Security Enhancement of IIOT with Permissioned Blockchain and Cloud Computing

Prof. KavyaShree M K, Assistant Professor of the Department of Electronics and Communication Engineering, JSS Science and Technology University, Mysuru, India. kavyashreemk@sjce.ac.in

Zainab Mudassir, *Department of Computer Science and Engineering Sri Jayachamrajendra College of Engineering* Mysore, India. zainabmudassir@gmail.com

***Abstract*—Blockchain has proven itself to be of value in various fields of technology. In today's world every kind of technology implementation requires security, the research to make it better is constantly taking place. With such a requirement, blockchain has started to make a huge difference in the way security protocols are implemented. The data is stored in the form of blocks where in every one of them transactions are stored. Every block added connects itself to the existing blocks in a secure manner such that it is resistant to attacks and tamper. With emerging advances in IIoT, the requirement for better security has increased, and hence a permissioned blockchain security solution for IIoT has been proposed. In this paper, an additionally secure approach using cloud computing is used where the private keys provided to the user are broken down and stored on cloud is proposed.**

***Index Terms*—Permissioned Blockchain, IIoT, Security, IoT.**

I. INTRODUCTION

One of the most popular terms in the industry of science and technology currently is Internet of Things (IoT), making its way into our daily lives. It focuses on controlling devices across the globe easily and adding more features to a device leading to the advancements in its functioning. With mini- mal to none human interventions, these devices are either interconnected or communicate through wireless network to transfer necessary data. The possibilities are endless. 'Thing' here technically means any device fitted with sensors and has the ability to collect and transfer data over a wireless network. What we have discussed over here is an application of IIoT (Industrial Internet of Things). The difference between IoT and IIoT is the situation and service that they are used in. On a consumer-level, IoT is preferred. However, IIoT is used in places where the tasks are relatively critical. There can be a few differences found when factors like connectivity, data latency etc. are compared [9]. However, like every advanced technology, IoT also comes with risks and concerns that need to be addressed. In this paper we are addressing the issue of security by using another emerging technology, Blockchain. Blockchain is a distributed ledger technology and can be of use to the security challenges as it possesses the property of decentralization, which makes sure all of the data, credentials etc. are not at one place to be hampered. Many approaches towards blockchain have been introduced, the one we have discussed in this paper is permissioned blockchain. Our aim is to increase the extent of security in IIoT applications, hence, we will be introducing the storage of keys on a cloud platform.

II. RELATED WORK

Several authors have addressed this security issue and proposed solutions with blockchain technology. The authors in [1] have used an energy saving approach along with public blockchain, Ethereum, and aimed at secure data sharing. Ethereum has been used to maintain a shared ledger that cannot be tampered. The authors in [2] has proposed a solution in which the blockchain uses PoW credit based algorithm for less powered IIoT devices. A DAG-structure blockchain is utilized in [2] for reduction in power consumption as the IoT devices used in industries are characterized by heavy power consumption. This structure guarantees security and scalability as well. Another type of blockchain that can be used for secure data transfer is the fabric blockchain which is used in [3]. The authors here have used transaction certificates, without which the transactions are invalid, and authentication of newly added blocks takes place as an approach for security. Further the use of hash algorithm and public/private key pairs is used to ensure security. Another proposed solution for IIoT security using blockchain is in [4] where the authors have used Ethereum like in [1], except here Attribute-based encryption (ABE) for detailed access control. This solution was mainly for supply chain industry data sharing. Every node needs to be assigned a role so that role-based access control is provided. These role- based accesses are defined in the smart contract. The authors have discussed how to tackle a single point of failure attack. Another proposed solution in [5] uses private

 DOI : 10.35291/2454-9150.2021.0409

blockchain to ensure security in smart factories. It is a five layered architecture, in which verification mechanism, whitelisting, blacklisting, time-stamping etc are used to make sure the data input is not tampered, erroneous or malicious. In [6], one consensus algorithm is topped by another. The existing con- sensus method is revised by application of another trust-based mechanism. This approach secures the medium by certifying the users before communication occurs. The mechanism works in such a way that reputations are assigned to every node and are increased or decreased depending on its capability to add a node to the existing chain of blocks in a given time.

Year	Authors	Proposed Solution	IIoT Security Problem Addressed	Blockchain Approach
2019	Liu et al. [1]	A blockchain enabled energy efficient and secure data collection and sharing scheme	Secure data sharing	Ethereum
	Huang et al. [2]	PoW credit based consensus algorithm	Efficient access control scheme	DAGstructured blockchain
	Liang et al. [3]	A dynamic secret sharing mechanism in data transmission technique using power blockchain	Secure data transmission	Fabric
	Wen et al. [4]	Secure data sharing by combining supply chain, blockchain, and IIoT	Secure data sharing	Ethereum
	Wan et al. [5]	Improve processing power, security, and privacy of IIoT	Secure data sharing and communication	Private
2020	Wang et al. [6]	Reputation scheme to certify the miners are trustworthy and make the communication secure	Trust scheme for IIoT	Ethereum
	Lu et al. [7]	Secure data sharing architecture using blockchain	Secure data sharing	Permissioned
	Shen et al. [8]	A secure device authentication mechanism	Secure device and data communication	Consortium

Fig. 1. Comparison of Related work

Hence, only nodes with a good reputation can participate and considered normal, and a trust-based communication is achieved. Like in this paper, a permissioned blockchain has been utilized in [7] for secure IIoT data sharing. Data is retrieved upon request only from the local providers where it is stored. It can be requested only by permissioned parties, which ensures security. The next paper referred proposes the authentication by using a consortium blockchain with an extended version of IBS (Identity-based Signature) which does not require a public key certificate [8]. Third party involvement is non-existent as consortium blockchain is used. IBS further reduces the overhead caused by digital certificates issuing. Device authentication and secure data communication is achieved through blockchain writing process. Authors in [9] have made a good progress with respect to security in IIoT us- ing blockchain, but this time, permissioned blockchain. There are 3 types of blockchain; private, consortium/permissioned, and public. Depending on the area of usage, the appropriate one is chosen. In this case, permissioned blockchain is used, as it ensures more security than the other types. As the name suggests, permissioned here refers to the nodes that are allowed to make transactions after authorization and authen- tication. There are a set of nodes called the consensus nodes which are responsible for taking decisions of authorization and authentication, which transactions will be successful or not etc. The main technology used here is blockchain which is basically a well-protected distributed ledger. It does not require the intervention of a mediator and is capable of connecting several computers on a peer-to-peer (P2P) network. There has been a slew of blockchain implementations that have shown a slew of new uses for the technology [10]. This technology however loses the competition when it comes to scalability. Therefore, the increasing devices in the network may pose a challenge in future blockchain applications. This in turn effects the cost factor during application. A permissioned blockchain, on the other hand, helps in overcoming most of the shortcomings mentioned above. Since permissioned blockchain distinguishes itself by possessing better security features, such as letting only verified users participate in the chain, the authors in [10] have chosen this. The following table well depicts how a permissioned blockchain distinguishes itself from a regular blockchain technology by being more vigilant around who participates in the chain network. When security is our main goal, and it should be, permissioned blockchain is preferred. It performs better in areas like identity management, limiting access, validation of transactions etc. Whereas a public blockchain is vulnerable to entry of any user without verification or authentication which can pose a serious threat to the network. This is also the reason why we have implemented this paper using the former type of blockchain.

Features	Permissioned Blockchain	Public Blockchain
Identity Management	Yes	No
Limited Action	Yes	No
Anonymity	No	Yes
Restricted Transactions	Yes	No
Transaction Validation [26]	Limited	Open
Consensus Algorithms	PoS, BFT, PBFT	PoW, PoA, PoS, PoET
Platforms [3]	Hyperledger Fabric, Quorum, Corda	Bitcoin, Ethereum, Litecoin

Fig. 2. Differences between Permissioned and Regular Blockchain Technolo- gies

III. PROPOSED WORK

A permissioned blockchain is made up of numerous or- ganizations. As discussed earlier, permissioned blockchain is very advantageous while applying blockchain to an application where security is very important. In IIoT, security is vital as the industry's data cannot be risked to get tampered. Each group has its own members and only permits them to participate if they have been given permission. Members are assigned certain roles by the organizations so that they can undertake network transactions. The blockchain is made up of two or more organizations that work together to store the information of every transaction. Not only does permissioned blockchain carry all the benefits of a regular blockchain like decentralization but also additional

 DOI : 10.35291/2454-9150.2021.0409

advantages which protects the participants of the organizations. Hence, a permissioned blockchain could be a good fit for the IIoT network.

A. Permissioned Blockchain for IIoT

Permissioned blockchains enable IIoT machine connection by providing a quicker, more protected and confidential net- work. This is the reason why a permissioned blockchain is chosen to secure the IIoT application and their users. It is achieved by allowing only the trusted users to be a part of the network formed by authorized devices communicating with each other. Any device that is not included in this network is not trusted and is treated as malicious.

A Certificate Authority (CA) is one of the blockchain's components, and this is the component that makes sure only authorized users can join the network and communicate. It achieves this by granting digital certificates to them so that they can be recognized and authenticated. Like any other cryptography component, this component also generates public and private keys in order to recognize these participants. After this, the authority component has a set of rules which define the roles of each of the participants. These members have the access to perform any transactions because of the roles defined in the smart contract. When a new member tries to join and make any kind of transaction the consensus nodes have to allow or disallow it. If they allow it, it is added to the chain network and it becomes a trusted node in all the other nodes' ledgers. The next time it tries to make a transaction, the consensus nodes are not involved as it has already been verified by them.

B. Working

As discussed in the previous section about the authority component, it functions like a generic CA, and the only differ- ence here is that it is incorporated with the blockchain tech- nology in order to achieve permissioned blockchain method which ensures security. Thanks to permissioned blockchain's features, it does so while avoiding the traditional CA's security flaws. The CA creates certificates that verify the identities of the blockchain's organizational members. It creates two types of keys: public and private, which are used to complete transactions. The identity fills in the required information for the certificate and key pair to be generated. The key pairs and certificates are securely saved on the blockchain, as well as on the chain network's smart contract. The smart contract stores the state of the certificates for further processing. Following the generation of certificates for the identities, the smart contract establishes access control mechanisms for the various identities based on the certificates' stored information. The identities are given a role-based access control mechanism. As a result, the role-based access control system assures that identities undertake transactions in accordance with their responsibilities, and those transactions are only carried out if their roles permit it. When a member of the organization initiates a transaction, it is signed using the CA's public key. A small number of consensus nodes confirm that the transaction fulfils its purpose, authenticates it, and verifies that the transaction's public key matches the CA. Following the transaction, all network participants are alerted of the addition of the new block to the network, and organizations are required to update their ledgers in order to maintain consistency. If the consensus nodes reject a transaction, it will not be carried out, but the data will be preserved on the blockchain, even if the ledger's state will not be altered. The information about unapproved transactions will be useful in determining what happened across the network and who attempted to initiate a transaction but was denied. This provides an additional layer of protection to the network and aids in the tracking of transaction data. An additional step to ensure security is added where the keys provided by the authority are split and stored on a cloud platform. Only authorized personnel can access these split keys and rearrange them to form the key and use it. In this approach, two additional levels of security are added. The splitting of the keys ensures that even if somehow an attacker gets access to the storage of these keys he will be unable to rearrange them in the right order and use them.

C. Further Discussion

The proposed permissioned blockchain-enabled IIoT assures that the security of IIoT is improved and enhanced in terms of safe device connection, server, data exchange, and access control mechanisms. After only allowed players join the network, they have limited access to it, and an access control mechanism ensures that transactions are only executed in a limited number of ways.

The Industrial Internet of Things (IIoT) connects many in- dustrial equipment that collaborate and generate a vast amount of data, including both useful and sensitive information. It gathers and analyses information in order to provide new insights. As a result, securing the communication medium between IIoT devices and protecting sensitive data is critical, as compromising the IIoT network will have major conse- quences and will have a significant impact on the industry and its infrastructures. The use of a permissioned blockchain, which allows only selected and authorized parties to join the network and conduct transactions, would undoubtedly improve IIoT security. Because an organisation may define the responsibilities of the members using smart contracts and restrict their access to the network, a permissioned blockchain is well suited for a secure IIoT network of devices. The roles also specify which members have access to the network's data and can

 DOI : 10.35291/2454-9150.2021.0409

perform various write operations. Consensus nodes are critical to the network's success.

IV. IMPLEMENTATION

For the implementation of iiot, we have considered a smart card application which holds an RFID for recognition. Every swipe is considered as a transaction request. Further, these requests are approved or rejected based on the consensus algorithm carried out by the blockchain server. Here, the macid of the client's machine is compared with the database which contains the details of all the previously approved nodes, if it matches, the transactions are accepted, if it does not match then the authentication of the requesting client is carried out. The following steps are the flow of the system from client registration to accepting a transaction request.

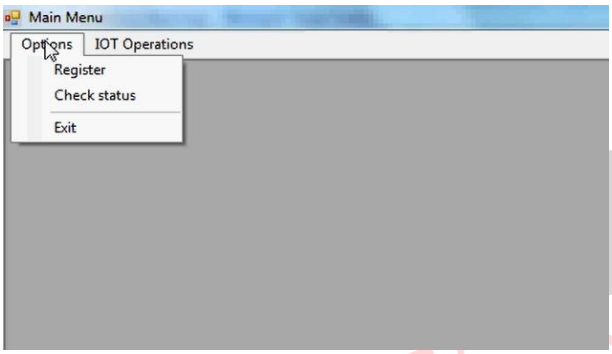

Fig. 3. Options in Client Application

A user accesses the client application from their device and authentication takes place. When they are accessing for the first time, they need to register.

The client application fetches the user's macid and checks in the database if it is authenticated or not and depending on that the next steps of registration or retrieval of information are carried out.

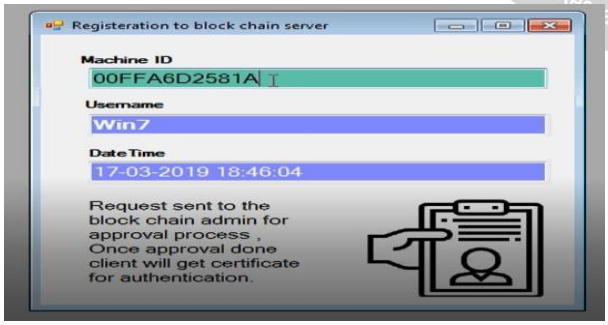

Fig. 4. Fetching Client Device Details

If it is a new user then the client has to check for status of approval or rejection by clicking on the check status option in Fig 3. If it is pending, the following screen appears. On the blockchain server side, these requests for registration or transactions are received as showing in Fig 6. If it is a request for registration, the screen is Fig 7 appears and gives the options to approve, reject or refresh the entries. Once the approval is done, the check status option on the client side will show a success pop-up. Next, in Fig 6, if Blockchain server management option is chosen, the following screen appears with transactions made by authenticated users with the rfid. If the IoT options in Fig 3 is chosen the following screen appears. Further, when all the processes here are carried out, the success of that process is shown next to that step as in Fig 9 along with all the transactions of different authenticated users. If anyone tries to change the data of the registered user,

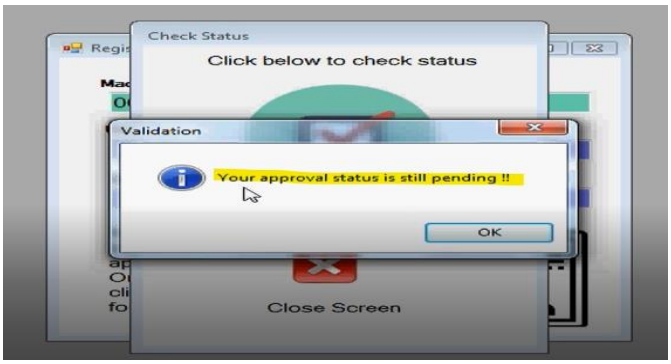

Fig. 5. Pending Approval

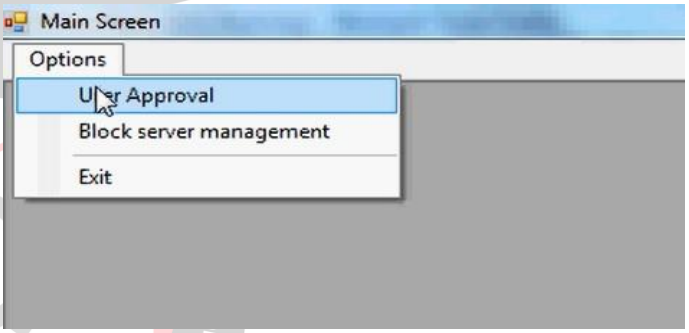

Fig. 6. Blockchain

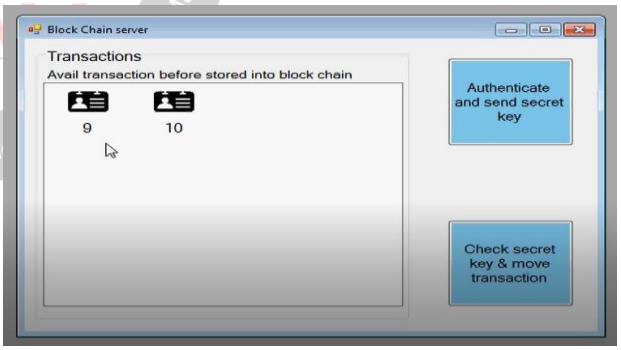

Fig. 7. Transactions

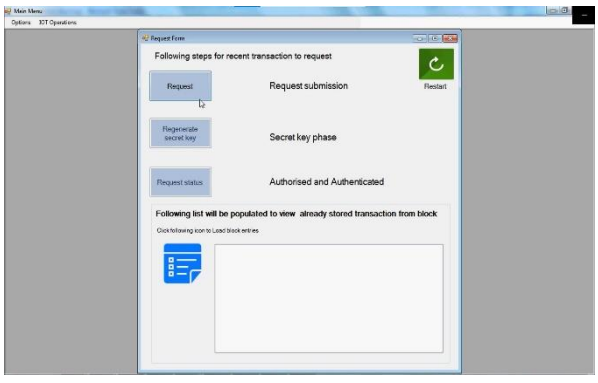

Fig. 8. IoT Options

 DOI : 10.35291/2454-9150.2021.0409

Fig. 9 Transaction Process

Server Options or tamper with the existing database a transaction with a bug like icon is registered.

V. CONCLUSION

Blockchain, being one of the most emergent technologies, has demonstrated its utility in a variety of industries, including IIoT. The combination of blockchain and IIoT has resulted in a big revolution and a slew of advantages. The rise of IIoT will have a significant impact on various industries. As a result, it's critical to understand and mitigate IIoT security flaws. The security challenges of IIoT have been investigated in depth in this research. Many recommendations have been made to use blockchain in IIoT to address cyber dangers and attacks. In addition, a Permissioned Blockchain enabled IIoT has been developed to address IIoT security concerns in terms of safe device connection, server, data sharing, and access control mechanisms. In a permissioned blockchain, the usage of a CA component, smart contract, and consensus nodes, as well as the execution of restricted transactions, assures privacy and security across the network.

VI. FUTURE WORK

Blockchain is effective when used with IIoT, according to a comprehensive analysis. Blockchain is projected to be transformative for IIoT technologies. The implementation of the suggested Permissioned Blockchain enabled IIoT will be done in future research. It will also be assessed in order to as- sess the permissioned blockchain's security and performance. Future work will involve a more thorough examination of the proposed blockchain, as well as an assessment of the influence of design choices on security and privacy. The impact of a permissioned blockchain, such as Hyperledger Fabric, on safe- guarding IIoT communication is currently being investigated. Furthermore, it is critical to consider blockchain security concerns that may affect IIoT systems. Because there are three main forms of blockchain, public, permissioned/consortium, and private, it's crucial to understand how they behave. A future study will be needed to see how the adoption of IIoT affects or improves the security vulnerabilities of blockchain. And since both technologies are still in their early stages of development, it will be fascinating to see what unprecedented meaning they will have for us in the future and how IIoT will effect blockchain security concerns.

REFERENCES

[1]C. H. Liu, Q. Lin and S. Wen, "Blockchain-Enabled Data Collection and Sharing for Industrial IoT With Deep Reinforcement Learning," in IEEE Transactions on Industrial Informatics, vol. 15, no. 6, pp. 3516- 3526, June 2019, doi:10.1109/TII.2018.2890203.

[2]J. Huang, L. Kong, G. Chen, M. Wu, X. Liu and P. Zeng, "Towards Secure Industrial IoT: Blockchain System With Credit-Based Consensus Mechanism," in IEEE Transactions on Industrial Informatics, vol. 15, no.6, pp. 3680-3689, June 2019.

[3]W. Liang, M. Tang, J. Long, X. Peng, J. Xu and K. Li, "A Secure FaBric Blockchain-Based Data Transmission Technique for Industrial Internet of Things," in IEEE Transactions on Industrial Informatics, vol. 15, no.6, pp. 3582-3592, June 2019.

[4]Q. Wen, Y. Gao, Z. Chen and D. Wu, "A Blockchain-based Data Sharing Scheme in The Supply Chain by IIoT," 2019 IEEE International Con- ference on Industrial Cyber Physical Systems (ICPS), Taipei, Taiwan, 2019, pp. 695-700.

[5]J. Wan, J. Li, M. Imran, D. Li and Fazal-e-Amin, "A Blockchain-Based Solution for Enhancing Security and Privacy in Smart Factory," in IEEE Transactions on Industrial Informatics, vol. 15, no. 6, pp. 3652-3660, June 2019, doi: 10.1109/TII.2019.2894573.

[6]E. K. Wang, Z. Liang, C. M. Chen, S. Kumari, and M. K. Khan, "PoRX: A reputation incentive scheme for blockchain consensus of IIoT," Future Generation Computer Systems, vol. 102, pp. 140-151, 2020.

[7]Y. Lu, X. Huang, Y. Dai, S. Maharjan and Y. Zhang, "Blockchain and Federated Learning for Privacy-Preserved Data Sharing in Industrial IoT," in IEEE Transactions on Industrial Informatics, vol. 16, no. 6, pp.4177-4186, June 2020.

[8]M. Shen et al., "Blockchain-Assisted Secure Device Authentication for Cross-Domain Industrial IoT," in IEEE Journal on Selected Ar- eas in Communications, vol. 38, no. 5, pp. 942-954, May 2020, doi:10.1109/JSAC.2020.2980916.

[9]Samira Yeasmin, Adeel Baig., "Permissioned Blockchain-based Security for IIoT," in 2020 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), Sept 2020, doi:10.1109/IEMTRONICS51293.2020.9216343.

[10]S. Yeasmin and A. Baig, "Unblocking the Potential of Blockchain," 2019 International Conference on Electrical and Computing Technologies and Applications (ICECTA), Ras Al Khaimah, United Arab Emirates, 2019, pp. 1-5, doi: 10.1109/ICECTA48151.2019.8959713.

 DOI : 10.35291/2454-9150.2021.0409