Consortium Blockchain for Certificateless Signatureless Scheme in Industrial IOT Environments.

Lakshwanth Prasad K
Department of CSE
S.A. Engineering College

Bhuvanesh H,
Department of CSE
S.A. Engineering College

Vasanth S,
Department of CSE
S.A. Engineering College

Dr. Subramaniam M,
Department of CSE
S.A. Engineering College

***Abstract* — Consortium Blockchain can be used as a layer of faith for complex industrial internet of things this type of blockchain can be cost effective for the industrial IoT.To implement the controllable blockchain for IIoT End devices the blockchain history must be written back to the original condition when an cycle breach is found. At eniese et al projected and productable blockchain by the usage of hash based on chameleon to replace usual hash method, this makes sure that blockchain chronicle to be written when required (Euro S&P 2017). By stating the first threshold chameleon hash (TCH) and accountable and sanitizable chameleon signature (ASCS) schemes is a public-key signature supporting file-level and block-level changes of signatures without impairing authentications.**

Keywords*— *Identity, blockchain, Ledger, Transactions, Consensus, Security.

I.INTRODUCTION

The Industrial Internet-of-things (IIOT) are earthly allotted, calculational-limited and affiliate various techniques. The conventional network can be used to achieve these features efficiently, but their availability is Zero. Nakamoto proposed an answer called “blockchain” [5] which provides open, dispersed and abiding trust layer. Due to the limited computing resources, lightweight cryptographic schemes are used for efficiency. The cryptographic schemes like SHA-256 and elliptic curve discrete signature algorithm (ECDSA)[4] are used for security. Blockchains are generally considered to be very secure, but the level of security they provide is proportional to the amount of hash power that supports the network. The more the count of miners there are and the more their mining hardware resource is, it is tough to perform an attack on the network.

Normally, centralized system architectures are exposed to various types of attacks which leads to the pact of data. Trusting the third party or any intermediate application which stores data to their location, these data can be shared or given to any other users who are prohibited without the knowledge of the author or the owner of the data.

However, while using blockchain there is no protection to the data and exposed to attacks a said before, to protect them and to reduce the cost of the IIoT devices certain hash and signatures are used, those are threshold chameleon hash (TCH) and Accountable Sanitizable Chameleon signature (ASCS). These two cryptographical hashing algorithms can be used to overcome the following issues such as Lack of threshold in the chameleon hash. Reducing the cost in IIoT devices. No authentication and validation of redaction. The above problems are the consequences of the attacks, due to the attacks they use chameleon hash by using that the above stated problem arises and the redaction is needed for the block chain.

This paper is organized in which Section II describes the current industrial IIOT Systems, Section III explains about the blockchain domain and the redactable blockchain features, Section IV illustrates the proposed architecture of the solution and also deals with the implementation part of the solution, section V provides the applications and challenges of the solution and section VI concludes the paper.

II.EXISTING SYSTEM.

Industries works on certain applications these applications use various types of sensors, network components and some expensive hardware for the processing various operations regarding the applications. Basically, these details are stored by the administrator of

the industry who has the control to protect them; these data should be protected highly because these leakages of data can cause billion problems[11].

A. Industrial Data.

Industrial Internet of Things (IIoT) has been a major attention grabber for the academics and industrial people which is noted as a significant future growth. Basically, these industries use specific data for their working the data might be network nodes or storage devices, network addresses, microgrids etc. The above data must be protected in order to maintain the confidentiality in the organization. Furthermore, there should not be any attacks on that data to protect them some authorized sensors are used for their protection. If an attack is been done due to the limitation of chameleon hash. The block chain must be repaired in order to get the working back

B. Repair of Blockchain.

Normally, public blockchains are exposed to various attacks, impairing anonymity and non-changeability to support and perform illegal trades & distribute illegal contents, various activities. To stop that the history of the blockchain should be written back. So, a redactable consortium blockchain is used.

III. BLOCKCHAIN TERMINOLOGIES AND REDACTABLE BLOCKCHAIN.

Blockchain is a technology in which the data and information are considered as blocks. It is an open ledger that is capable of storing and recording transactions that happens between two sections and makes sure that all the data are been verified. Blockchain normally possess peer- to-peer ledger for inter node communication and validation It ensures three major characteristics transparency, decentralization and immutability. Redactable Blockchain is been used in our experiment for re writing the history. Some of the important terminologies and concepts of blockchain and redactable blockchain are [7];

1. Distributed network.

Blockchain is a distributed network in which all the nodes are linked together to form a network without any centralized entity. All the nodes know each other and they can communicate using the message passing technique. There are two types of nodes in this network ordinary nodes and miner nodes[8].

2. Redactable Blockchain

A Redactable blockchain is built by the chain of transactions generated by units because of the "lock" between them. Each chain is mapped to an administrator who is the only owner of the key. It is used to correct factual errors and typos and bring the data compliance with the requirement of an legislation change. This is implemented by adding an lock to the link of hash chain. Important Motive is to rewrite the blockchain to its original state when the chain is breached[9].

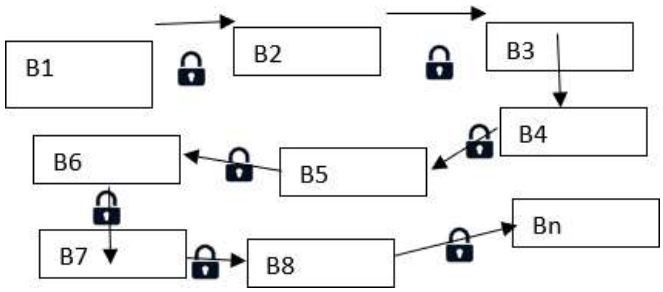

Fig 1: Redactable blockchain & it's working.

3. Chameleon Hash

Chameleon Hash is a type of hash function where hashing is done and parameterized by public-key. It specifically uses trapdoor function which acts as a resistant function where there will be no collisions but this chameleon hash provides some limitation that it is exposed to various attacks and it cannot be further used for the experiment. So, a threshold version of the chameleon hash is been used so the above limitation is rectified.

4. Accountable and Sanitable Chameleon Signature(ASCS)

This is a chameleon signature. It is a public key signing scheme where it withstands the file level and block level changes & modifications without affecting the authentication. It does not require any permission from the user for the modification of the data, the modifications are been done by the authorized sensors. It is used to remove disruptions from the blockchain after some breach.

IV. PROPOSED ARCHITECTURE AND IMPLEMENTATION

A. Proposed System Features.

The proposed system basically helps to disregard break from blockchain once the chain offended. It also gives better and efficient simulation results of rcb redaction even if it is carried out at a small sector or run as a record-level which is coarse grained mechanism.

For better working of these following advantages, redactable blockchain can be constructed with better and efficient ASCS and TCH hashes [6].

1. Structure Of Block

Block is the fundamental structure of the blockchain. It consists of different fields such as nonce a random integer field, target denotes the difficulty of the mining operation, and previous hash indicates the previous block level hash. A timestamp filed provides the time the block is created which also indirectly leads to the difficulty of the block. A block may consist of any number of transactions as per the requirement of the client [11].

The first block created in a blockchain is known as a genesis block whose previous hash is 0. Each and every block must be signed explicitly by the corresponding sender. Thus, storing the data inside a block ensures a high-level security due to the usage of complex cryptographical algorithms such as public key encryption and hashing functions.

All the blocks of the blockchain are strongly connected using the field called previous block hash [9]. A hash of a particular block is obtained by combining all the fields of the block.

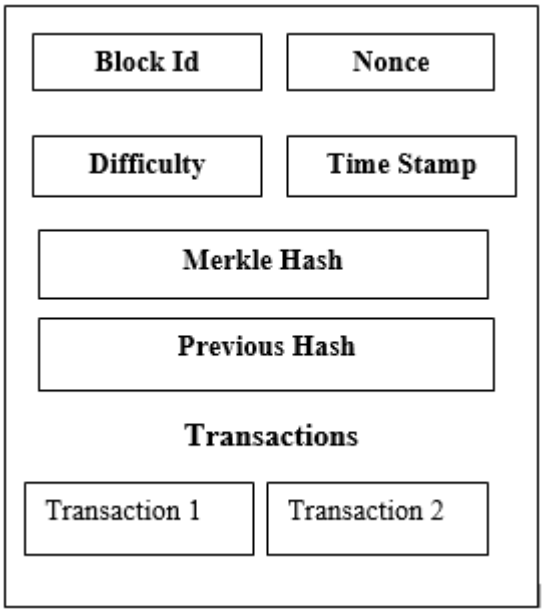

Fig 2: Structure of Block.

2. Architecture Of Redactable Blockchain

There are 5 main role players in redactable blockchain,

- System manager,
- Client,
- User,
- Consortium blockchain,
- Private blockchain.

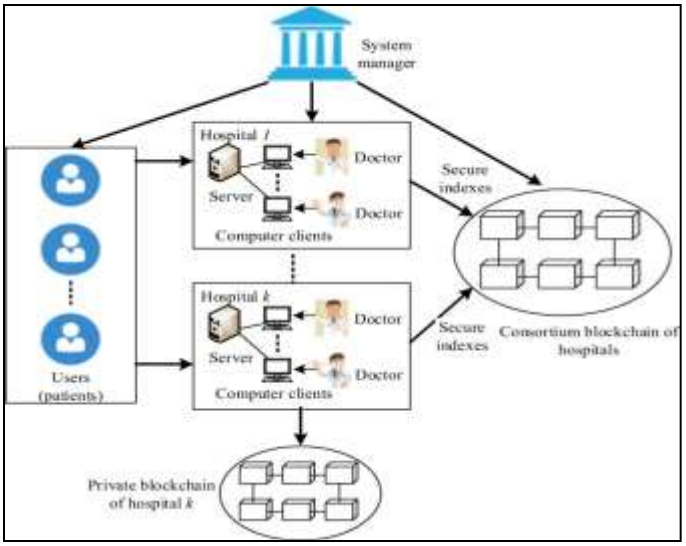

Fig 3: Working of Consortium Blockchain

3. Figures and Tables

All the participants the network will have a copy of the recent blockchain in a ledger. Since all the nodes share a same copy of the blockchain ledger it is a distributed one. It consists of the blocks provided by the nodes in a chain form. All the blocks are mined by the respective miners and after approval of the main ordinary nodes to accept a block, the particular block is added to chain and all the nodes will update their own ledger. This ledger feature of blockchain ensures a transparent environment to the network for handling the request of the nodes as well as identifying the invalid information.

4.Immutabilitiy Feature

One of the most core security feature provided by the blockchain is the immutability of the data which are stored in a block. It is tedious to alter the data due to the well-organized way of hashing the data in form of transactions in a special tree called Merkle tree. Any attacker who tried to alter the block data may need to change the all subsequent block hashes since all the blocks are linked together. It may require a lot of resources to mine all the blocks to alter a single block data in a blockchain. This feature ensures a high-level security to the data stored in a blockchain.

B.IMPLENTATION OF SOLUTION

Even though redactable blockchain has its own benefits there can be further improvements in it. It is suggested that a stabilized building of ASCS scheme and protection analysis in this area. Commonly our ASCS produces sum of the chameleon signature notion and sanitizable signature, it permits reducing to occur dissimilar according to the set of sanitizable group while a new rejected convention is designed to hold reducable accountable at any time. It also proposes a concrete raising of TCH and protection report is the base of this task. It basically provides the base for current and propose blockchain.it also permits chameleon hash collision hash to be found in a scattered way [10].

The previous diagram is how redactable consortium usually works. Now to improve this process, a system is been proposed that it redacts the blockchain at any time. To achieve this following change are to be done.

- Tch Setup
- Tch Key Generation
- Tch Hash and Forge
- Ascs Setup
- Ascs Key generation
- Ascs Sign
- Ascs Verify and Sanitize

Upon the proposed system, the following properties are achieved:

- Unforgeability,
- Indistinguishable,
- Non-Transferable,
- Non-Repudiation,
- Deniability,
- Sanitizer-Accountability.

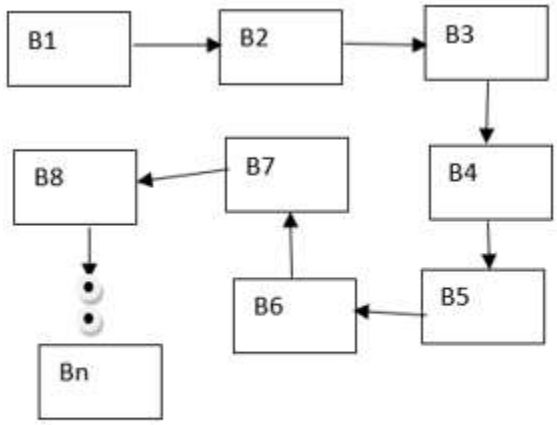

Figure 4: Working of Blockchain

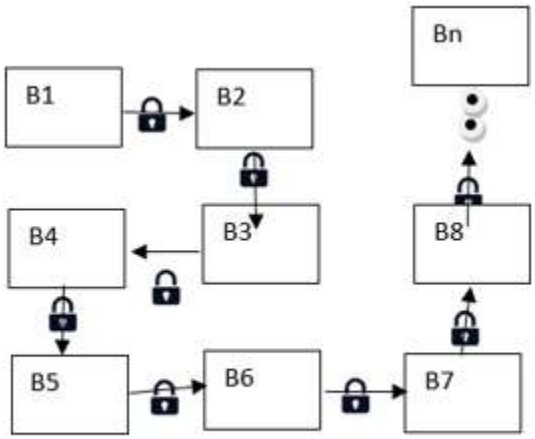

Figure 5: Working of Consortium Blockchain

V.Challenges.

Some of the important challenges associated with the redactable blockchain application are listed as follows;

1. Compromise in the security.

One of the major challenges associated with a blockchain is the 51% attack. This type of attacks is possible only if a certain attacker holds about 51% of the resources for attacking. But that much of resource may be very expensive to hold such huge resource and use it. Hence this attack can be reduced easily due to the complexity of the attack. Another issue with the blockchain is the transaction execution due to the high-level mining process taking place to validate the blocks.

VI.CONCLUSION

There are 2 theoretical primitives needed for the construction of redactable consortium blockchain for IIoT devices those are TCH and ASCS these two things cater for decentralization, low computation & authentication modifications. The IIOT devices work in a controllable manner so the serious aftermaths are controlled File-level redaction is executed with sacrifice of protection or redaction is kept at small scale to show redaction is useful. That is why it is acceptable that diminish is required only for small requirements on the chain, and there is always an off trade between protection and usability

VII.REFERENCES

[1] S. Jeschke, C. Brecher, T. Meisen, D. Ozdemir, and T. Eschert, "Industrial internet of things and cyber manufacturing systems," *Ind. Internet Things.*, pp. 3-19, 2017.

[2] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial internet of things: challenges, opportunities, and directions," *IEEE Trans. Ind. Informa.*, 2018.

[3] R. Lacuesta, G. Palacios-Navarro, C. Cetina, L. Penalver, and J. Lloret, "Internet of things: where to be is to trust," *EURASIP J. Wireless Commun. Netw.*, no. 1, pp. 1-16, 2012.

[4] X. Du, M. Guizani, Y. Xiao, and H. H. Chen, "A routing-driven elliptic curve cryptography based key management scheme for heterogeneous sensor networks," IEEE Transactions on Wireless Communications, Vol. 8, No. 3, pp. 1223-1229, March 2009.

[5] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system."2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[6] Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things, Zhetao Li, Member, IEEE, Jiawen Kang, Rong Yu, Member, IEEE, Dong dong Ye, Qingyong Deng, Yan Zhang, Senior Member, IEEE.

[7] https://www.tutorialspoint.com

[8] https://blockgeeks.com

[9] https://wiki.hyperledger.org

[10] https://ics.uci.edu

[11]https://en.wikipedia.org