Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 9, September : 2023

SECURE AND PRIVATE DATA STORAGE IN IOT USING BLOCKCHAIN TECHNOLOGY

[#1]PEDDI GANGAIAH,
[#2]B.ANVESH KUMAR, ***Assistant Professor,***
[#3]Dr.V.BAPUJI, ***Associate Professor& HOD,***
Department of Master of Computer Applications,
VAAGESWARI COLLEGE OF ENGINEERING, KARIMNAGAR, TELANGANA.

ABSTRACT
The Internet of Things (IoTs) is a network of sensing devices with diverse capabilities that can be used for a number of tasks. Due to limited data management abilities, limited storage, and security issues, it is extremely difficult to protect networks from unauthorized information access and effectively utilize storage in such settings. Few of the data storage and security options investigated by researchers are suitable for WSN-enabled IoTs. For secure communication in Internet of Things (IoT) devices employing wireless sensor networks (WSN), a blockchain-based decentralized architecture with authentication and privacy-preserving mechanisms is being developed. A cloud computing system communicates with sensor nodes and base stations via protocols for registration, certification, and revocation. The cluster heads use this method to deliver the accumulated data to the BS. As a result, BS keeps all vital data on a decentralized blockchain and sends large amounts of data to the cloud. BS removes all certificates revoked by rogue nodes from the blockchain. The effectiveness of the proposed method is evaluated using detection precision, certification latency, computational and communicational overheads. Simulation, comparison analysis, and security validation results reveal that the proposed technique outperforms existing solutions.

1. INTRODUCTION

One of the most well-known, useful, and preeminent technologies of the present day, the Internet of Things (IoTs) has revolutionized wireless communication and information processing [1]. Internet-enabled "things" (or "IoTs") are those that can be recognized, analyzed, controlled, and localized online. Since the internet is capable of both communication and processing, it can be used to link nearly all IoT devices already in use, enabling the development of new and better uses for these devices [2]. The Internet of Things relies on a vast network of sensor nodes for its monitoring, sensing, and automation capabilities. Together, these nodes form Wireless Sensor Networks (WSNs), which are essential to the IoT [3] due to their ability to detect and track any objects in their immediate vicinity.

Sensor nodes, sometimes known as "motes," are inexpensive, easy to deploy, can communicate with one another, and may cover large regions [4]. By combining sensing, processing, and communication capabilities in a wireless medium, sensor nodes in WSNs allow for real-time tracking and identification of physical events. WSNs are used for a variety of purposes, including but not limited to monitoring, sensing, broadcasting, and data processing [5] [6]. The information volume, however, is enormous and expanding at an unprecedented rate, thus this challenge must be met.

Now, in the information era. WSNs are used in many fields and industries, from the military and business to smart homes and healthcare to surveillance and environmental monitoring and agriculture. [7] [8]. The sensor nodes that make up a WSN have finite resources, including time, memory, processing speed, and communication speed. Thus, as the Internet of Things raises demand for WSNs, new difficulties in effectively implementing them arise. Additionally, security is

a major issue for WSN-enabled IoT. If an attacker successfully compromises a significant number of nodes inside the network, the integrity of the entire network is at risk.

Therefore, WSNs must first detect malicious nodes and remove them from the network before they can participate in the IoT's infrastructure. A synopsis of the results Effective and efficient data storage in WSNs when used with IoT is challenging since sensor node storage is a hot topic of study. The issue of security is also significant in WSN-enabled IoT. Adding blockchain technology and cloud storage for privacy protection, authentication, and storage helps with the aforementioned WSN in IoT issues. The blockchain-based system integrates authentication methods with cloud storage to guarantee secure communication with WSNs, while cloud storage disperses the entire sensor node storage limit. Key benefits of the proposed concept include: Each sensor node is given its certification by the base station, which also serves as its authority. An immutable key mechanism stores all certification keys for nodes. 4) Clouds accumulate vast quantities of sensory information.

2. EXISTING SYSTEM

The proposed network model and the resulting discoveries must be reexamined before moving forward.

The purpose of this research is to conduct a systematic review of the literature about the use of WSNs in IoT applications, with a special emphasis on the incorporation of blockchain technology. This study's key goals include looking into how WSNs can be used for things like secure data storage and user authentication. The data generated by IoT devices can quickly accumulate, so it's important to have a reliable system in place to store it. Previous studies have noticed a variety of problems with storing data from IoT devices in cloud systems [9]. Utilizing hash values has enabled the optimization of cloud computing-based data storage in IoTs, guaranteeing the best possible distribution of that data [10]. As part of an innovative energy-efficient architecture aimed at meeting the problems of the Internet of Things (IoT) and the processing of enormous amounts of data, fog computing is now being applied within the healthcare industry. The ability to retrieve data in real time is facilitated by minimal latency and delay [11]. Recent research has shown a game-changing strategy for improving IoT data handling.

Recovery and survivability, two measures of the scheme's performance, contribute to the system's resilience in the face of localized network outages [12]. To improve data optimization across fog nodes/miniclouds in edge devices, a distributed cloud-IoT system was used. Through efficient traffic aggregation and processing, the proposed method shows promising results in terms of latency and energy utilization [13]. Some have advocated using edge computing in conjunction with sensor nodes to compress data locally and process it quickly.

To get the best results with the least amount of back-and-forth possible, the integrated approach incorporates various monitoring, reconfiguration, and data adaption processes [14]. In order to safely manage and delete individual data from IoT gadgets, a new method has been developed. Key derivation encryption and statistical analysis form the basis of this tactic. Users can rest assured that their private data will remain secure.

Data privacy is maintained while unnecessary costs associated with page transmission are kept to a minimum by employing the derivation key technique [15]. There are more examples of modern authentication procedures developed by various scholars in this reference. There is nothing in the user's material that needs to be rewritten for an academic audience. See also Footnotes 17 and 18. Using mutual authentication, agreement, and random node join procedures, the team created a smart card authentication solution for WSNs. As evidenced by prior research [19], the major goal of this innovation was to improve authentication's efficacy. Without the need for a smart card, a new user-friendly authentication method has been

devised. This technique protects any Wireless Sensor Network (WSN) [20] from insider attacks, theft attacks, and session recovery attacks. Improved privacy and authentication inside a predetermined Wireless Sensor Network (WSN) have been accomplished through the use of a three-factor authentication mechanism that has been shown to increase operational efficiency.

Formal security verification methods were used by the largest project, Automated Validation of Internet Security Protocols and Applications (AVISPA) [21]. In order to provide adequate password verification, a new technique based on mutual authentication was presented [22] that combines biological data with hash and XOR computations. In an effort to tighten up security without sacrificing usability, a new multi-gateway wireless sensor network (WSN) has been developed. This innovative method uses familiar parts from well-known systems, like password authentication and biometric authenticators, to achieve the necessary level of safety. The concept of bio-hashing was also developed to reduce the likelihood of false positives.

The goal is to keep the false-rejection rate low while minimizing the effect on the false-acceptance rate [23].

Disadvantages:

The use of post-attack methods renders the current system vulnerable to a wide variety of assaults.

An adversary can cause confusion among a trustworthy governing body by casting doubt on the veracity of both sent and received messages or packets due to the ineffectiveness of the aforementioned mechanism.

3. PROPOSED SYSTEM

The security concerns were addressed by the proposed method by including a central database. This research describes a method that makes use of both standard sensor nodes (RSN) and nodes that act as the heads of their respective clusters (CHSN). Energy, storage, and processing capabilities of RSNs are severely constrained. The sensor nodes are able to detect nearby occurrences and relay that information to the CHSN, which is a centralized high-sensitivity sensing network. The CHSN, acting in its role as a BTA, is responsible for collecting information from the RSN and facilitating its transfer to the Base Station. All sensor nodes are the BTA's obligation to certify. The BTA checks the legitimacy of each sensor node before accepting it into the network. Sensor nodes in the BTA network have access to login credentials and a wide variety of metrics. The sensor RSN is another source of information that the CHSN collects. Furthermore, hackers can easily intercept and manipulate many sorts of data, such as location, velocity, identity, and detected information, during transmission because of the wireless nature of data transfer in CHSN. As a result, we have blockchain technology.

As a possible answer to these problems, the implementation of a privacy protection approach is proposed.

Initialization, registration, authentication of sensor nodes, message signature and verification, key update, revocation, and tracking are all separate steps in the proposed system. Each stage of the BTA algorithm relies on previously calculated parameters. The CHSN may then collect information from all regular sensor nodes, such as their locations, velocities, identifiers, and power reserves. Additionally, CHSN is accountable for sending its own data to BTA along with any other information deemed necessary. After the CHSN data is acquired, the BTA creates an Untamperable Key Mechanism (UKM) and sends it out to every entity in the CHSN. After then, the CHSN's UKM and any additional keys are propagated to regular sensor nodes

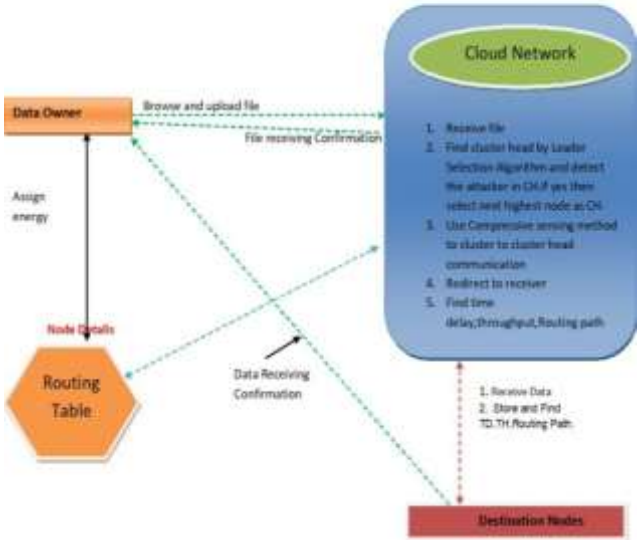
Advantages:

In this proposal, we present a blockchain-based cloud storage service for authentication and data isolation. The Untamperable Key Mechanism is used to safely store the certification keys associated with each sensor node, while the base station is in charge of certifying the nodes. Much of the data collected from sensors is stored on the cloud.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 9, September : 2023

4. SYSTEM ARCHITECTURE

Architecture Diagram



5. MODULES

Data Owner:

The Data Owner will perform a comprehensive review of the data file within this module before delivering the data to the designated Nodes. After the data owner sends the data file to the router, the router activates the sensor node with the highest energy level and distributes the data to individual nodes within a cluster (Nodes A, B, C, etc.). Furthermore, the data owner will reallocate the sensor node's energy if an attacker changes the node's energy.

Cloud Network

The fundamental function of the Cloud Network is to provide a data storage service, hence it is responsible for managing multiple clusters. The most powerful sensor node in the cluster acts as the cluster chief and takes the initiative to start talking to the others. Data Owners can look at things like node specifics, the routing path, latency times, and possible attackers within the context of a router. The data owner sends the file, and the router is responsible for receiving it. The file will then be compressed by the cluster leader based on its relative importance. Another node will become the new cluster leader in the upcoming file transfer. The leader of the cluster will then select a special node by giving priority to the node with the most available energy. The time lag will be calculated based on the delay experienced in the network.

Cluster as Block Chain

Connectivity has been set up between clusters 1, 2, 3, and 4. There are a total of n nodes in the cluster. The most energetic sensor node in a cluster is called the cluster head. The data manager is in charge of deciding how much power to give each node. Clusters and cluster-based networks will be activated once the data manager uploads the necessary data file to the router. The networks will then be able to locate sensor nodes with the highest energy production and simplify the transmission of that energy to the appropriate nodes.

Nodes (End User)

Within this section, the data's owner (hence referred to as "Data Owner") can use a router to distribute the data file to the network's other nodes. No changes are done to the file before it is sent to the nodes. Files of a given type can be downloaded from the internet.

Attacker

The perpetrator places errant radiation sources within range of the intended detectors. The offender has spoken his or her mind about the sensor node's energy source. When an assault is launched against routers in a network, the router's energy is transformed.

6. CONCLUSION

For Internet of Things (IoT) gadgets that use Wireless Sensor Networks (WSNs), a privacy-protecting authentication mechanism has been developed. The blockchain and cloud computing are the foundation of this system. The base station (BS) was in charge of coordinating the initial registration and certification processes for all sensor nodes. A certified Untamperable Key Mechanism (UKM) was required, and its safekeeping and use were under the purview of the cluster administrators. Additionally, the cluster leaders permitted the transfer of the data gathered

by their respective members to the central base station (BS), where it was further divided into two unique groups: critical parameters and sensed data. Data from these sensors was uploaded to the cloud for more secure and convenient long-term storage. New blockchain technology was used to improve data collecting, as it allowed for the immutable and transparent recording of crucial parameters. Defective sensor nodes were removed from the network via the certification revocation procedure. In terms of detection accuracy, certification time, and computing load, the proposed method excelled. The proposed technique has been shown to increase average detection accuracy by 19.33% in simulations and comparative evaluations. A large amount of data was moved to cloud-based storage, ensuring the plan's dependability and efficiency. Our goal for the upcoming time period is to improve the framework by enhancing its data management and resource allocation.

REFERENCES:

1. Y. A. Abdulrahman, M. Kamalrudin, S. Sidek, and M. A. Hassan, ”Internet of things: Issues and challenges,”Journal of Theoretical and Applied Information Technology, vol. 94, no. 1,pp. 52–60, 2016.
2. SK Lo, Y Liu, SY Chia, X Xu, Q Lu, L Zhu, H Ning, Analysis of blockchain solutions for IoT: A systematic literature review, IEEE Access, vol. 7, 2019, pp. 58822-58835.
3. R. V Kulkarni, S. Member, A. F¨orster, and G. K. Venayagamoorthy, ”Computational Intelligence in Wireless Sensor Networks: A Survey,” Communications Surveys & Tutorials, IEEE, vol. 13, no. 1, pp. 68–96, 2011.
4. A. H. Bagdadee, M. Z. Hoque, and L. Zhang, ”IoT Based Wireless Sensor Network for Power Quality Control in Smart Grid,” Procedia Computer Science, vol. 167, pp. 1148–1160, 2020.
5. J. Wang, Y. Cao, B. Li, H. jin Kim, and S. Lee, ”Particle swarm optimization based clustering algorithm with mobile sink for WSNs,” Future Generation Computer Systems, vol. 76,pp. 452–457, 2017.
6. Z. Song-Juan and Y. Jian, ”Distributed data storage strategy in wireless sensor networks,” International Journalof Online Engineering, vol. 12, no. 11, pp. 52–57, 2016.
7. L. Buttyan, D. Gessner, A. Hessler, and P. Langendoerfer, ”Application of wireless sensor networks in critical infrastructure protection: challenges and design options Security and Privacy in Emerging Wireless Networks,” IEEE Wireless Communications, vol. 17, no. 5, pp. 44–49, 2010.
8. {8] R. Singh, D. K. Singh, and L. Kumar, ”A review on security issues in wireless sensor network,” vol. 2, no. 7, pp. 28–34, 2010.
9. H. Cai, B. Xu, L. Jiang, and A. V. Vasilakos, “IoT-Based Big Data Storage Systems in Cloud Computing: Perspectives and Challenges,” IEEE Internet of Things Journal, vol. 4, no. 1,pp. 75–87, 2017.
10. M. Wang and Q. Zhang, “Optimized data storage algorithm of IoT based on cloud computing in distributed system,” Computer Communications, vol. 157, pp. 124–131, 2020.
11. C. Feng, M. Adnan, A. Ahmad, A. Ullah, and H. U. Khan, “Towards Energy-Efficient Framework for IoT Big Data Healthcare Solutions,” Scientific Programming, vol. 2020, pp. 1–9, 2020.
12. M. Asiri, T. Sheltami, L. Al-Awami, and A. Yasar, “A Novel Approach for Efficient Management of Data Lifespan of IoT Devices,” IEEE Internet of Things Journal, vol. 7, no. 5, pp.4566–4574, 2020.
13. P. Maiti, J. Shukla, B. Sahoo, and A. K. Turuk, “Efficient Data Collection for IoT Services in Edge Computing Environment,” in Proceedings - 2017 International Conference on Information Technology, ICIT 2017, 2018, pp. 101–106.

14. M. Adel Serhani, H. T. El-Kassabi, K. Shuaib, A. N. Navaz, B. Benatallah, and A. Beheshti, "Self-adapting cloud services orchestration for fulfilling intensive sensory data-driven IoT workflows," Future Generation Computer Systems, vol. 108, pp. 583–597, 2020.