iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VII **Month of publication:** July 2022

DOI: https://doi.org/10.22214/ijraset.2022.45238

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VII July 2022- Available at www.ijraset.com

Block Chain Based Information Storage with Concealment and Authentication in Internet of Things

E.Thrishu[1], V. Shreya[2], M. Prassananjali[3]
Department of Computer Science And Engineering, Sridevi Women's Engineering College,Vattinagulapally, Gandipet, R.R.DIST-500075, India

Abstract: ***In both academics and industry, the Internet of Things (IOT) is driving a digital revolution. It makes people's life easier, but it also raises concerns about security and privacy. Blockchain, a decentralised database based on cryptographic principles, has the potential to impact a wide range of industries, including manufacturing, banking, and commerce. Though researchers offer a variety of security and data storage solutions, only a few are suitable for WSN- enabled IoTs. As a result, a blockchain- based decentralised framework with authentication and concealment- preserving techniques has been established for secure communication in WSN-enabled IoTs. Cluster heads send the collected data to the Base Station (BS) in this scheme. As a result, BS keeps track of all the key parameters on the distributed blockchain, which is quite extensive.***
Keywords: Blockchain, Concealment and Authentication, security, Wireless Sensor Network.

I. INTRODUCTION

Internet of Things (IoTs) is one of the most popular, beneficial, and dominant technologies in wireless communication and data processing in today's world. IoTs are described as "things" that are identifiable, comprehensible, manageable, and can be located through the internet. Because of the internet's communicational and computing capabilities, practically all things in IoT can be connected to it in today's world, allowing for the development of a variety of more relevant and suitable applications. In the Internet of Things, several sensor nodes are used for monitoring, sensing, and automation. Wireless Sensor Networks (WSNs) are a collection of these nodes that are an inseparable aspect of IoT because they can sense and monitor any physical things/activities within a given area. When itcomes to the rapid development of information technology in the field of security, blockchain plays a key role, as it is a decentralised system. Blockchain technology is a distributed public ledger in which all transaction details are recorded without the useof a third party intermediary, and it stores a massive amount of data in a single block, as well as providing more security to the data through hashing techniques that prevent data loss. To frame a blockchain technology, blocks are interconnected to form a chain structure, with each block containing both the hash value and the previous hash. The prior hash of the current block is compared to the previous block's hash value, which aids in determining if the block is malicious or not. Data in theblockchain has immutability features, which means that once it is updated into the block, it cannot be changed, preventing data changes. Blocks provide broad access to users linked to the blockchain network, but not to their personal data. A significant proportion of sensed data is stored in clouds .To store sensitive data, blockchain uses consensus methods such as proof of labour and proof of stake. Security, storage, sharing, and authentication of data are some of the difficulties that big data and cloud face. Where the research obstacles are found from the survey, blockchain is explored to overcome these issues. Furthermore, with a WSN-enabled IoT, security is a major concern. The network security becomes a threat if an attacker assaults the network and purposefully compromises the nodes. As a result, before becoming an active member of the IoT infrastructure, WSNs must be able to identify and remove rogue nodes from the network.

II. OBJECTIVES

The Internet of Things (IoTs) is made up of a huge number of sensing devices with a variety of capabilities that can be used for a variety of purposes. Due to low data handling capabilities, limited storage, and security considerations, it is difficult to protect networks against unauthorised information access and efficiently utilise storage in such settings. Though researchers offer a variety of security and data storage solutions, only a few are suitable for WSN-enabled IoTs. As aresult, a blockchain-based decentralised framework with authentication and concealment-preserving techniques is beingdeveloped for secure communication in IoTs that are supportedby wireless sensor networks (WSNs).

III. METHODOLOGY ANDDATABASE USED

Using a centralised database, the approach is designed to tackle security concerns. The suggested approach employs two types of sensor nodes: Regular Sensor Nodes (RSN) and Cluster Head Sensor Nodes (CHSN). In terms of energy, storage, and processing capability, RSN are limited. These sensor nodes detect occurrences in their environment and send the data to CHSN. CHSN is in charge of obtaining data from RSN and forwarding itto the base station, which acts as a Trusted Authority (BTA). BTAis in charge of certifying all sensor nodes. BTA first verifies the legitimacy of sensor nodes before allowing them to join the network. BTA provides authentication information and many parameters to sensor nodes. In addition, the sensor RSN sends thedata it has gathered to CHSN. Furthermore, because the data is sent from CHSN to BTA via wireless media, it is very easy for attackers to steal and fake data such as position, speed, identity, and sensed data during transmission. As a result, a privacy- preserving system based on block chains is presented to address these issues. Initialization phase, Registration phase, sensor node authentication phase, message signing and verification phase, key After then, all regular sensor nodes can begin the initialization process by sending their data to CHSN (such as location, speed, identity, residual energy, and detected data). In addition, CHSN broadcasts all information, including its own, to BTA. After gathering data from CHSN, BTA uses that data to create an Untamperable Key Mechanism (UKM), which it then distributes to all CHSN. After that, CHSN stores UKM and distributes additional keys to ordinary senor nodes.

The following are the primary benefits of the proposed scheme:

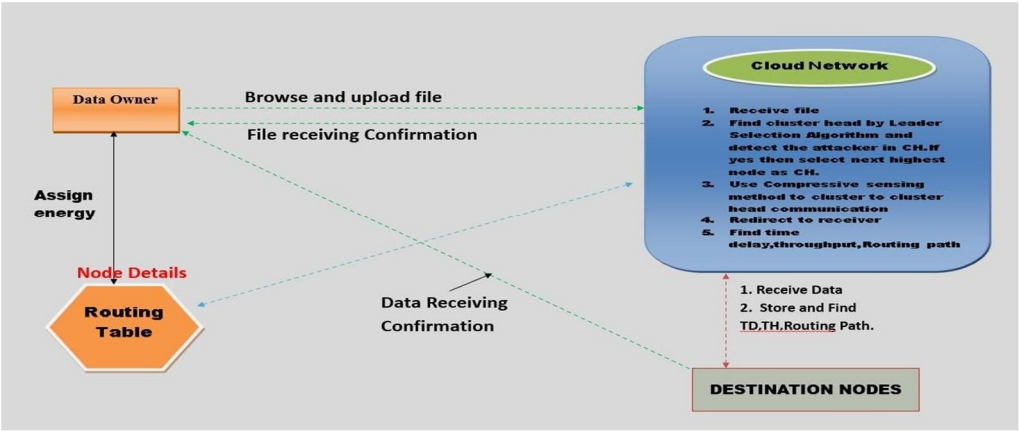
1) A blockchain-based approach for maintaining privacy andauthentication while storing data in the cloud.
2) All sensor nodes are certified by the base station, and theircertification keys are stored in the Untamperable Key Mechanism.
3) Clouds hold a significant amount of sensory data. Components of the blockchain concept that has been proposed

- *Base Station (BTA):* The Base Station (BTA) is a critical component of the WSN-enabled IoTs Blockchain system. (BTA) created the new messages and carried out the block generation mining operation. The validated blocks are then uploaded to the blockchain and disseminated throughout the network. When a sensor node's certificate is revoked by (BTA), the blockchain is updated with the new key parameters. (BTA) ensures sensor node authentication and gives certification to them within its communication range.
- *Cluster heads (CHSN):* Cluster heads (CHSN) are also important parts of the blockchain. During the certification procedure, (BTA) provides (CHSN) with the key parameters that are kept in blockchain. All of these parameters were saved in UKM by (CHSN). These nodes are in charge of broadcasting acquired data to other nodes (BTA).
- *Messages:* In WSN-enabled IoTs, there are basically three messages that are crucial. There are three types of messages: registration, certification, and revocation.

The blockchain's fundamental components are blocks, update phase and revocation phase, and tracing phase are all included in the proposed scheme. which have a block header and a block body. A block's header typically includes a time stamp, a list of transactions, and a hash of the previous and current block.block generally consists of time stamp, list of transactions, and hash of previous and current block.

IV. RESEARCH DISCUSSION

The Data Owner will upload the data file to the router; clusterswill be activated in the router, and cluster-based networks willbe used to choose the highest energy sensor nodes and transmitthem to a specific node. The Data Owner can send the data fileto the Nodes via router. The file is received by the Nodes without any changes to the File Contents. Users may only get



A. Architecture

Data Owner, Cloud Network, Destination Nodes, and Routhing Table are the modules we used in our project. specific data files from within the network.

V. RESULT

The Data Owner will first browse the data file before sending it to the appropriate Nodes. The data owner will upload their data file to the router, and the router will connect to the cluster. The highest energy sensor node in the cluster will be enabled, and it will send data to specific nodes (A,B,C, etc.). To provide data storage services, the Cloud Network manages numerous clusters (cluster 1, cluster 2, cluster 3, and Cluster 4). There are n-number of nodes in a cluster (n1,n2,n3,n4,...), and among the clusters, the sensor node with the most energy is considered the cluster head, and it communicates first. The energy will be assigned by the Data Owner to each and every node.

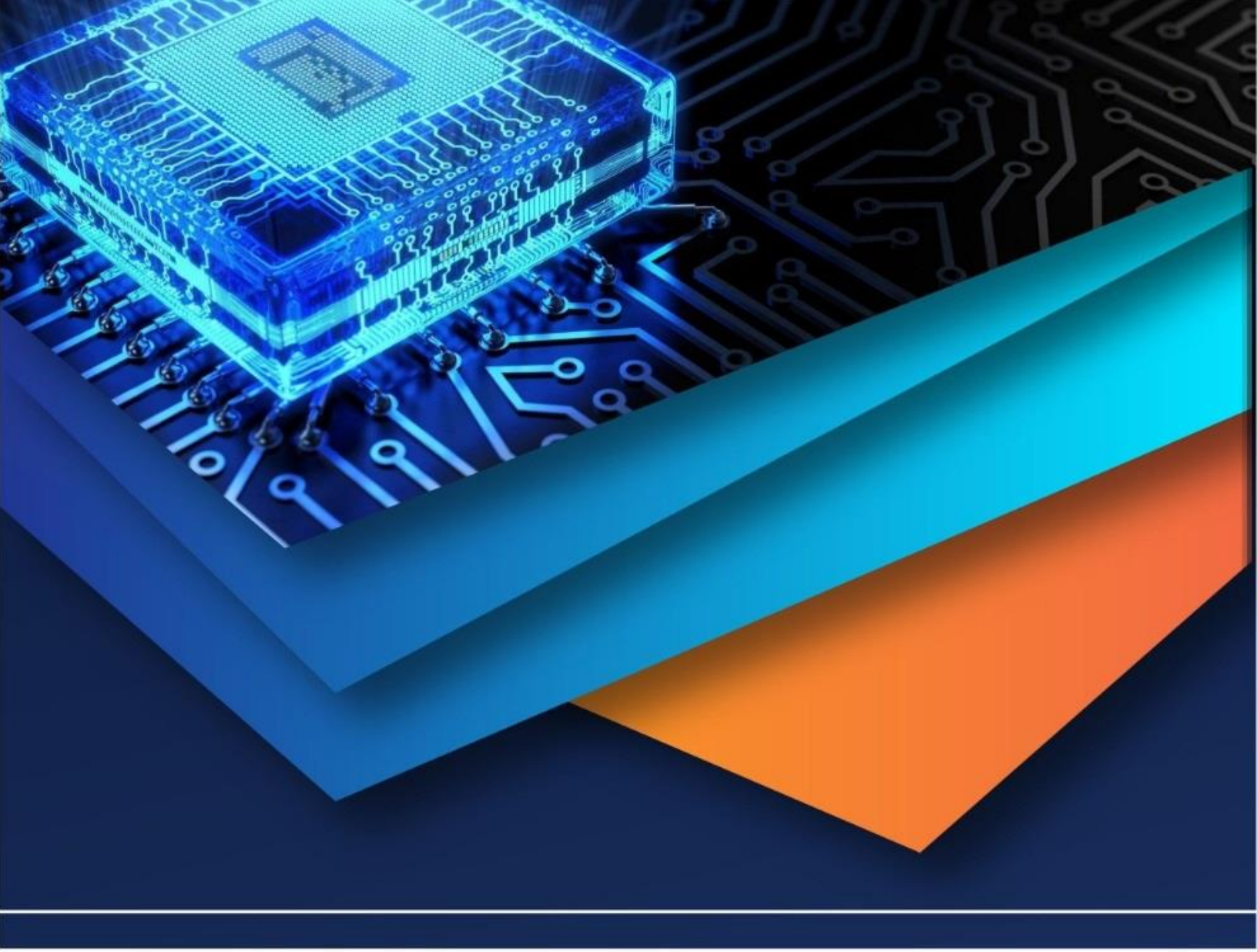
For WSN enabled IOTs, a privacy-preserving authentication mechanism based on block chain with cloud data storage was successfully implemented. The Data Owner will then explore the files and choose one to send to a cloud network.The cloud network then maintains several clusters, initialises all nodes, and selects the node with the most energy as the cluster head, which determines time delay, throughput, and routing paths, and transmits data to a specific target node.

VI. CONCLUSION

For WSN enabled IoTs, a privacy-preserving authenticationtechnique based on block chain with cloud data storage wassuccessfully implemented. BS was in charge of the registration and certification of all sensor nodes at first. All key parameters were kept in an Untamperable KeyMechanism (UKM) managed by the cluster heads after the certification procedure was completed. Furthermore, the cluster heads broadcast the information gathered from its members to BS, which is then divided into two parts: I important parameters and ii) sensed data. The vast amount of data collected was then uploaded to the cloud for more secure and efficient storage.

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. Forster, and G. K. Venayagamoorthy, ¨ ”Computational Intelligence inWireless Sensor Networks: A Survey,” Communications Surveys & Tutorials, IEEE, vol. 13, no. 1, pp. 68–96, 2011.
[4] Jin Ho Park, and Jong Hyuk Park (2017), ‘Blockchain security in cloud computing: Use cases, challenges, and solutions’, Symmetry, No. 9(8), pp.164-177.
[5] Wenli Yang, ErfanAghasian, Saurabh Garg, David Herbert, Leandro Disiuta and Byeong Kang (2019), 'A Survey on Blockchain - based Internet Service Architecture:requirements, challenges, trends and future', IEEE Access
[6] Turesson H., Roatis A., Laskowski M. and Kim H., (2019). 'Privacy-Preserving Blockchain Mining: Sybil- resistance by Proof-of-Useful-Work', arXiv preprint, arXiv:1907.08744.
[7] Niranjanamurthy M., Nithya B.N. and Jagannatha S., (2018), ‘Analysis of Blockchain technology: pros, cons andSWOT’, Cluster Computing, pp.1-15.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY