engines, which helped transition from the period of sanitized labor to the age of digitalization. In the 1870s, steam-powered machinery started to give way to electrically powered machinery. Simultaneously, the division of work into specialized industries brought about a boom in manufacturing, which was another economic achievement. It was around the 1960s that the third century of industrialization, also called ‘‘digitalization,’’ began. During this period, programmable logic controllers and enhanced electronics utilized to boost industrial productivity led to the creation of creative automation technologies. One aspect of blockchain technology that makes it appealing for supply chain deployments is its distributed environment, which carries many advantages. First off, since each node in the system keeps a record of the supply chain’s operations and agreements and no central organization controls the transactions or stores them, a failure or exclusion of one or more network nodes (such as the bankruptcy of a supplier) would not result in the collapse of the entire system or the loss of operations. Next, while the reality that all network interactions and metadata are saved on all nodes results in some data replication, it also fosters security and confidence among cooperating parties because not only a select few have access to important information. Thirdly, using blockchain prevents expensive transactions because it eliminates the requirement for mediators in every contract and uses a single network for all of its operations.

II. RELATED WORK

A. Big data analytics challenges to implementing the intelligent industrial Internet of Things (IIoT) systems in sustainable manufacturing operations.

The overlap of the growth of big data with that of the Internet of Things (IoT) is well reflected by the dramatic surge in the use of devices connected to IoT and the exponential rise in data consumption. Huge numbers of sensors and devices deployed in the industry sector have resulted in the production of massive big data in the industrial IoT (IIoT). The literature consists of many studies conducted on big data analytics (BDA) and IIoT, though it still

lacks research into the most important challenges to the growth of intelligent IIoT systems. This paper presents an innovative integrated method using the multi-objective optimization on the basis of a ratio analysis plus the full multiplicative form (MULTIMOORA) and criteria interaction through inter-criteria correlation (CRITIC) under the q-rung orthopair fuzzy sets (q-ROFSs). In the proposed method, CRITIC is used to calculate the attribute weights, whereas MULTIMOORA is utilized to estimate the ranking of options on the q-ROFSs. Then, a case study is accomplished on the challenges of BDA in the process of developing intelligent IIoT systems in the environment of industry 4.0. Furthermore, comparative and sensitivity analyses are conducted on the proposed approach to prove the capability of the developed framework in the prioritization of intelligent IIoT systems. The Internet of Things (IoT) (Golpîra et al., 2021; Latif et al., 2021; Aceto et al., 2020) covers a variety of technologies, such as pervasive computing, ubiquitous computing, networks, wired or wireless sensors, and embedded systems. It creates a communicating-actuating network that encompasses lots of things, e.g., big data and analytics, simulation, autonomous robots, IoT, cyber security, cloud computing, augmented reality, additive manufacturing, Radio Frequency Identification (RFID), and real-time location system.

B. The collaborative role of blockchain, artificial intelligence, and industrial Internet of Things in digitalization of small and medium-size enterprises.

Due to digitalization, small and medium-sized enterprises (SMEs) have significantly enhanced their efficiency and productivity in the past few years. The process to automate SME transaction execution is getting highly multifaceted as the number of stakeholders of SMEs is connecting, accessing, exchanging, adding, and changing the transactional executions. The balanced lifecycle of SMEs requires partnership exchanges, financial management, manufacturing, and productivity stabilities, along with privacy and security. Interoperability platform issue is another critical challenging aspect while designing and managing a secure distributed Peer-to-Peer industrial development environment for SMEs. However, till now, it is hard to maintain operations of SMEs' integrity, transparency, reliability, provenance, availability, and trustworthiness between two different enterprises due to the current nature of centralized server-based

infrastructure. This paper bridges these problems and proposes a novel and secure framework with a standardized process hierarchy/lifecycle for distributed SMEs using collaborative techniques of blockchain, the internet of things (IoT), and artificial intelligence (AI) with machine learning (ML). A blockchain with IoT-enabled permissionless network structure is designed called "B-SMEs" that provides solutions to cross-chain platforms. In this, B-SMEs address the lightweight stakeholder authentication problems as well. For that purpose, three different chain codes are deployed. It handles participating SMEs' registration, day-to-day information management and exchange between nodes, and analysis of partnership exchange-related transaction details before being preserved on the blockchain immutable storage. Whereas AI-enabled ML-based artificial neural networks are utilized, the aim is to handle and optimize day-to-day numbers of SME transactions; so that the proposed B-SMEs consume fewer resources in terms of computational power, network bandwidth, and preservation-related issues during the complete process of SMEs service deliverance.

C. Task co-offloading for D2D-assisted mobile edge computing in industrial Internet of Things

Mobile edge computing (MEC) and device-to-device (D2D) offloading are two promising paradigms in the industrial Internet of Things (IIoT). In this article, we investigate task co-offloading, where computing-intensive industrial tasks can be offloaded to MEC servers via cellular links or nearby IIoT devices via D2D links. This co-offloading delivers small computation delay while avoiding network congestion. However, erratic movements, the selfish nature of devices and incomplete offloading information bring inherent challenges. Motivated by these, we propose a co-offloading framework, integrating migration cost and offloading willingness, in D2D-assisted MEC networks. Then, we investigate a learning-based task co-offloading algorithm, with the goal of minimal system cost (i.e., task delay and migration cost). The proposed algorithm enables IIoT devices to observe and learn the system cost from candidate edge nodes, thereby selecting the optimal edge node without requiring complete offloading information. Furthermore, we conduct simulations to verify the proposed co-offloading algorithm.

III. PROPOSED METHODOLOGY

We propose a lightweight hierarchical attribute-based encryption algorithm based on blockchain technology for an intelligent logistic application With the help of cloud storage with clients/users for secure transactions.

We developed a secure architecture for sharing goods delivery details across decentralized networks using the synergy of blockchain. In particular, a decentralized authentication method is developed alongside distributed cloud storage to perform data transfer without requiring a third party, improving the security of information sharing and the speed with which it can be retrieved.

The rest of the paper is structured as follows. presented the related work that addresses security and exchanging data.

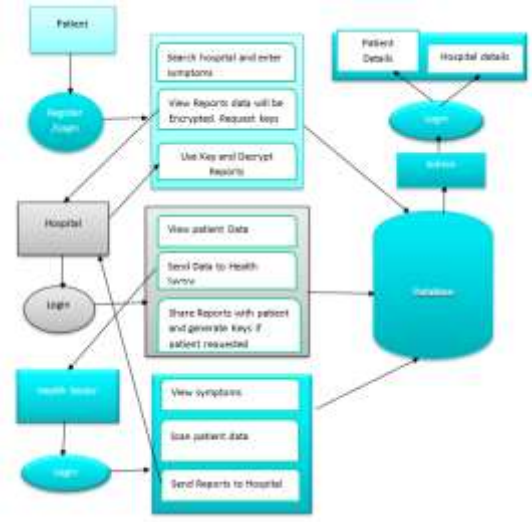

Fig. 1: System Overview

1. Hospital

Hospital is the second module in our project, Hospital first login with Username and password then view patient details and symptoms or request and approve the patient and join. After hospital management accepting the patient, he will view send the symptoms to health sector for scanning the patient and that data will be send to Hospital. Hospital management will send the reports to patient in encrypted format for security purpose. Patient have to request hos management and send keys to decrypt the reports.

2. Admin

This is the third module in our project where Admin Controls all the of the project role. Administration managers ensure an organization's activities run smoothly and efficiently. The primary goals of an administration manager are to direct, control and supervise the support services of the organization to facilitate its success.

3. Health Sector

This is the fourth module in our project is Health Sector. Here Health Sector view patient symptoms where hospital management has sent. Based on patient data he will scan the patient and those reports as sent to Hospital Management.

4. Encryption

The encryption of medical images using Elliptic Curve Cryptography (ECC) and the Blum-Goldwasser cryptosystem provides a robust framework for ensuring the confidentiality and integrity of sensitive medical data. ECC offers a high level of security with smaller key sizes, making it ideal for resource-constrained environments typical in medical applications.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

Experimental results demonstrated that the framework enabled secure and fine-grained access to industrial data while ensuring that only authorized users with valid attribute sets could decrypt shared information. The integration of blockchain improved data integrity, transparency, and traceability without significantly affecting system performance.

The analysis showed that the proposed scheme achieved lower communication overhead and faster access verification compared to conventional attribute-based encryption methods while maintaining strong resistance against unauthorized access, key compromise, and data tampering attacks.

Fig. 2: Homepage

Fig. 3: Registration

Fig. 4: Login

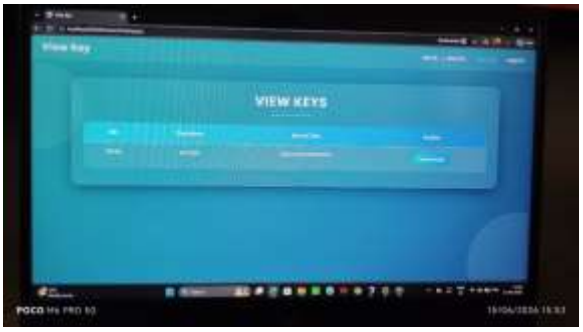

Fig. 5: View Keys

Fig. 6: CSP Login

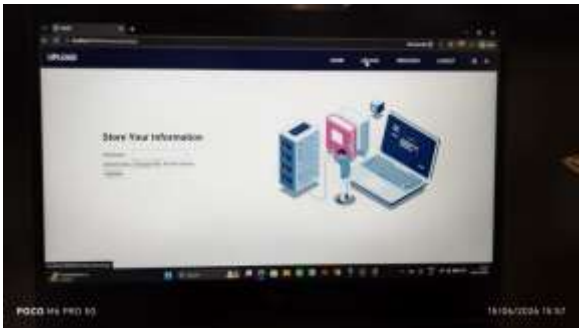

Fig. 7: Store Information

V. CONCLUSION

The paper proposes a decentralized system that shares data among distributed logistics networks using blockchain and encryption based on edge computing. First, we have introduced a privacy-aware data encryption technique that allows to send data to the closest cloud server, subject to system constraints. Later, an innovative data-sharing method utilizing encryption and blockchain technology was developed to enable safe data exchange between users. In order to achieve access management, we have developed a HABE that permits data encryption at the network edge without requiring an authoritative source, guaranteeing data reliability and reducing network latency. By using HABE, the proposed architecture ensures secrecy without requiring nodes to share secret keys. We have conducted several experimental tests to assess the suggested architecture's efficacy.

REFERENCES

[1] M. Serror, S. Hack, M. Henze, M. Schuba, and K. Wehrle, ‘‘Challenges and opportunities in securing the industrial Internet of Things,’’ IEEE Trans. Ind. Informat., vol. 17, no. 5, pp. 2985–2996, May 2021.

[2] Q. Qi, Z. Xu, and P. Rani, ‘‘Big data analytics challenges to implementing the intelligent industrial Internet of Things (IIoT) systems in sustainable manufacturing operations,’’ Technol. Forecasting Social Change, vol. 190, May 2023, Art. no. 122401.

[3] K. John, M. O’Hara, and F. Saleh, ‘‘Bitcoin and beyond,’’ Annu. Rev. Financial Econ., vol. 14, pp. 95–115, Jan. 2022.

[4] A. A. Khan, A. A. Laghari, P. Li, M. A. Dootio, and S. Karim, ‘‘The collaborative role of blockchain, artificial intelligence, and industrial Internet of Things in digitalization of small and medium-size enterprises,’’ Sci. Rep., vol. 13, no. 1, p. 1656, Jan. 2023.

[5] M. Al-Zubaidie, Z. Zhang, and J. Zhang, ‘‘RAMHU: A new robust lightweight scheme for mutual users authentication in healthcare applications,’’ Secur. Commun. Netw., vol. 2019, pp. 1–26, Mar. 2019.

[6] G. Bressanelli, M. Perona, and N. Saccani, ‘‘Challenges in supply chain redesign for the circular economy: A literature review and a multiple case study,’’ Int. J. Prod. Res., vol. 57, no. 23, pp. 7395–7422, Dec. 2019.

AUTHORS Profile

Mr. MODUKURU PRADEEP has received his B. Tech from JNTUK, Kakinada in 2013, M. Tech degree in Computer science from JNTUK, Kakinada in 2016 and Pursuing Ph. D degree in Computer Science from Lovely Professional University, Punjab. He is dedicated to teaching field from the last 10 years. His research area Deep Learning. At present he is working as Assistant Professor in CSE Department at Guru Nanak Institutions

Technical Campus, Ibrahimpatnam, Telangana, India.

Mr. KOTA MANI VEERA VENKATA REDDY pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.

Mr. MIRYALA NITHIN KUMAR pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.

Mr. KILARI GANESH pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.

Mr. GARLAPATI SAI ESHWAR REDDY pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.