ISSN: 2096-3246
Volume 54, Issue03, Dec,2022

Hyper ledger Fabric Block chain for dataSecurity in IOT Devices

Dr B. Srinivasa Kumar[1], Dr Farha Anjum[2], Dr B. Ratnakanth [3], Dr.B. Doss[4] , Dr.R Prabhakar5 .

1 Assoc Professor Of Engineering Mathematics Dept, Koneru Lakshmaiah Eduction Foundation Vaddeswaram,Guntur ,Andrapradesh,India
[2] Professor Of ECE Dept Siddhartha Institute Of Engineering And Technology, Hyderabad, India
[3]Professor Of CSE Dept,Sri Indu Institute Of Engineering And Technology , Hyderabad, India
[4] Professor Of ECE Dept, CMR Technical Campus, Hyderabad, India
[5] Professor Of ECE Dept, Malla Reddy Institute Of Technology And Science, Maisammaguda, Hyderabad,India
Sk.Bhavirisetti@Gmail.Com, Farha.Ece@Gmail.Com, Bratnakanth@Gmail.Com, Dasalways4u@Gmail.Com
Rpr612@Gmail.Com

***Keywords*:**

Block chain, distributed system, hyper ledger fabric, Internet of Things (IOT).

***Abstract*:**

In modern world Data security plays a major role in all fields such as IOT, ML and AI etc due to digitalization. In home appliance also IoT based smart energy developed to take the power reading by providing data security. However, also it may beget serious profitable loss for the authorities, If the Power reading signals are tampered. The particular information violation leads lot of problems. To reduce it, we recommend a authorization block chain network. Block chain preserve time marked tally records that is tough to interfere. Every sale is recorded and distributed across numerous party bumps, these records are inflexible because they've blocks of data which are linked to each other with strong cryptographic hash. The block chain network is erected using hyperactive tally fabric, where all the party bumps are registered and only registered bumps involve in agreement process of sale. In fabric, MSP (class service provider) identifies the identity of the party bumps through X. 509 digital instruments issued by instrument authority. Along with creation of block chain network for the operation, a mobile customer, a web customer, an Arduino customer and web garçon is created. ARDUINO customer is the power consumption. The web garçon POSTs the details to the Block chain Network, where deals undergoes agreement to add this information to block chain tally. It distribute to all rake knot has the original dupe of tally. The streamlined information appear on internet platform interfaces. Obscurity- enhanced block chain has beenenforced succession requests and concurrent requests fromnumerous tackle module that has an energy cadence measurethe druggies using different tools

I. INTRODUCTION

A strong safety is necessary to preserve the serene records undamaged between IOT devices. There are many challenges in implement data protection for Internet of Things (IoT) policy. The capability of an illegal customer

to right to use the scheme desires to be sterile for attacks such as disagreement of service, and only the certified users should be permissible to admission the information in a protected scheme with no holdup. It is very vital for the message to be classified to build convinced that facts cannot be altered or viewed throughout the society. In an IOT function such as tidy meter, one should focus to stay away from any bother due to impression foremost to severe loss. A result for information safety, private in order violation and tampering of facts at the check supplier, after getting it. Block chain is originate as one of rising skill to address these issues. The information can be disseminated transversely the systems and the sanctuary of these spread information can be achieved. Transactions are saved in the system as ledger records. Contract data in blocks and connected cryptographically with strong hash encryptions. Each hunk store previous , as the present hunk comprise the hash. If a hacker tries to modify one block, then it immune to do modification. As the block chain technology is distributed, if the data is crashed, the ledger stuffing inside the other nodes. So tampering and data loss is avoided.

Permission block chains build a chain delimited by all standard, recognized foundations. The applicant contain a analogous core, but may not belief all extra fully. Authorization assist for protected the commands among contestants. Authorization block chain consist consent protocols. These consensus protocols may CFT or BFT. Conventional block chain stay away from any intended malevolent codes. So every proceedings beginning an function to bring up to date ledger are verified. Interpretation and distribution through the interpret power meter and uploading it to server using a authorization block chain Network. A Smart contract contain regulations for growing the dependability of customers.

II. RELATED WORK

Security is implemented at the design stage to avoid the security concerns. Threat taxonomy at different levels. A collection of safety and solitude provisions for web metering derivative support on the accessible threats. Dealing with issues of records alter by middle attack, and sophisticated metering with MICAz motes for statement between smart meters. The assault free customer and malevolent customer to protect solitude in communal system. Block chain provides distinctiveness, security to the clients by parallel answer. Protected link between 2 IOT devices using ethereum block chain platform. 2 research in IoT devices with and without block chain. We focus on concerns by the sub model of IoT. Server failures, which is centralized causing a single point failure and ethical hacking causes the data tampering. A pub/sub architecture developed for block chain that conserve discretion of confidential data. Block chain method for a spread technique to provide protection in preserve the patient's health check proceedings. Authentication, encryption, accessing steps to get the data in Block chain. An IoT server platform used to address the vulnerabilities and pressure to safety in Mysql's Mobius configuration. The information composed and broadcast strongly [9]. Deal with finding of user personal data in block chain IOT environment process the proof. The zero knowledge proof developed and ABAC on Hyper ledger Fabric block chain framework for access control in IOT system is projected . The block chain based frame-work using Ethereum to maintain EMR was planned. The frame-work intend at conserve isolation of the patient data and right to use the medical records to approved person.

III. PRELIMINARIES

The specific members are connected through a channel for specific transactions by providing security and discretion. In earlier systems have the order-execute architecture.

A. Hyper ledger Fabric architecture [13], [14]

Hyper ledger Fabric client SDK provides the structured libraries for chain code applications. The elements are described below.

Peers: A no. of peer nodes are in block chain system. The ledger and smart contracts are hosted by peers, they are considered as fundamental elements of block chain network. The instances of ledger and chain code are hosted by peer. Any transaction generated by smart contract is recorded immutably in a ledger. In a block chain

network the shared process are encapsulated by smart contract and shared information is encapsulated by ledgers. If the block chain resources have to be accessed by application and administration, then they should have an interaction with peer since the ledgers and chain code are hosted by peers. Due to these reasons peers are considered to be basic construction blocks of a hyper ledger fabric block chain network. Peers of organization are connected through channel. A peer performs many roles such as an endorsing peer, committing peer, anchor peer or a leading peer.

The endorsing peers involve in executing smart contract during a transaction and they return signed response back to client application. The committing peers involve in validating the blocks of transactions that are orderly arranged and applies block to its local ledger copy. Since all peers store a copy of ledger, hence all peers in the network can take the role of committing peer. An anchor peer will be the first peer in the channel that will be discovered by other organizations on the network. If institute have many peer nodes important peers engage in converse with others.

Block chain ledger: It have database and block chain**.** The collection of states stored to assist the developer to reduce the work by checking the whole contract log. Block chain hold deal, enclose as interlinked. Deals are stored in each block to specify the information. It confine all updates and deals are accrue inside and added to it.

The block chain data cannot be customized. It is varied when updates taken place. A block chain consisting a chain of blocks dealings which are unchallengeable.

*Elegant Agreement: R*ight of entry have many laws. If a customer request data, it should be mount.

Orderer nodes: Local replica of ledger is stored in blocks. An ordering service is a collection of ordered nodes within the network and there will be a single ordering service for a network. The policies of channel and membership information of each member of channel are maintained in channel configuration. Ordering service will have the channel configuration for the network and hence they administer a network.

Network Policies: The official document power offer the acquiescence proof for business to validate the system. The customer request apply credential to prove business proposal to support business suggestion and append transaction to the ledger.

Channel: Channel is the secure communication link between the members by creating a particular channel can communicate, data isolation and confidentiality.

Identities and MSP: X.509 digital certificate have identities, that are used to determine the particular actor permissions to access resources and information. MSP provides the policies that govern valid identities for organization. The X.509 certificates are used as identities in implementation of MSP in fabric. The MSP lists the identities to define the members of an organization.

IV.SYSTEM MODEL AND DESIGN

In IOT system architecture blocks are Block chain Network, Web server, Web client, Mobile client, Arduino client (smart energymeter)

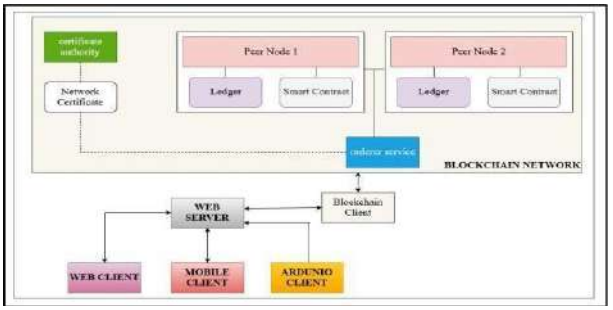


Fig. 1.IOT System overview

Implementation Steps:

1. Create web server and host APIs.
2. Set up contact between the IOTsensor machine and the server.

3. Create a web client and manage admin activities.
4. Create a mobile client for registered users.
5. Set of connections with the web server.

A. Block chain network:

Certificate Authority (CA) issues the certificates for actors to authenticate to the network. The peers, orders etc are the active elements provides/use digital identities. X.509 certificate have the permissions and used in implementation and reorganization of MSP from a authorized source.

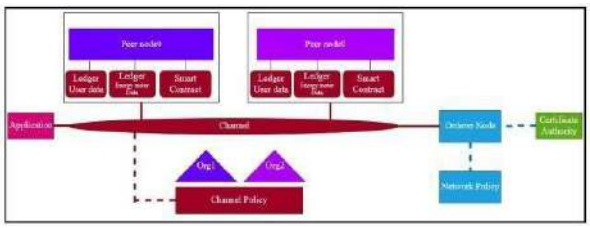


Fig. 2.Block chain network

According to network policy, network constructed and should have single order node and one peer for two organizations The digital certificate issued to the participants. The permission granted to the linked channel. The network maintain 2 ledgers for User Data and Usage data. A single smart contract with multiple functions runs on peers.

Web server:

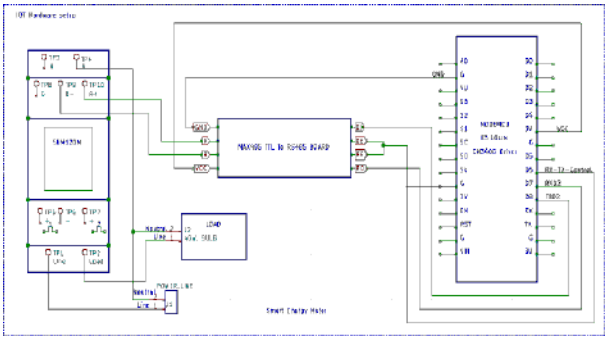
It is a system program that serves Web pages to the users. The web server processes and provides a web page to the client. In azure cloud system requirements will change as the size of the block chain changes .The system requirements are 2 core CPU, 4GB Memory, 10 GB of HDD/SSD, Linux based OS. The application is divided into UI routes and API routes. The API routes start with the path /API. POST, GET for a user ID data and dependent on the block chain module. The block chain module is packaged as a javascript module and is imported using RequireJS pattern. All are keen with essential javascript constructs and exported as functions. The respective REST APIs are programmed to switch the queries and chant requests.

B. Web and Mobile client:

They fetch the information from the server and provide user interface. Mobile application developed. Mobile client can only fetch in sequence of a exacting user. The Web client is provided with contact to analysis all users information and also with right to use for creation of new users. A User ID for every new user created to generate transactions.

C. Arduino client:

The Node MCU acts as an Arduino client, which reads the energy meter data through serial port and POSTs this data to the web server. SDM120M is used as the energy meter which is capable of measuring the Voltage in Volts(V), current in amperes(A), power in Watts(W), frequency in Hertz(Hz), energy in KWh, power factor etc. of the connected load.



ISSN: 2096-3246
Volume 54, Issue03, Dec,2022

Fig. 3.Arduino Client

SDM120M for reading of measured value. SDM120 with RS485 to communicate with systems using the Modbus RTU Protocol. It uses a MAX485 TTL - RS485 board provides two way serial communication signal conversion between theRS485 to TTL and vice versa.

v. RESULTS AND ANALYSIS

Transaction details are stored with V,I,T,F, P and energy along with user ID.

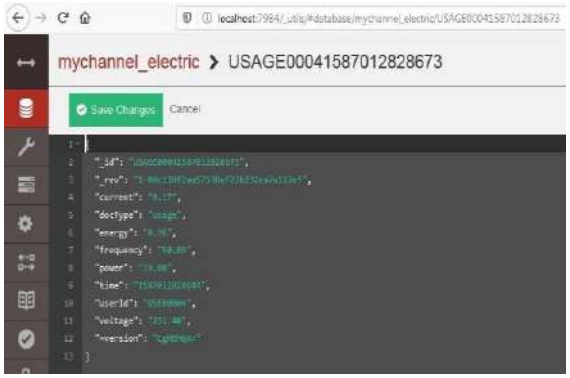


Fig. 4.Details of data in one of the transaction

On observing the transaction records, both peers data have same. So it is decentralized and distributed.

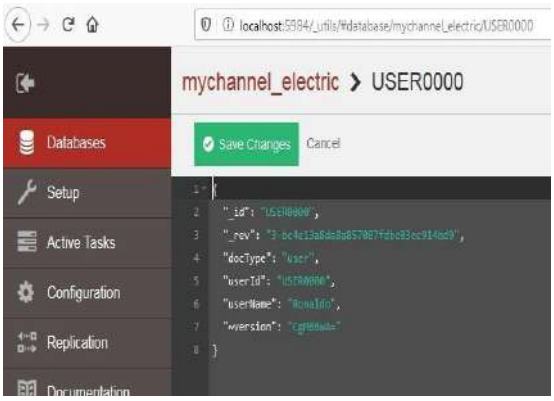


Fig. 5.The detailed transaction record of USER0000 reflected in peer0 of Org1

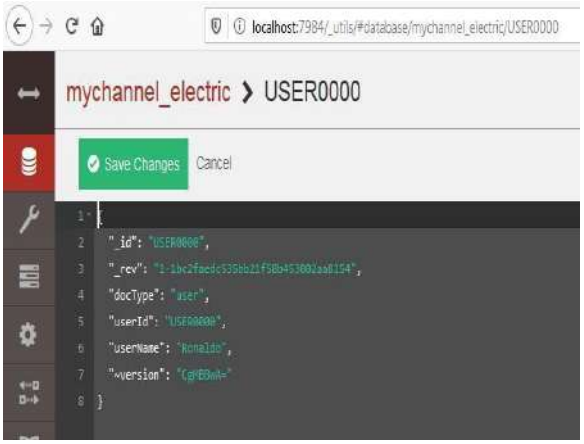


Fig. 6.The detailed transaction record of USER0000 reflected in peer0 of Org2

To ensure the safety of information, anybody tamper the peer data, the original information in another peer, thus provides the protection of data.

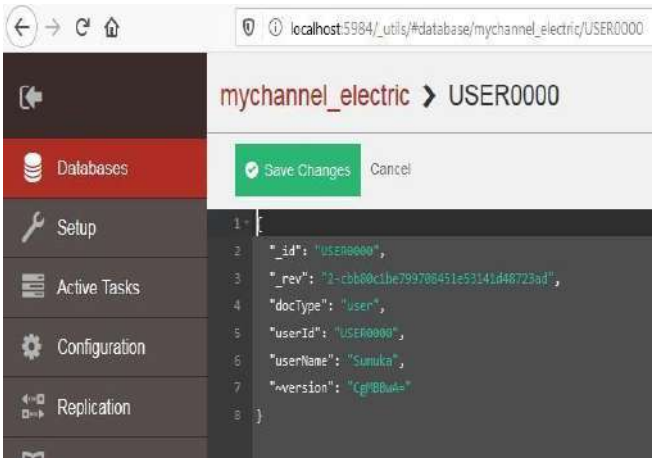


Fig. 7.Transaction details in peer0 of Org 1 aftermodifying username.

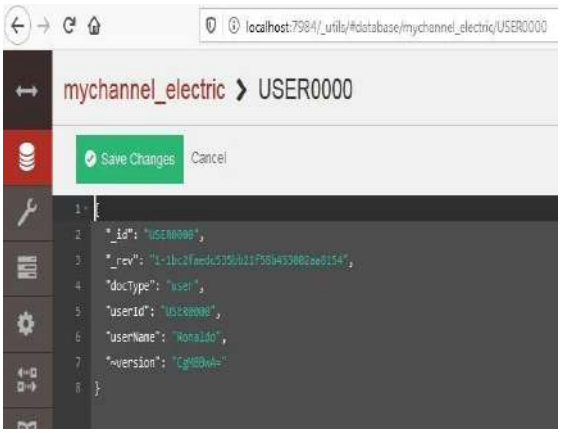


Fig. 8.Transaction details in peer 0 of Org 2 aftermodifying username in peer0 of Org 1

The data is modified in the peer with username and results are on mobile app.

Fig. 9. Mobile client sending a GET request andobtaining a response from web server

ISSN: 2096-3246
Volume 54, Issue03, Dec,2022

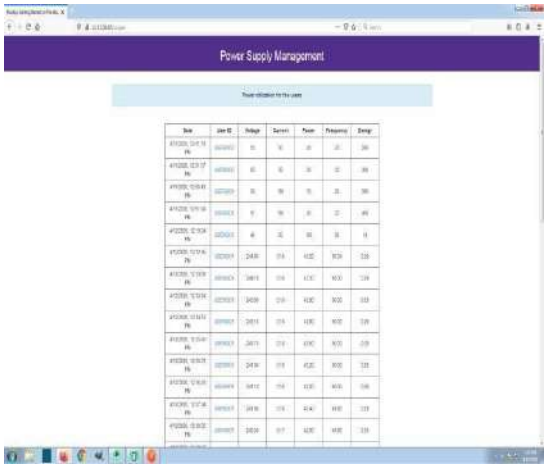


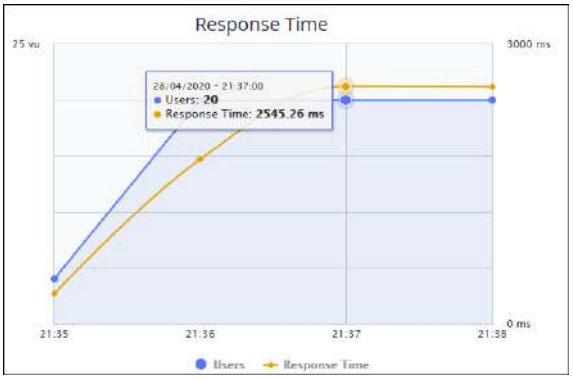
Fig. 10.Web Client sending a GET request andobtaining a response from the web server.

In block chain height increases after each write operation.

Fig. 11.block chain hash information before updatingthe usage details of USER0009

Fig. 12.Block chain hash information after updatingthe usage details of USER0009

Performance analysis: The application was produced and examined for performance by POST and GET requests. The performance examined on different platforms.



ig. 13.sequential test results for 100 POST requestswithin 30 seconds using postman.

Fig. 16.Load test graph for concurrent GET request

Using Blazeter tool

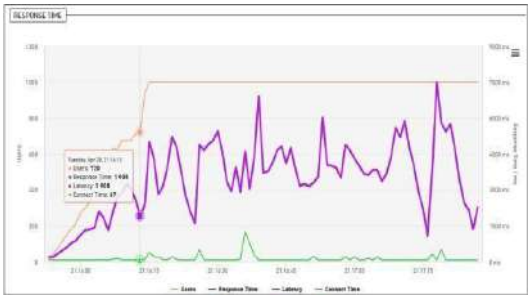


Fig. 17.Response time graph for concurrent GET request using Blazemeter tool

Multiple test tools are used for specific information to update the request. In a single threaded application sequential execute the request and proposed testing measure average time for a transaction and identify with the actions for contemporaneous requests

CONCLUSION AND FUTURE SCOPE

It provides the visualization of an IOT ecosystem for trusted and non-trusted parties. The integrity of data is maintained across the ecosystem with tamper-proof system. The performance test results shows the normal functioning and usability. The comparative performance analysis also shown in result. The basic requirement of IoT are information protection, back up, availability, scaling. The tamper proof provides tight security in IoT. In this send data from Arduino client to server in a encryption technique at the client and at the server side decryption technique gives the protection to the data. It is conducted for two organizations in the network and assists to many IOT devices and applications.

REFERENCES

1. Obaid Ur-Rehman, NatasaZivic, ChristophRuland,“ Security issues in smart metering systems”, IEEE International Conference on Smart EnergyGrid Engineering (SEGE) , 2015
2. Pardeep Kumar, Yun Lin , Guangdong Bai ,Andrew Paverd, Jin Song Dong , Andrew Martin, “Smart Grid Metering Networks: A Survey on Security, Privacy and Open Research Issues”, IEEE Communications Surveys & Tutorials ,Volume: 21 , Issue: 3 , 2019.
3. Mohsin Kamal , Muhammad Tariq, “Light-Weight Security and Block chain Based Provenance for Advanced Metering Infrastructure”, IEEE Access (Volume: 7), 2019, INSPEC Accession Number: 18826750

4. Ruiguo Yu, Jianrong Wang, Tianyi Xu , Jie Gao , Yongli An , Gong Zhang , Mei Yu , "Authentication With Block-Chain Algorithm and Text Encryption Protocol in Calculation of Social Network ", IEEE Access (Volume: 5), 09 November 2017
5. DinanFakhri, KusprasaptaMutijarsa, "Secure IoT Communication using Block chain Technology", International Symposium on Electronics and Smart Devices (ISESD), 2018, INSPEC Accession Number: 18374691
6. Pin Lv , Licheng Wang , Huijun Zhu , Wenbo Deng , LizeGu, "An IOT-Oriented Privacy-Preserving Publish/Subscribe Model Over Block chains", IEEE Access (Volume: 7), march 2019, INSPEC Accession Number: 18576298
7. Mary Subaja Christo, AnigoMerjora A, ParthaSarathy G, Priyanka C and Raj Kumari M, "An Efficient Data Security in Medical Report using Block Chain Technology", International Conference on Communication and Signal Processing (ICCSP), 2019
8. Jin HyeongJeon ; Ki-Hyung Kim ; Jai-Hoon Kim, "Block chain based data security enhanced IoT server platform", International Conference on Information Networking (ICOIN), 2018, INSPEC Accession Number: 17720930
9. XiPeiyu,ZhangQian,WangHaining ,ZhaoHaoyue ,WangChunyan , "Exploration of Block chain Technology in Electric Power transaction", International Conference on Power System Technology (POWERCON), 2018, INSPEC Accession Number: 18392665.
10. Chan Hyeok Lee , Ki-Hyung Kim, "Implementation of IoT system using block chain with authentication and data protection", International Conference on Information Networking (ICOIN), 2018, INSPEC Accession Number: 17720922.
11. Han Liu ; Dezhi Han ; Dun Li, "Fabric-iot: A Block chain-Based Access Control System in IoT", IEEE Access (Volume: 8 Page(s): 18207 – 18218), January 2020,Electronic ISSN: 2169-3536.
12. Eman-Yasser Daraghmi, Yousef-AwwadDaraghmi, Shyan-Ming Yuan, "MedChain: A Design of Block chain-Based System for Medical Records Access and Permissions Management", IEEE Access (Volume:
7 , Page(s): 164595 - 164613), November 2019,INSPEC Accession Number:19144264.
13. https://hyper ledger -fabric-ca.readthedocs.io/en/release-1.4/users-guide. html
14. https://hyper ledger -fabric.readthedocs.io/en/release-2.0/key_concepts.h tml
15. https://hyper ledger -fabric.readthedocs.io/en/release-2.0/build_network. html
16. https://kotlinlang.org/docs/reference/android-overview.html
17. Markus Schäffer,Monika di Angelo and GernotSalzer, "Performance and scalability of private ethereum Block chains", International conference on process Management, August 2019, Online ISBN 978-3-030-30429-4