International Journal for Innovative Engineering and Management Research

PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL

www.ijiemr.org

COPY RIGHT

ELSEVIER

SSRN

IJIEMR Transactions, online available on 13 Aug 2023. Link :http://www.ijiemr.org/downloads.php?vol=Volume-12&issue=Issue 08

10.48047/IJIEMR/V12/ISSUE 08/31

Title **Credit-Based Blockchain Integration for Enhanced Security and Efficiency in Industrial IoT**

Volume 12, ISSUE 01, Pages: 201-206

Paper Authors **Dr.Madhavi Pingili, Mrs.K.Sushma, Mrs.C.Madhuri**

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Credit-Based Blockchain Integration for Enhanced Security and Efficiency in Industrial IoT

Dr.Madhavi Pingili, Professor & HoD, Department of Information Technology, CMR Engineering College, Hyderabad, Telangana, **E-Mail-id :** madhavipingili2@gmail.com
Mrs.K.Sushma, Asst. Professor, Department of Information Technology, CMR Engineering College, Hyderabad, Telangana
Mrs.C.Madhuri, Asst. Professor, Department of Information Technology, CMR Engineering College, Hyderabad, Telangana

ABSTRACT
The Industrial Internet of Things (IIoT) plays a crucial role in the context of Industry 4.0, where the goal is to establish a versatile, scalable, and secure IIoT framework that can be adopted across various industries. However, current IIoT systems face vulnerabilities in terms of potential single points of failure and susceptibility to malicious attacks, making it challenging to ensure consistent and reliable services. Recognizing the reliability and security benefits of blockchain technology, there has been growing interest in integrating blockchain with the Internet of Things (IoT). Yet, it's important to note that blockchains come with their own set of limitations, such as their high energy consumption and limited transaction processing speed. These characteristics make traditional blockchains less suitable for IoT devices that have constraints on power consumption. To address these issues, we introduce a blockchain system that utilizes a credit-based consensus mechanism specifically designed for IIoT. Our solution involves implementing a credit-based proof-of-work (PoW) mechanism tailored for IoT devices. This innovative approach serves to ensure both the security of the system and the efficiency of transactions simultaneously. In order to maintain the confidentiality of sensitive data, we have developed a data authority management system that governs access to sensor data. This mechanism helps regulate who can access the data, adding an extra layer of protection. Additionally, our system is constructed based on directed acyclic graph (DAG) structured blockchains, which prove to be more efficient in terms of performance when compared to the conventional Satoshi-style blockchain architecture. Our comprehensive evaluation and analysis demonstrate the effectiveness of the credit-based PoW mechanism and the data access control in enhancing the security and efficiency of IIoT applications.
Keywords: IIoT security, Blockchain integration, Credit-based consensus, Data confidentiality, DAG-structured blockchain.

1. INTRODUCTION

THE integration of IoT and industry is important modus to promote automation and informatization of industry. IIoT helps cut down on errors, reduce costs, improve efficiency and enhance safety in manufacturing and industrial processes, which has a great chance to make industry field a higher level of integrity, availability and scalability. However, security attacks and failures could cause great trouble against the global IoT network [1], which may outweigh any of its benefits. For example, the central data center is vulnerable to single point failure and malicious attacks such as DDoS, Sybil attack [2], which cannot guarantee services availability. In addition, sensor data stored in a data center are at the risk of disclosure. Also, data interception may occur in communications between IoT devices, which cannot promise the credibility's of collected data. In recent years, with the emergence of blockchain, the idea of combining blockchain and IoT has gained considerable interest [3]–[5]. By leveraging the features of tamper-proof and decentralized consensus mechanism in blockchain, we have the chance to solve the aforementioned security issues in IIoT systems.

2. RELATED WORK

There are some existing researches on this topic, for example, O. Novo [4] proposes an access control system based on the blockchain technology to manage IoT devices. However, the system is not fully built on a distributed architecture because of the usage of the central management hub. Once the management hub is failed or attacked, IoT devices connected to it become unavailable. Z. Li et al. [6] exploit the consortium blockchain technology to propose a secure energy trading system. But they do not consider privacy issues such as the sensitive data disclosure risk, and thus it cannot guarantee sensitive data confidentiality. [7]The aforementioned systems all adopt chain-structured blockchains in IoT systems, which are overloaded for power-constrained IoT devices. Z. Xiong et al. [8] introduce edge computing for mobile blockchain applications and present a Stackelberg game model for efficient edge resource management for mobile blockchain [9]. They reduce computational requirements of mobile devices by leveraging edge computing. [10] In addition, there are some other challenges that also brought in the meantime when introducing the novel design of blockchain into IIoT systems.

We summarize three folds main challenges:

1) The trade-off between efficiency and security: We know that consensus algorithms in blockchain can effectively help to defend malicious attacks, and PoW is the most widely used consensus algorithm, which forces nodes to run high complexity hash algorithms to verify transactions. However, it is overloaded for power-constrained IoT devices. While eliminating the PoW mechanism can potentially improve efficiency of transactions, it causes system security issues. As a result, how to make the trade-off between security and efficiency in consensus mechanisms is the first challenge of this work.

2) The coexistence of transparency and privacy: 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.

3) The conflicts between high concurrency and low throughput: IoT devices report data continuously in IIoT systems, leading to a high concurrency. Unfortunately, complex cryptographic based security mechanisms largely limit the throughput of blockchain. Besides, the synchronous consensus model in chain-structured blockchains cannot make full use of bandwidth in IIoT systems. So how to improve the throughput of blockchain to satisfy the need of frequent transactions in IIoT systems becomes the third challenge.

To address these challenges, we propose a blockchain system with credit-based consensus mechanism for IIoT. In order to decrease the power-consumption in consensus mechanism, we present a self-adaptive PoW algorithm for power-constrained IoT devices. It can adjust the difficulty of PoW based on nodes' behaviour, which can decrease the difficulty for honest nodes while increasing for malicious nodes. We also present an access control scheme based on the symmetric cryptography in the transparent blockchain system, which provides a flexible data authority management method for users. Our system infrastructure is built based on the DAG structured blockchain, which improves the system throughput by leveraging its asynchronous consensus model.

3. PROPOSED SYSTEM

A blockchain is a growing list of information, called blocks, which are linked using cryptography. Each block contains a special hash function which is related to the previous block, a timestamp to securely keep track of the creation and modification time of a document, and transaction data. By design, a blockchain is resistant to change in the data. For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively complying to a protocol for inter-node communication and verifying new blocks. Once recorded, the data in any given block cannot be changed without alteration of all related blocks, which requires unanimity of the majority of the network. Although the information is not completely unchangeable, blockchain design may be considered secure and depict a distributed computing system with high fault tolerance.

A blockchain is a decentralized, distributed and a public digital ledger that is used to record transactions across many devices so that any involved record cannot be changed easily, without modifying all subsequent blocks. This allows the participants to verify transactions independently. A blockchain database is managed separately using a peer-topeer network and a distributed time stamping server. They are validated by mass collaboration powered by collective self-interests. Such a design facilitates sturdy workflow where participants' uncertainty regarding data security is marginal. The use of a blockchain confirms that each unit of value was transferred only once, solving the long-established problem, that is the double spending problem.

Blocks hold batches of valid transactions that are hashed and encoded into a cryptographic hash tree. Each block includes the cryptographic hash value of the prior block in the blockchain, linking the two blocks. This forms a chain of blocks. This iterative process confirms the integrity of the previous block, all the way back to the root block.

3.1 SYSTEM STUDY

FEASIBILITY STUDY

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

Three key considerations involved in the feasibility analysis are

- ECONOMICAL FEASIBILITY
- TECHNICAL FEASIBILITY
- SOCIAL FEASIBILITY

ECONOMICAL FEASIBILITY

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

TECHNICAL FEASIBILITY

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

SOCIAL FEASIBILITY

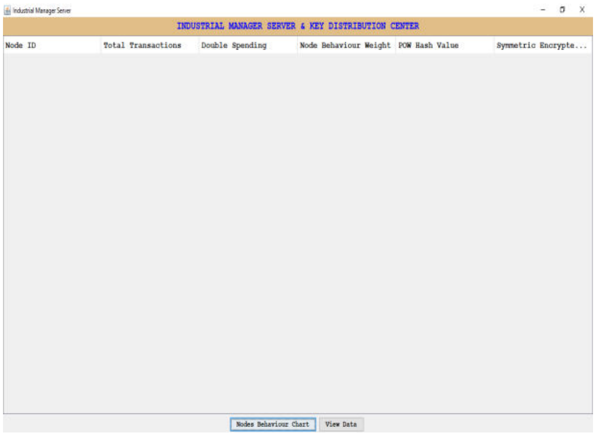
The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

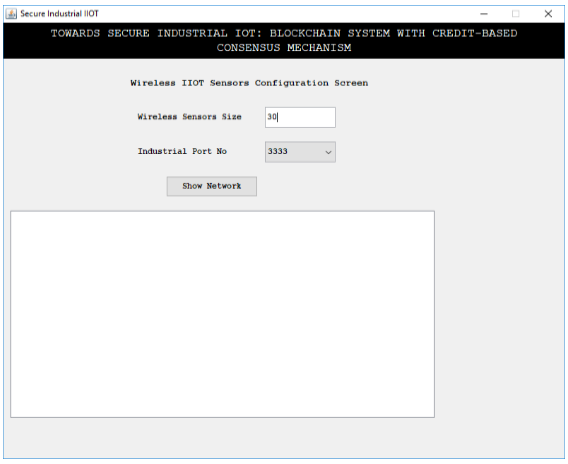
the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system

4. RESULTS

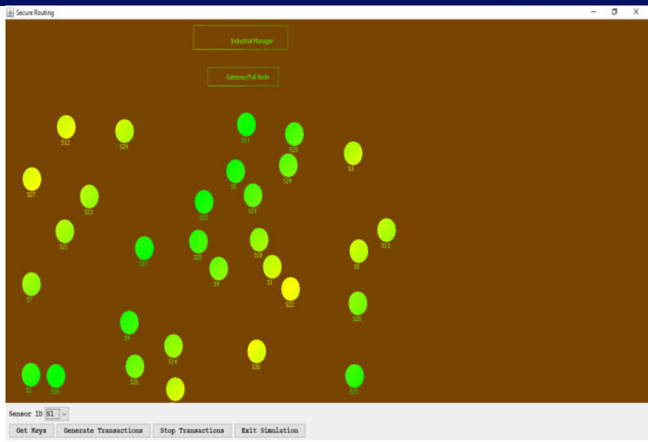
First double click on 'run.bat' file from 'Industrial Manager' to get below screen and let it run



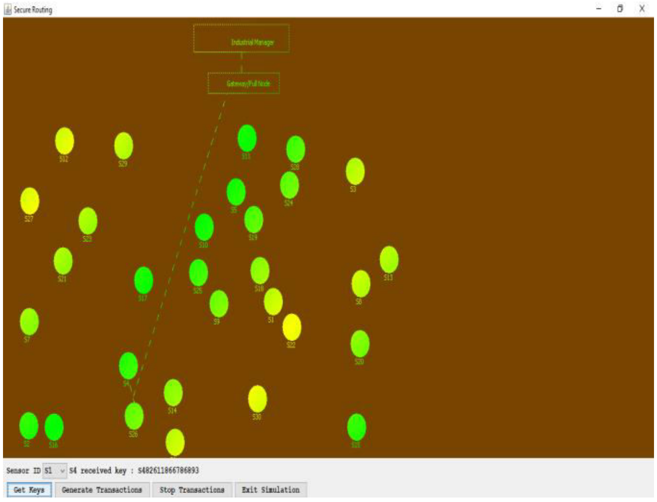
In above screen we can see each transaction details from each node and then monitor node to detect its normal or abnormal behaviour'. Now double click on 'run.bat' file from 'Wireless_Sensors' folder to get below screen.



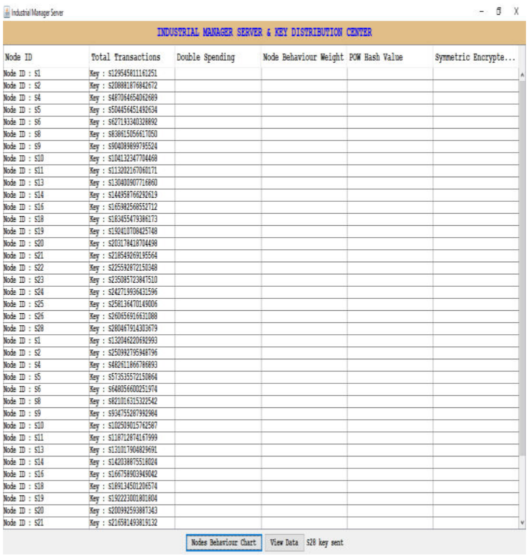
In above screen enter number of sensors and then click on 'Show Network' screen to get below screen



In above screen click on 'Get Keys' button to allow all sensors to obtain keys from gateways

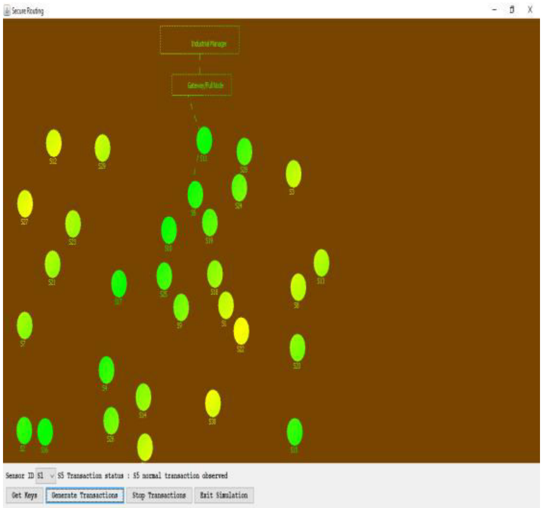


In above screen we can see each node is getting keys from gateway and this keys details we can see at 'manager screen' also

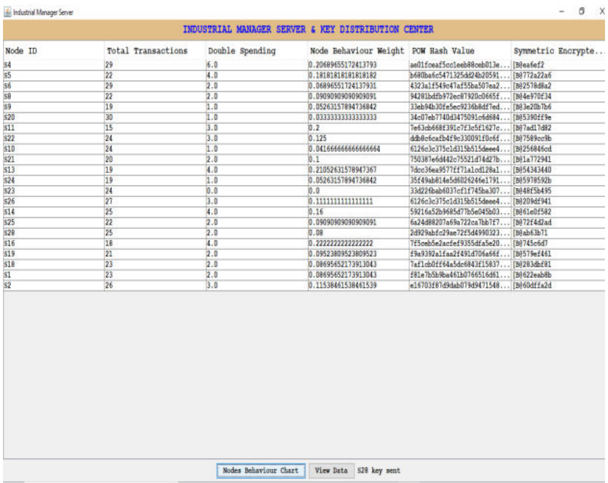


International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Now go to simulation screen and click on 'Generate Transactions' button to select random nodes and to send random transaction data to gateway. Due to random data sometime nodes will report same transaction then POW detects it as abnormal transaction. This random data and continuous data sending concept just I am using to make some node to report same data and POW can record it. After some time you can click on 'Stop Transaction' to stop it.



In above screen we can see transaction sending to gateway for processing. Now we can see each transaction process status at below manager screen

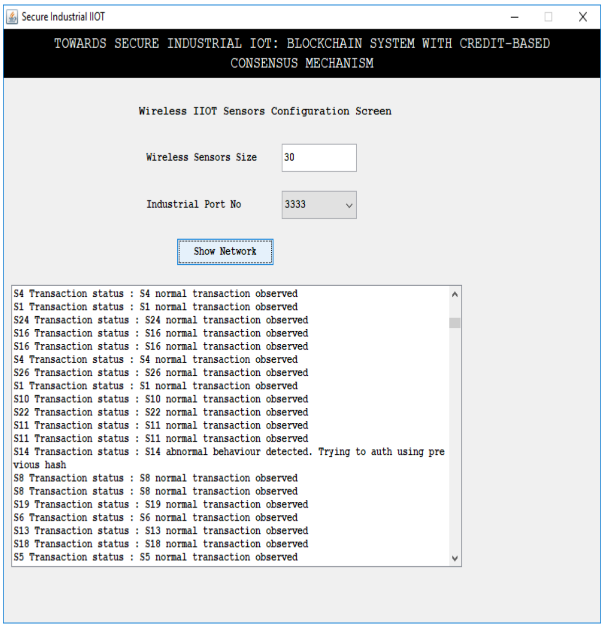

Industrial Manager Server

INDUSTRIAL MANAGER SERVER & KEY DISTRIBUTION CENTER

Node ID	Total Transactions	Double Spending	Node Behaviour Weight	POW Hash Value	Symmetric Encrypte...
S4	29	6.0	0.20689655172413793	ae01fceaf5cc1eeb88ceb013e...	[B@ea6ef2
S5	22	4.0	0.18181818181818182	b680ba6c5471325dd24b20591...	[B@772a22a6
S6	29	2.0	0.06896551724137931	4323a1f549c47af55ba507ea2...	[B@2578d8a2
S8	22	2.0	0.09090909090909091	94281bdfb972ec87920c0665f...	[B@4e970f34
S9	19	1.0	0.05263157894736842	33eb94b30fe5ec9236b8df7ed...	[B@3e20b7b6
S20	30	1.0	0.03333333333333333	34c07eb7740d3475091c6d684...	[B@5390ff9e
S11	15	3.0	0.2	7e63cb668f391c7f3c5f1627c...	[B@7ad17d82
S22	24	3.0	0.125	ddb8c6cafb4f9c330091f0c6f...	[B@7589cc9b
S10	24	1.0	0.041666666666666664	6126c3c375c1d315b515deee4...	[B@256846cd
S21	20	2.0	0.1	750387e6d442c75521d74d27b...	[B@1a772941
S13	19	4.0	0.21052631578947367	7dcc36ea9577ff71a1cd128a1...	[B@54343440
S24	19	1.0	0.05263157894736842	35f49ab814e5d6026246e1791...	[B@5978592b
S23	24	0.0	0.0	33d226bab6037cf1f745ba307...	[B@48f5b495
S26	27	3.0	0.1111111111111111	6126c3c375c1d315b515deee4...	[B@209df941
S14	25	4.0	0.16	59216a52b9685d77b5e045b03...	[B@61e0f582
S25	22	2.0	0.09090909090909091	6a24d88207a69a722ca7bb7f7...	[B@72f4d2ad
S28	25	2.0	0.08	2d929abfc29ae72f5d4990323...	[B@ab63b71
S16	18	4.0	0.2222222222222222	7f5ceb5e2acfef9355dfa5e20...	[B@745c6d7
S19	21	2.0	0.09523809523809523	f9a9392a1faa2f491d706a66f...	[B@579ef461
S18	23	2.0	0.08695652173913043	7af1cb0ff64a5dc6843f15837...	[B@283dbf81
S1	23	2.0	0.08695652173913043	f81e7b5b9ba461b0766516d61...	[B@622eab8b
S2	26	3.0	0.11538461538461539	e16703f87d9dab079d9471548...	[B@60dffa2d

Nodes Behaviour Chart | View Data | S28 key sent

In above screen each node data report is recording and their hash values checking to collect their behaviour, if they send old transaction data hash value then it will be consider as 'abnormal behaviour'. In above screen I am showing all nodes sending abnormal attack data and in real time this will not happen. Just to show the concept of old hash values I sent random continuous request and all nodes send repeated data and becomes in abnormal behaviour. From above screen we can see first nodes sent total 29 transactions and out of that 6 transaction report old hash values then it will detect as abnormal behaviour. If it reports 1 or 2 times then it can be manage and consider as normal behaviour. Now in above screen click on 'Node Behaviour Chart' button to see which nodes report same old hash value more no of times.



In above screen also we can see normal or abnormal behaviour.

5. CONCLUSION

We proposed 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 designed a data authority management method to regulate the access to sensor data. In addition, our system is built based on directed acyclic graph -structured blockchains, which is more efficient than the Satoshi-style blockchain in

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

performance. Extensive evaluation and analysis results demonstrate that credit-based PoW mechanism and data access control are secure and efficient in IIoT.

REFERENCES

[1] Y. Lu and L. D. Xu, "Internet of things (iot) cybersecurity research: A review of current research topics," IEEE Internet of Things Journal, pp. 1–1, 2018.

[2] H. Yu, P. B. Gibbons, M. Kaminsky, and F. Xiao, "Sybillimit: A near-optimal social network defense against sybil attacks," in IEEE Symposium on Security and Privacy (S&P), May 2008, pp. 3–17.

[3] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for iot security and privacy: The case study of a smart home," in IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), March 2017, pp. 618–623.

[4] O. Novo, "Blockchain meets iot: An architecture for scalable access management in iot," IEEE Internet of Things Journal, vol. 5, no. 2, pp. 1184–1195, April 2018.

[5] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchainbased decentralized trust management in vehicular networks," IEEE Internet of Things Journal, pp. 1–1, 2018.

[6] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium blockchain for secure energy trading in industrial internet of things," IEEE Transactions on Industrial Informatics, vol. 14, no. 8, pp. 3690– 3700, Aug 2018.

[7] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, "When mobile blockchain meets edge computing," IEEE Communications Magazine, vol. 56, no. 8, pp. 33–39, August 2018.

[8] M. Swan, Blockchain: Blueprint for a new economy. " O'Reilly Media, Inc.", 2015.

[9] K. Karlsson, W. Jiang, S. Wicker, D. Adams, E. Ma, R. van Renesse, and H. Weatherspoon, "Vegvisir: A partition-tolerant blockchain for the internet-of-things," in IEEE 38th International Conference on Distributed Computing Systems (ICDCS), July 2018, pp. 1150–1158.

[10] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in Big Data (BigData Congress), 2017 IEEE International Congress on. IEEE, 2017, pp. 557–564.