INTEGRATION OF BLOCKCHAIN IN IOT TO PREVENT PERSONAL DATA VIOLATION

NIVYAA. A. S, SANDHIYA. M , SHARMI. R. A , SUBASH CHANDAR .A

Department of Computer Science and Engineering
Jeppiaar Engineering College,
Chennai.

Department of Computer Science and Engineering
Jeppiaar Engineering College,
Chennai.

Department of Computer Science and Engineering
Jeppiaar Engineering College,
Chennai.

Associate professor,
Department of Computer Science and Engineering,
Jeppiaar Engineering College,
Chennai.

Abstract -- **Internet of Things (IoT) plays an indispensable role for Industry, people are committed to implementing a general, scalable and secure IoT system to be adopted across various industries. However, existing IoT systems are vulnerable to single point of failure and malicious attacks, which cannot provide stable services. Due to the resilience and security promise of blockchain, the idea of combining blockchain and IoT gains considerable interest. However, blockchains are power-intensive and low-throughput, which are not suitable for power-constrained IoT devices.**

We propose a blockchain-enabled efficient data collection and secure sharing scheme combining. Blockchain and deep reinforcement learning (DRL) to create a reliable and safe environment. In this scheme, DRL is used to achieve the maximum amount of collected data, and the blockchain technology is used to ensure security and reliability of data sharing.

The proposed system takes advantage of blockchain technology in terms of its transparency and tamper-proof nature to support fair goods exchange between merchants and suppliers. Additionally, the decentralization and pseudonymity property will play a significant role in preserving the privacy of participants in the blockchain.

Keywords – **security promises , secure sharing , deep reinforcement learning , decentralization .**

1 - INTRODUCTION

Existing security technologies are just not enough to deal with this problem. Blockchain has emerged as the possible solution for creating more secure IoT systems in the time to come. In this paper, first an overview of the blockchain technology and its implementation has been explained; then we have discussed the infrastructure of IoT which is based on Blockchain network and at last a model has been provided for the security of internet of things using blockchain.

1.1 OVERVIEW

Internet of Things (IoT) is a technique in which physical objects are interconnected through wired or wireless technologies, which in turn connected to the Internet, that can be accessed from anywhere at any time. In recent days, we can see that various industrial sectors were adopting many IoT applications, including manufacturing, home automation, transportation, and healthcare any many more. Many large-scale industrial IoT (IIoT) infrastructures are developed, deployed and maintained by individual parties nowadays and they are cloud-based and depend on centralized communication models, in which all devices are identified, authenticated, and connected through cloud servers that provide more computation and storage capacities.

Along with the fast growth of the size and complexity of IIoT networks, centralized IIoT solutions is also becoming more cost expensive because of the high deployment and maintenance cost for the network and cloud infrastructures. This problem is further inflamed by the increasing demand that IIoT networks from different parties should be able to communicate and collaboratively provide unchangeable and verifiable data. With long established IIoT networks, data provided by individual industrial parties may not be reliable because they can be fake or tampered by attackers or the owner of the data. It is important to have mechanisms to verify the reliability of data in IIoT networks.

The fast-developing Industrial Internet of Things (IIoT) technologies provide a promising opportunity to build large-scale systems to connect numerous heterogeneous devices into the Internet. Most existing IIoT infrastructures are based on a centralized architecture, which is easier for management but cannot effectively support immutable and verifiable services

among multiple parties. Blockchain technology provides many desired features for large-scale IIoT infrastructures, such as decentralization, trustworthiness, trackability, and immutability.A blockchain-based IIoT architecture to support immutable and verifiable services is created here. However, when applying blockchain technology to the IIoT infrastructure, the required storage space posts a grant challenge to resource-constrained IIoT infrastructures. To address the storage issue, a hierarchical blockchain storage structure, ChainSplitter is used. Specially, the proposed architecture features a hierarchical storage structure where the majority of the blockchain is stored in the clouds, while the most recent blocks are stored in the overlay network of the individual IIoT networks.

The proposed architecture seamlessly binds local IIoT networks, the blockchain overlay network, and the cloud infrastructure together through two connectors, the blockchain connector and the cloud connector, to construct the hierarchical blockchain storage. Theblockchain connector in the overlay network builds blocks in blockchain from data generated in IIoT networks, and the cloud connector resolves the blockchain synchronization issues between the overlay network and the clouds. We also provide a case study to show the efficiency of the proposed hierarchical blockchain storage in a practical Industrial IoT case.

Internet of Things (IoT) is now in its initial stage but very soon, it is going to influence almost every day-to-day items we use. The more it will be included in our lifestyle, more will be the threat of it being misused. There is an urgent need to make IoT devices secure from getting cracked. Very soon IoT is going to expand the area for the cyber-attacks on homes and businesses by transforming objects that were used to be offline into online systems. Blockchain has emerged as the possible solution for creating more secure IoT systems in the time to come.

Blockchain technology is now getting too much of attention from software scientists since it has been cre- ated. Actually, it has the ability to revolutionize and optimize the global infrastructure of the technologies connected with each other through internet. Motivated by these challenges, a blockchainbased IIoT architecture, which uses the blockchain as a distributed ledger to maintain records of all transactions in the IIoT networks. The proposed architecture separates the IIoT infrastructure into three layers: local IIoT networks, the blockchain overlay network, and the cloud infrastructure. To address the storage challenges in IIoT networks, a novel blockchain storage structure is proposed to store the blocks in a hierarchical manner: the majority of the blockchain is stored in the cloud to leverage its abundant storage capacity, while the most recent blocks are stored in the overlay network of the individual IIoT networks. As the blocks continue to be appended to the blockchain, the percentage of each part is maintained dynamically, depending mainly on two factors: the size of the current blockchain and the size of the storage (e.g., disk) provided on consensus nodes. To seamlessly connect these three layers, the design details of two connectors, the blockchain connector and the cloud connector, are also presented. The blockchain connector in an overlay network prepares blocks from transactions (data generated in IIoT networks), and the cloud connector addresses the blockchain synchronization issues between the overlay network and the clouds.

2 – RELATED WORKS

2.1 REGISTRATION/ LOGIN:

This module is responsible for the authentication purpose. It will contains the Id and password of the user.Every time the user try to login it verifies the correctnessof the details provided.And also for every new Registration it save the details for accessing the new user.

2.2 DATA ANALYSIS:

In this module, when the user try to user try to upload the the data it will check the data for its correctness .It allows only the valid data to upload.

2.3 HASHING MODULE:

For every data to be store in blockchain it has to be provided with a hash value. A Hashing establishes the validity of a piece of data by using a cryptographic algorithm. It is also a scheme for verifying that a piece of data has not been tampered with. blockchain is a linked list of transactions which contains data and a hash pointer to the previous block in the blockchain. A given blockchain functions based on the verification of a hash and digital signatures. Hashing is the process that the blockchain uses to confirm its state. Each transaction requires one or more digital signatures. Signatures ensure that the transaction is only made by the owner of the address. And that it is received by the correct recipient.

2.4 SMART CONTRACT:

This module is used to validate each and every block before linking it to chain. It verifies the hash value and the signature and random number(nonce). If these values are not correct it will drop the block.

2.5 CREATING BLOCKS :

This module is simply for linking the blocks to the chain which is obtained after all the verification process

3 -METHODOLOGY

Proposed Algorithm: Raft Consensus Algorithm

3.1 ADVANTAGES OF RCA

> Raft protocal can be easily understood whichwill be more useful to implement consensus on distributed system ,thus the understandingand implementing of this system will be hard.

>The consensus algorithm is easy to implement as it doesn't depend a single point failure but it's a distributed system.

> Since the raft consensus algorithm works in a distributed system even if the minority server fails, this system remains operational. For example, we have a 5 server, if 2 fails, the system will operate.

3.2 PROPOSED SYSTEM

The proposed is a blockchain system with credit-based consensus mechanism for IIoT. We propose a credit-based proof-of-work (PoW) mechanism for IoT devices, which can guarantee system security and transaction efficiency simultaneously. In order to protect sensitive data confidentiality, we design a data authority management method to regulate the access to sensor data. In addition, our system is built based on directed acyclic graph (DAG)-structured blockchains, which is more efficient than the satoshi-style blockchain in performance.

Blockchain features of transparency, which is an important characteristic in the finance field. However, it may become a drawback for some IIoT systems, where the collected sensitive data require the confidentiality and are only accessible by authorized ones. It is therefore important to design an access control scheme in a transparent system.

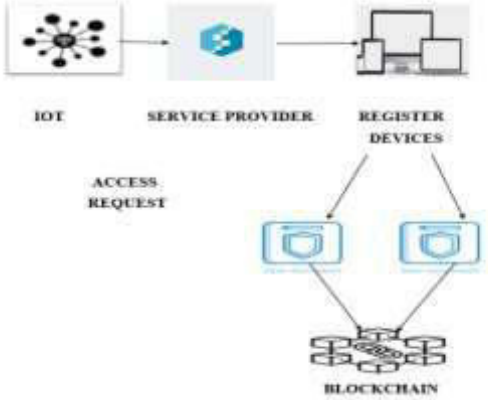

Fig. 1. Architecture Diagram

3.3 ADVANTAGES OF PROPOSED SYSTEM

✓ The design objective is to provide a secured, tamper free and efficient platform for the IoT users to safeguard their personal as well as industrial data.

Since the sensor data from the IoT devices are vulnerable to breaches it is

more important to protect them. For that the data are managed in blockchain.

- ✓ A webpage is created in such a way that the user will register if he/she is new user or else login into their accounts. The data from IoT sensor can be uploaded in CSV format and then it is converted into database.
- ✓ The uploaded data can be converted into graphs using EDA for easy visualization of data. These data will be stored in a block and given a hash value which contains the combination of digital signature and random number(nonce)
- ✓ The POW mining which is the consensus Algorithm will check the validity of the nonce and the signature if both are valid it will append it to the blockchain otherwise it will drop the block and record it in the transaction process.
  And this is the reason for immutability and security in block chain.

4 - RESULTS AND DISCUSSIONS

4.1 UPLOADING IOT DATA:

The system is presented to users in the form of web application. Users need to register an account on the web application. After registration is completed, users can upload their IIoT data. The system will validate the data and store uploaded file in the application .

Fig.2. Uploading Data

4.2 DATA ANALYSIS

Exploratory data analysis is a process of sifting through data in search of interesting information or patterns. Analysts' current tools for exploring data include database management systems, statistical analysis packages, data mining tools, visualization tools, and report generators. Since the exploration process seeks the unexpected in a data-driven manner, it is crucial that these tools are seamlessly integrated so analysts can flexibly select and compose tools to use at each stage of analysis. Few systems have integrated all these capabilities either architecturally or at the user interface level.

Visage's information-centric approach allows coordination among multiple application user interfaces. It uses an architecture that keeps track of the mapping of visual objects to information in shared databases.

EDA relies heavily on visualizations and graphical interpretations of data. While statistical modeling provides a "simple" low-dimensional representation of relationships between variables, they generally require advanced knowledge of statistical techniques and mathematical principles. Visualizations and graphs are typically much more interpretable and easy to generate, so you can rapidly explore many different aspects of a dataset. The ultimate goal is to generate simple summaries of the data that inform your question(s). It is not the final stop in the data science pipeline, but still an important one.

Graphs generated through EDA are distinct from final graphs. You will typically generate dozens, if not hundreds, of exploratory graphs in the course of analyzing a dataset. Of these graphs, you may end up publishing one or two in a final format. One purpose of EDA is to develop a personal understanding of the data, so all your code and graphs should be geared towards that purpose. Important details that you might add if you were to publish a graph2 are not necessary in an exploratory graph.

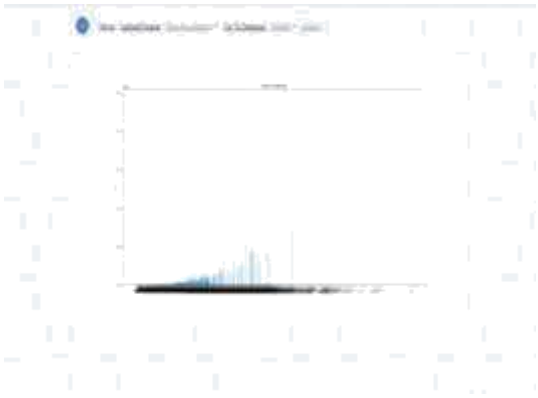

Fig .3. Area Vs Season Visualization

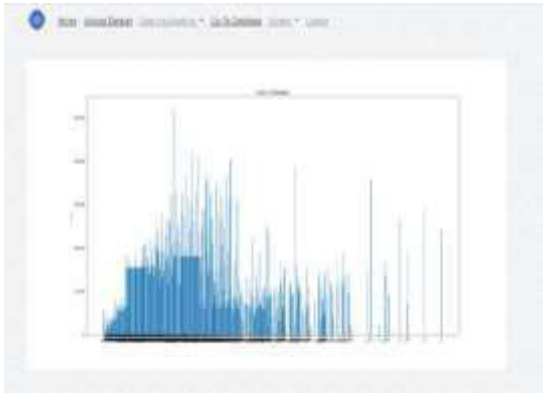

Fig .4. Cost Vs Distance Visualization

4.3 FORMATION AND MANAGEMENT OF BLOCKS

A blockchain is a digital concept to store data. This data comes in blocks, so imagine blocks of digital data. These blocks are chained together, and this makes their data immutable. When a block of data is chained to the other blocks, its data can never be changed again.

The IoT Data blocks in a blockchain are not chained based on block addresses. They are chained based on cryptographic hashes derived from the IoT Data data in the blocks. That is, each IoT Data block contains the hash of its previous IoT Data block to form a chain. Due to this structure, if the IoT Data data in a published block is changed due to a malicious attack, then its hash will be changed. This will cause the hashes of all subsequent IoT Data blocks to change. This mechanism can be used to detect unwanted modifications of published IoT Data blocks. This is also why there is the statement "published IoT Data blocks are not modifiable in a IoT Data blockchain".

A IoT Data transaction is a record of a IoT Data transfer often identified by its hash. IoT Data Transactions are signed and can be verified. A IoT Data block can contain multiple transactions. Citizen Transactions need to be valid otherwise they will not be included in a block. The validity refers to a transaction being properly signed and the signer has eligibility to make the transaction. The IoT Data nodes that check for transaction validity are called mining nodes.

IoT Data Blocks containing invalid transactions will not be added to the IoT Data blockchain.

To add a new block to a IoT Data blockchain, a mining node prepares a candidate block using IoT Data transactions and other required information to build a block, such as the hash of the previous block, as well as a difficulty parameter. At the IoT Data block approval stage, many valid blocks may be added to the chain. This happens when multiple received blocks point to the same previous block. Most mining nodes will be following a particular branch causing it to be longer than others. By committing the IoT Data block to the blockchain, the inquirers can check the summary, i.e.,the consensus made for the requested event. Further, the consensus can be accessed by any other IoT Data blockchain users for future use or consultancy. Future IoT Data events that are submitted to the blockchain should have a unique ID to distinguish them from the previously submitted IoT Data events.

Fig .5. Blockchain Report

5-CONCLUSION AND FUTURE ENHANCEMENTS

5.1 CONCLUSION

In this paper, we discuss the advantages of blockchainintegrated IoT solutions compared with traditional IoT structure. An IoT-Blockchain fusion model is proposed, which integrates the blockchain as well as distributed storage system. IoT devices interact with the blockchain directly or just send data to a gateway because of the limit power. To prove the transparency, traceability and security of blockchain-powered IoT applications.

We have discussed the new and emerging blockchain technology cybersecurity point. Blockchain technology mostly using and concentrating the finance area research work, as we know Bitcoin is a cryptocurrency which is based on blockchain technology. But in our article we try to introduce blockchain technology for internet of things to make secure data transmission between the internet connected devices. For this we have provide oview of blockchain technology, security issues on IoT environment and also discuss and propose blockchain is as a solution of IoT Security.

5.2 FUTURE ENHANCEMENTS

However, there are still some limitations in our systems, such as sensor data quality control, storage limitations. In future directions, we can explore sensor data quality control schemes in blockchain-based systems and some methods to store huge amounts of data.

6 –ACKNOWLEDGEMENT

We are very much indebted to **(Late) Hon'ble Colonel Dr. JEPPIAAR, M.A., B.L., Ph.D.,** Our Chairman and Managing Director **Dr. M. REGEENA JEPPIAAR, B. Tech., M.B.A., Ph.D.,** Our Principal **Dr. V.NATARAJAN., ME., Ph.D.,** to carry out the project here.

We would like to express our deep sense of gratitude to **Dr. J. AROKIA RENJIT M.E., Ph.D.,** our Head of the Department and also to **Mr.A.SUBASH CHANDAR M.E.,** our guide for giving valuable suggestions for making this project a grand success.

I also thank the teaching and non-teaching staff members of the department of **Computer Science and Engineering** for their constant support.

7- REFERENCES

[1] "Meng Shen" , "Xiangyun Tang" , "Liehuang Zhu" and "Mohsen Guizani" , **"Privacy -Preserving Support Vector Machine Training Over Blockchain- Based Iot Data in Smart Cities"** , IEEE Internet of Things Journal , Vol:6 Issue:5 ,2019.

[2] "Junqin Huang" , "Linghe Kong" , "Guihai Chen" , "Min- you Wu" , "Xue Liu" and "Peng Zeng" , **"Towards Secure Industrial Iot : Blockchain System with Credit- Based Consensus Mechanism"** , IEEE Transaction on Industrial Informatics , Vol:15 Issue:6 , 2019.

[3] "Oscar Novo" , **"Blockchain Meets Iot :An Architecture for Scalable Access Management in Iot"** , IEEE Internet of Things Journal , Vol:14 Issue:8, March 2018.

[4] "Lijing Zhou" , Licheng Wang" , " Yiru Sun" and " Pin Lv" , **"Beekeeper: A Blockchain -Based Iot System With Secure Strorage and Homomorphic Computation"** , IEEE Access Journal , Vol:14 Issue:8 ,August 2015.

[5] "Charbel El Kaed" , "Imran Khan" , "Andre Van Den Berg" , "Hicham Hossayni" and "Christophe Saint-Marcel" , **"SRE: Semantic Rules Engine for the Industrial Internet-Of-Things Gateways"** , IEEE Transactions on Industrial Informatics , Vol:14 Issue:2 , Feb 2018. **[6]** "Anam Sajid" , "Haider Abbas" and " Kashif Saleem" , **" Cloud-Assisted Iot-Based SCADA Systems Security : A Review of the State of the Art and Future Challenges"** , IEEE Access Journal , Vol:4 , 2016.

[7] " Dennis Miller" , **"Blockchain and the Internet of Things in the Industrial Sector"** ,IEEE IT professional Article , Vol:20 Issue:3 , May/June 2018.

[8] " Rongbo Zhu" , "Xue Zhang" , "Xiaozhu Liu" , "Wanneng Shu" , " Tengyue Mao" and " Brian Jalaian" , **"ERDT: Energy-Efficient Reliable Decision Transmission for Intelligent Cooperative Spectrum Sensing in Industrial Iot"** , IEEE Access Journal , Vol:3, 2015.

[9] "Saad Mubeen" , "Pavlos Nikolaidis" , "Alma Didic" , "Hongyu Pei-Breivold" , "Kristian Sandstrom" and "Moris Behnam" , **"Delay Mitigation in Offloaded Cloud Controllers in Industrial Iot"** , IEEE Access Journal ,Vol:5, 2017.

[10] "Li Da Xu" , "Wu He" and " Shancang Li" , **"Internet of Things in Industries : A Survey"** , IEEE Transactions on Industrial Informatics , Vol:10 Issue:4 , Nov 2014.

[11] "Wattana Viriyasitavat" , " Li Da Xu" , "Zhuming Bi" and " Danupol Hoonsopon" , **"Blockchain Technology for Applications in Internet of Things- Mapping From System Design Perspective"** , IEEE Internet of Things Journal , Vol:6 Issue:5 , 2019.

[12] " J.Indumathi" , "Achyut Shankar" , "Muhammad Rukunuddin Ghalib" , "J.Gitanjali" , " Qiaozhi Hua" and "Xin Qi" , **"Block Chain Based Internet of Medical Things for Uninterrupted , Ubiquitous , User-Friendly , Unflappable , Unblemished , Unlimited Health Care Services (BC IoMT U6 HCS)"** , IEEE Access Journal , Vol:8 , 2020.

[13] "Xiaolin Fu" , "Hong Wang" and " Zhijie Wang" , **" Research on Block-Chain – Based Intelligent Transaction and Collaborative Scheduling Strategies for Large Grid"** , IEEE Access Journal , Vol:8 , 2020.

[14] "Sahib Khan" , " Muhammad Abeer Irfan" , "Arslan Arif" , "Arslan Ali" , "Zain Anwer Memon" and "Aleem Khaliq" , **"Reversible-Enhanced Stego Block Chaining Image Steganography : A Highly Efficient Data Hiding Technique"** , IEEE Journal , Vol:43 Issue:2 , 2020.

[15] "Yang Huang" , " Xin Guan" , " Hongyang Chen" , " Yi Liang" , "Shanshan Yuan" and "Tomoaki Ohtsuki" , **" Risk Assessment of Private Information Inferences for Motion Sensor Embedded Iot Devices"** , IEEE Transaction on Emerging Topics in Computational Intelligence , Vol:4 Issue:3 , 2020.

[16] "Jin Hyeong Jeon" , "Ki-Hyung Kim" and " Jai-Hoon Kim" **, " Block Chain Based data Security enhanced Iot server platform"** , IEEE Conference paper, 2018.

[17] "Chan Hyeok Lee" and "Ki-Hyung Kim" , **"Implementation of Iot system using block chain with authentication and data protection"** , IEEE International Conference on Information Networking , 2018.

[18] "Misbah Anwer" , "Afshan Saad" and " Ayesha Ashfaque" , **"Security of Iot using Block Chain : A Review"** , IEEE International Conference on Information Science and Communication Technology , 2020.

[19] "Bruno Cruz" , "Silvana Gomez-Meire" , "David Ruano-Ordas" , " Helge Janicke" , "Iryna Yevesyeva" and "Jose R.Mendez" , **"A Practical Approach to Protect Iot Devices against Attacks and Compile Security Incident Datasets"** , Hindawi Scientific Programming , Vol 2019 , Article ID 9067512 , 11 pages.

[20] " Tianqi Zhou" , "Jian Shen" , " Sai Ji" , " Yougjun Ren" and " Leiming Yan" , **"Secure and Intelligent Energy Data Management Scheme for Smart Iot Devices"** , Hindawi Wireless Communication and Mobile Computing , Volume 2020 , Article ID 8842885 , 11 pages.