SECURING IOT DATA WITH BLOCKCHAIN: PRIVACY AND AUTHENTICATION

#1MITTAPALLY SRIHARI,
#2JUPAKA SRINIVAS,
#3SADULA SANKEERTH, *Assistant Professor,*
Department of Computer Science and Engineering,
SREE CHAITANYA INSTITUTE OF TECHNOLOGICAL SCIENCES, KARIMNAGAR, TS.

ABSTRACT: The Internet of Things (IoT) is made up of a diverse set of tracking devices with a variety of tasks. Networks struggle to keep data secure, optimize storage, and prevent illegal access, making it difficult to manage information efficiently. While scientists have devised various approaches to ensure data security and privacy, only a handful of these techniques are effective for Internet of Things (IoT) devices that are integrated with Wireless Sensor Networks. As a result, a decentralized blockchain framework has been developed. To enable secure communication in Internet of Things (IoT) devices that employ wireless sensor networks (WSNs), this architecture includes authentication and privacy measures. The Base Station (BS) and sensor nodes link in a cloud computing environment through a series of stages that include registration, certification, and revocation. In this arrangement, the cluster leaders communicate the collected data to the base station. BS use blockchain technology to store critical data on a public ledger, with enormous amounts of data transmitted to cloud storage. BS removes any invalidated certificates issued by hostile nodes from the blockchain. The effectiveness of the proposed method is evaluated in terms of item detection efficiency, certification time, and computation and communication expenses. Moreover The security validation, comparison analysis, and simulated results all indicate that the proposed solution is preferable to the existing ones.

Keywords:Detection accuracy, Certification delay, Computational,Communicational overheads

I. INTRODUCTION

People increasingly regard the Internet of Things as a widespread, valuable, and versatile instrument for data processing and wireless communication. The Internet of Things (IoT) is a collection of objects, or "things," that can be found, understood, controlled, and identified via the internet. Because the internet can manage and deliver data, practically everything can be linked to it in the twenty-first century. This makes it easier to create multiple applications that perform effectively together. A group of sensor modules is configured in a standardized manner to facilitate IoT automation, tracking, and sensing. This group of nodes, known as Wireless Sensor Networks (WSNs), is an important component of the Internet of Things because it can detect and monitor physical objects or activities in a specific region.

The previously stated sensor nodes, or "motes," are small, low-cost, internally connected, and distributed in specific locations. These sensor nodes enable WSNs to monitor and perceive physical objects in real time by combining many sensing, processing, and transmission tasks via wireless media. The specifics of how WSNs work vary by area, but their primary goals remain the same: process information, broadcast it, perceive it, and monitor it. However, in this technological age, data is being generated at an unprecedented rate, and this must be noted. Many individuals agree that WSNs have a wide range of applications, including business, smart homes, surveillance, and habitat tracking. There are limitations to how much data a sensor node can keep, how much power it can utilize, how much energy it can consume, and how quickly it can communicate with other nodes. As a result, the Internet of Things' WSN requirements are expanding with time, posing new challenges in terms of its effective implementation. In addition, security remains a critical problem for WSN-enabled IoT. If an attacker gains unauthorized access to the system with the intent of compromising the nodes, they pose a threat to network security.

As a result, for WSNs to be functional in the IoT system, they must be able to detect and remove malicious nodes. Summary of the Contribution (A) The limited storage space of sensor nodes makes it difficult to store data effectively and efficiently in WSNs when paired with IoT. This is an important field of study. Security is another critical concern that arises with WSN-enabled IoT. To address the WSN concerns mentioned above in IoT, cloud storage and blockchain technology should be used to secure privacy, simplify authentication, and store data. A blockchain-based solution combines cloud storage and authentication mechanisms to enable secure access to WSNs. The cloud storage itself determines the storage limits for sensor nodes. The proposed approach would primarily accomplish the following:

- ➢ A blockchain-based method for storing data in the cloud, protecting privacy, and proving identity
- ➢ The master station sends green light to each sensor node.
- ➢ The certification key for each node is stored on an immutable key device.

A large amount of information has been detected and is saved in the cloud.

2. EXISTING SYSTEM

To examine data storage, authentication, and security, a brief overview of current research on WSN-based IoT employing blockchain technology is conducted before delving into the specifics of the suggested network design and the findings that were discovered. The massive volumes of data generated by IoT devices must be swiftly stored for real-time usage and retrievable when required. The idea of keeping data from Internet of Things devices in the cloud has raised several concerns. When storing data in the cloud, hash values ensure that data sharing within the Internet of Things operates as efficiently as possible. A novel energy-efficient approach for IoT big data solutions in healthcare has been developed through the usage of fog computing. With minimal latency and delay, the information can be accessed in real time. It has been discovered that there is one more special method for efficiently managing data in Internet of Things devices:

Recoverability and survivability metrics, which both indicate how well the system can withstand a network outage in a specific location, were used to evaluate the efficacy of the plan. Data across fog nodes and miniclouds in edge devices has been improved with a distributed cloud-IoT design. Through effective traffic collection and processing, the proposed method provides favorable latency and energy consumption results. Rapid data compression and processing near data storage locations has been integrated with edge computing and sensor nodes.

Because the integrated technique handles duties like data adaption, reconfiguration, and monitoring, communication costs are reduced. Using key derivation encryption and data analysis, a secure method for managing and erasing personally identifiable data stored on Internet of Things (IoT) devices has been developed. A technique that perfectly balances data privacy and page transfer costs is used to safeguard sensitive user data. More recently, academics have developed a wide range of widely applicable authentication techniques.

To make authentication as fast and simple as feasible, a mutual authentication, agreement, and random node join-based smart card authentication system for WSNs was created. In any WSN, a novel, user-friendly identification technique has been developed to thwart insider, theft, and session recovery assaults. A smart card is not necessary for this procedure.

To enhance performance, a three-factor authentication technique has also been included. In particular, this improves privacy and authentication in WSNs.

For the significant project known as Automated Validation of Internet Security Protocols and Applications (AVISPA), formal security checking procedures have to be implemented.

An further class of mutual authentication-based techniques combined hash and XOR operations with biological information to verify the accuracy of the password. The development of a multi-gateway WSN, aimed at enhancing security, represents a new development in user authentication convenience. This innovative approach provides the necessary level of security by combining elements of popular authentication schemes, methodologies, and password sensor authenticators. Another concept that was developed to reduce the quantity of incorrect acceptances and false rejections while maintaining a low quantity of false rejections is bio-hashing.

Disadvantages:

The current investigation uses post methods, which lowers system efficiency and could lead an attacker to claim that files or messages sent and received are not counted, which would be perplexing to a reliable authority.

3. PROPOSED SYSTEM

The proposed solution takes use of a central database to alleviate security concerns. The suggested method uses both cluster head sensor nodes (CHSN) and regular sensor nodes (RSN). RSNs have limited energy, storage, and processing capabilities. Sensor nodes identify local occurrences and transmit the information they collect to the CHSN. CHSN is responsible for collecting data from RSNs and transmitting it to the Base station, where it acts as a Trusted Authority BTA. BTA is responsible for approving all sensor nodes. Before joining the network, the sensor nodes must first obtain BTA legality. The BTA feeds the sensor nodes with various parameters and authentication information. Furthermore, the sensor RSN communicates the detected information to CHSN. Furthermore, CHSN uses wireless data transfer to BTA, making it vulnerable to attacks from hackers who can simply take and manipulate data such as position, speed, identity, and information felt during transmission. As a result, a blockchain-based privacy-preserving solution is implemented to address these issues.

Text is not included.The recommended architecture includes multiple phases such as setup, registration, authentication of sensor nodes, message signing and verification, key update, revocation, and tracing. BTA initially identifies the parameters needed for each step. Following that, each typical sensor node can begin the initialization process by providing CHSN with pertinent information (such as position, velocity, identity, remaining energy, and detected data). CHSN also transmits BTA all of its own data. Following data collection from CHSN, BTA uses the information to create an Unalterable Key Mechanism (UKM), which is subsequently sent to each CHSN. After that, CHSN kept UKM and later distributed additional keys to ordinary sensor nodes.

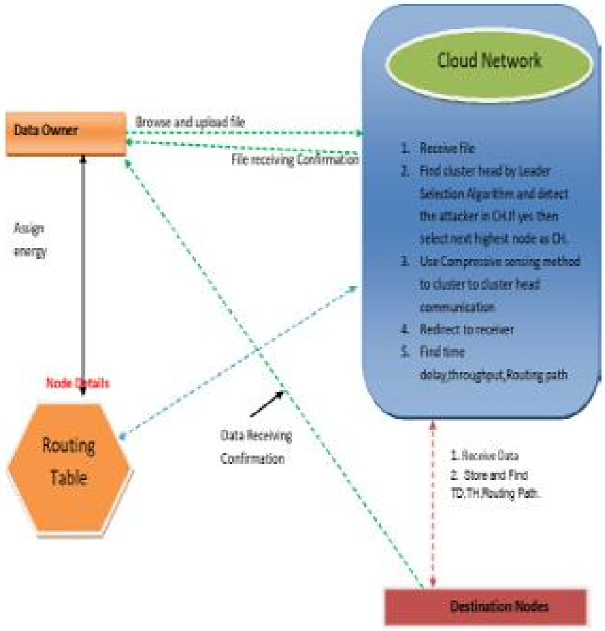
Advantages:

This method uses blockchain technology to ensure privacy and authenticity by utilizing cloud storage. Every sensor node's certification credentials are kept at the base station in an immutable key mechanism.

A huge amount of observed data is kept in clouds.

SYSTEM ARCHITECTURE:

Architecture Diagram


Cloud Network
Data Owner
Browse and upload file
File receiving Confirmation
1. Receive file
2. Find cluster head by Leader Selection Algorithm and detect the attacker in CH.If yes then select next highest node as CH.
3. Use Compressive sensing method to cluster to cluster head communication
4. Redirect to receiver
5. Find time delay,throughput,Routing path
Assign energy
Node Details
Routing Table
Data Receiving Confirmation
1. Receive Data
2. Store and Find TD,TH,Routing Path.
Destination Nodes

4. MODULES

Data Owner:

The Data Owner will review this module's data file before sending it to the designated nodes. Once the router receives the data file from the data owner, it will join the cluster. The sensor node in each cluster with the highest energy will be activated and routed to certain nodes (A, B, C, etc.). In addition, if an attacker modifies the energy of a sensor node, Data Owner will redistribute it.

Cloud Network

The Cloud Network is in charge of multiple groups, including 1, 2, 3, and 4. A cluster is made up of n nodes (n1, n2, n3, n4). The cluster leader is the sensor node with the most energy in the group. It will start communicating with the other nodes. People who have data in a router can view information about nodes, routing routes, time delays, and attackers. Before the router receives the file from the data owner, the cluster head determines which files to compress based on their size. When the file is transmitted again, a different node becomes the cluster master. In the same manner, the cluster head will select a different node based on its energy level. The route delay will be used as a starting point to calculate the time delay.

Cluster as Block Chain

Clusters 1, 2, 3, and 4 are all linked to each other and their respective n-nodes.The most powerful sensor unit in the cluster is known as the Cluster Head. The individual who controls the data will determine how much electricity each node requires. The individual who owns the data will submit the file to the router. The router will then activate clusters and use cluster-based networks to identify the nodes with the most energy monitors and route them to specified nodes.

Nodes (End User)

With this module, the Nodes can use a server to retrieve data files from the Data Owner. The Nodes receive the file but make no changes to it. Certain data files can only be transferred to users on the network.

Attacker

The attacker is the one who transmits bogus energy to the appropriate sensor nodes. The attacker extracts the energy from encryption and delivers it to the specified sensor site. A node attack causes a server's power to change.

5. CONCLUSION:

For IoTs connected to a Wi-Fi network, a powerful authentication solution that protects privacy was developed using block chains and cloud storage. Initially, BS was in responsible of validating and registering each sensor point. Each key setting was saved in an Untamperable Key Mechanism (UKM), which was controlled by the cluster head once certified. Furthermore, the leaders of each cluster communicate the information gathered from their members to BS. It is separated into two categories:

(i) key factors and (ii) detected data. The massive amount of data acquired was subsequently transferred to the cloud, where it was stored more reliably and promptly. The important factors were also retained on the new blockchain technology to make the data more difficult to modify and more transparent. The procedure for revoking certification effectively removed sensor nodes that were not performing properly. The suggested method outperformed others in terms of locating things, taking longer to certify, and utilizing more resources. The comparison analysis and simulated results demonstrate that the suggested strategy is 19:33% more accurate than the average for finding objects. Sharing a large amount of information on the cloud ensured that the anticipated plan would function properly and reliably. We intend to achieve better future results by improving the framework's resources and data management.

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 Journal of 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] 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 Perspectives and Challenges,” Computing: 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.