Hyper ledger Fabric Block chain for data Security in IOT Devices

Ms. Imrose Basha[1], Mr. G Ahmed Zeeshan[2], Mr. D Kamalakar Reddy[3]
1,2 Associate Professor, Assistant Professor[3]
1,2,3Department of ECE
1,2,3Global Institute of Engineering and Technology Moinabad, Ranga Reddy District, Telangana State.

***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 istough 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 throughX. 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 tackle module that has an energy cadence measure 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. Itdistributeto allrake knot has the original dupe of tally. The streamlined information appear on internet platform interfaces. Obscurity-enhanced block chain has been enforced to avoid the exposure of exact records. Also operation's performance investigation is carried out for number of succession requests and concurrent requests from numerous druggies using different tools.

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

I. INTRODUCTION

A strong safety is necessary to preserve the serenerecordsundamagedbetween IOT devices. There are many challenges inimplementdataprotectionforInternetofThings(IoT) policy.Thecapabilityofanillegalcustomer to right to use theschemedesirestobesterileforattackssuchasdisagreement ofservice, and only the certified users should be permissible toadmissiontheinformationinaprotectedschemewith noholdup.Itisveryvital for the message to be classified to buildconvincedthatfactscannotbealteredorviewedthroughoutthesociety. In an IOT function such as tidy meter, one should focus to stay away from any bother due toimpressionforemosttosevereloss.A resultforinformationsafety,privatein orderviolationandtamperingoffactsat the checksupplier, after gettingit.Block chainisoriginateasoneof risingskill to address these

issues. The informationcan be disseminatedtransversely the systems and the sanctuary ofthese spreadinformation can be achieved.Transactions are saved in the system asledger records.Contractdata in blocks andconnectedcryptographically withstrong hash encryptions. Eachhunkstore previous , as the presenthunkcomprise thehash. Ifahackertries to modify one block, then it immune todo modification. As the block chain technology is distributed,if the datais crashed, theledger stuffinginside the other nodes. So tampering and data loss is avoided.

Permissionblock chainsbuildachain delimited by all standard, recognizedfoundations. The applicantcontaina analogous core, but may not beliefallextrafully. Authorizationassistfor protected thecommands among contestants. Authorization block chain consist consentprotocols. These consensus protocols mayCFTorBFT. Conventionalblock chainstay away fromanyintendedmalevolentcodes. So everyproceedingsbeginning an function tobring up to dateledger areverified. Interpretation and distribution through the interpretpower meter and uploading it to serverusing a authorizationblock chain Network. ASmart contract containregulations for growingthedependabilityofcustomers.

II. RELATEDWORK

Security isimplementedat the design stage to avoid the security concerns.Threattaxonomy atdifferent levels. A collection of safety and solitudeprovisionsfor webmeteringderivativesupportontheaccessiblethreats .Dealing withissuesofrecordsalter by middle attack, and sophisticatedmeteringwithMICAz motes for statement between smart meters. The assault freecustomer and malevolentcustomerto protectsolitude in communalsystem. Blockchainprovides distinctiveness, security to the clients by parallelanswer.Protectedlink between2 IOT devices using ethereum block chain platform.2research in IoTdeviceswithandwithoutblock chain.We focus on concerns by the sub model of IoT. Server failures, whichis centralized causing a single point failure and ethical hacking causes the data tampering.Apub/subarchitecturedeveloped forblock chainthatconservediscretionofconfidentialdata. Block chainmethodforaspreadtechniquetoprovideprotectio ninpreservethepatient's health checkproceedings. Authentication, encryption, accessing steps to get the data in Block chain.An IoTserver platform used to address thevulnerabilitiesandpressuretosafetyinMysql'sMobi usconfiguration. The informationcomposedand broadcaststrongly[9].Deal withfindingof user personal data in block chain IOT environment process the proof. The zeroknowledgeproof developed and ABAConHyper ledger Fabricblock chainframework for access control in IOT system is projected . The block chain based frame-work usingEthereum to maintain EMR wasplanned. The frame-work intend at conserveisolationof the patient data and right to usethe medicalrecordstoapprovedperson.

III. PRELIMINARIES

The specific members are connected through achannel for specifictransactions by providing security and discretion. In earlier systems havetheorder-executearchitecture.

A.Hyper ledger Fabricarchitecture[13],[14]

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

Peers: A no. of peer nodes are in block chainsystem. Theledgerandsmartcontractsarehostedbypeers,theyar econsideredasfundamentalelements of block chain network. The instances of ledgerandchaincodearehostedbypeer.Anytransaction generated by smart contract is recorded immutably in aledger.In a block chain network the shared process areencapsulated by smart contract and shared information isencapsulated by ledgers. If the block chain resources haveto be accessed by application and administration, then theyshould have an interaction with peer since the ledgers

andchaincode are hosted by peers. Due to these reasons peersareconsideredtobebasicconstructionblocksofahyper ledger fabricblock chainnetwork.Peersoforganizationareconnectedthroughchannel.Apeerperformsmanyrolessuchasanendorsingpeer,committingpeer,anchorpeeroraleadingpeer. Theendorsingpeersinvolveinexecutingsmartcontractduring a transaction and they return signed response backtoclientapplication.Thecommittingpeersinvolveinvalidatingtheblocksoftransactionsthatareorderlyarranged and applies block to its local ledger copy. Sinceall peers store a copy of ledger, hence all peers in thenetwork can take the role of committing peer. An anchorpeerwillbethefirstpeerinthe channel that will bediscovered 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 collectionofstatesstored to assistthedeveloper to reduce the work by checking the wholecontractlog.Block chainholddeal,enclose asinterlinked. Deals are stored in each block tospecifythe information.Itconfine all updates and deals are accrueinside and added to it.

The block chain data cannot be customized. It is variedwhenupdates taken place. A block chainconsisting a chain of blocksdealings whichareunchallengeable.

*ElegantAgreement:R*ight of entry have many laws.If a customerrequestdata, it should be mount.

Ordererrnodes: Local replica of ledgeris stored in blocks. An orderingservice is a collection of ordered nodes within the network andtherewillbea single ordering service for a network. Thepoliciesofchannelandmembershipinformationofeachmember of channel are maintained in channel configuration.Ordering service will have the channel configuration for thenetworkandhencetheyadministeranetwork.

*NetworkPolicies:*Theofficial documentpowerofferttheacquiescenceproofforbusinesstovalidatethesystem. The customerrequestapplycredential to prove business proposal to supportbusinesssuggestionandappendtransactiontotheledger.

*Channel:*Channel is the secure communication link betweenthemembers by creatinga particular channel cancommunicate,dataisolationandconfidentiality.

Identitiesand MSP: X.509digitalcertificate have identities, that are used to determine theparticular actor permissions to access resourcesand information. MSP provides the policies thatgovern valid identities for organization.TheX.509 certificates are used as identities in implementation ofMSPinfabric.TheMSPliststheidentitiesto define themembersofanorganization.

IV.SYSTEMMODELANDDESIGN

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

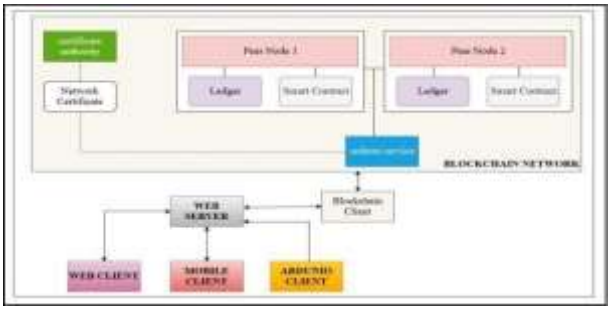


Fig.1.IOTSystemoverview

ImplementationSteps:

1. CreatewebserverandhostAPIs.
2. Set upcontactbetweentheIOTsensormachineandtheserver.
3. Create a web client and manage adminactivities.
4. Createamobile client forregisteredusers.
5. Set of connectionswiththewebserver.

A. Block chainnetwork:

Certificate Authority(CA)issuesthecertificatesforactorstoauthenticate to the network. Thepeers, orders etc are the active elements provides/use digitalidentities.X.509certificate have the permissions and used in implementation and reorganization of MSPfromaauthorizedsource.

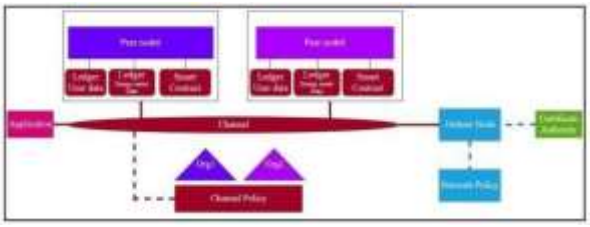


Fig.2.Block chainnetwork

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 linkedchannel. The networkmaintain2ledgersforUser Data and Usagedata.

Asinglesmartcontractwithmultiplefunctionsrunsonpeers.

Webserver:

It is a system program that servesWebpagestothe users.Thewebserverprocessesandprovidesawebpage totheclient.In azurecloudsystemrequirements will change as the size of the block chain changes.The systemrequirementsare 2coreCPU, 4GBMemory, 10GBofHDD/SSD, LinuxbasedOS.Theapplicationisdividedinto UI routes andAPI routes. The API routes start with the path /API.POST,GETforauserID data and dependentontheblock chainmodule. The block chainmodule is packaged as a javascript module and is importedusingRequireJSpattern. All arekeenwith essential javascript constructs and exported as functions.TherespectiveRESTAPIs areprogrammed to switch the queries and chant requests.

B. WebandMobileclient:

Theyfetchtheinformation from the server and provideuserinterface.Mobileapplicationdeveloped. Mobile client can only fetch in sequenceof a exacting user. The Web client is provided with contact toanalysis all users information and also with right to use for creation ofnew users. A User ID for every new user createdtogeneratetransactions.

C. Arduinoclient:

The Node MCU acts as an Arduino client, which reads theenergy meter data through serial port and POSTs this data tothe web server. SDM120M is used as the energy meter whichis capable of measuring the Voltage in Volts(V), current inamperes(A),powerinWatts(W),frequencyinHertz (Hz),energyinKWh,powerfactoretc.oftheconnected load.

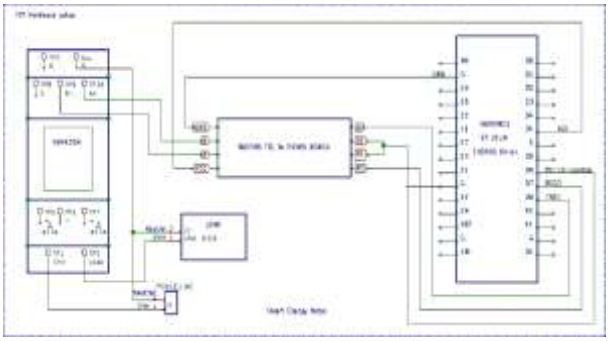


Fig.3.ArduinoClient

SDM120M for reading ofmeasuredvalue.SDM120 with RS485tocommunicatewithsystemsusingtheModbus RTUProtocol.Itusesa MAX485 TTL -RS485 board provides two wayserialcommunicationsignalconversionbetweenth eRS485toTTLandviceversa.

V. RESULTSANDANALYSIS

Transaction details are storedwith V,I,T,F, P and energyalongwithuserID.

Fig.4.Detailsofdatainoneofthetransaction

On observing the transaction records, both peers data have same. So it is decentralizedanddistributed.

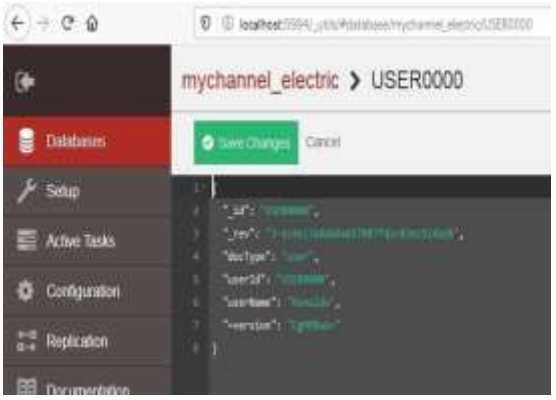


Fig. 5.The detailed transaction record ofUSER0000reflectedinpeer 0ofOrg1

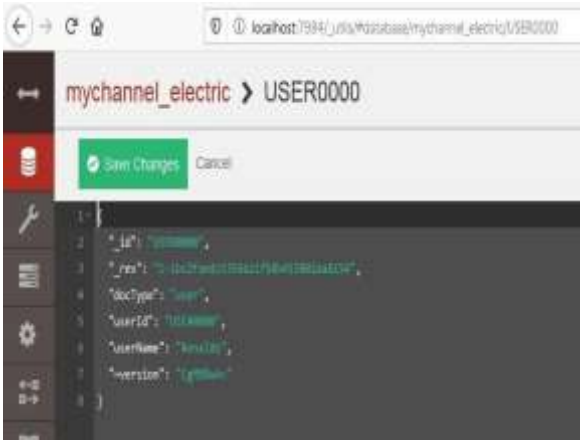


Fig. 6.The detailed transaction record ofUSER0000reflectedinpeer 0ofOrg2

To ensure the safety of information, anybody tamper the peerdata, the originalinformation in another peer,thusprovides the protection of data.

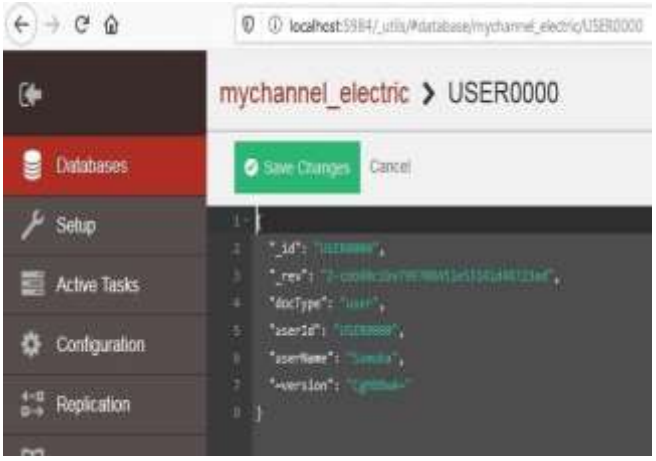


Fig. 7.Transaction details in peer0 of Org 1 aftermodifyingusername.

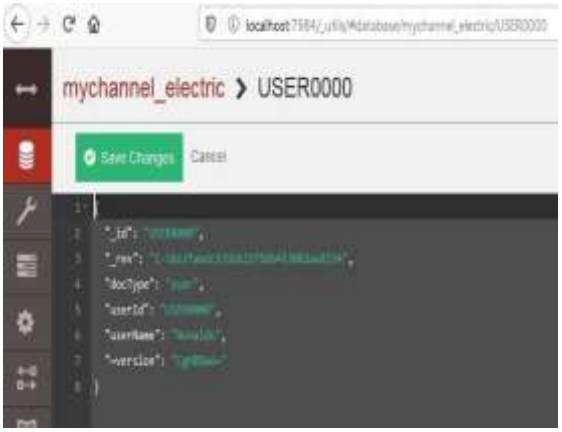


Fig.8.Transactiondetailsinpeer0ofOrg2aftermodifyingusernameinpeer0ofOrg1

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

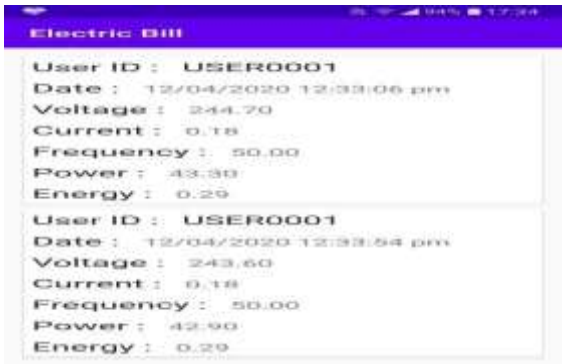


Fig.9.MobileclientsendingaGETrequestandobtainingaresponsefromwebserver

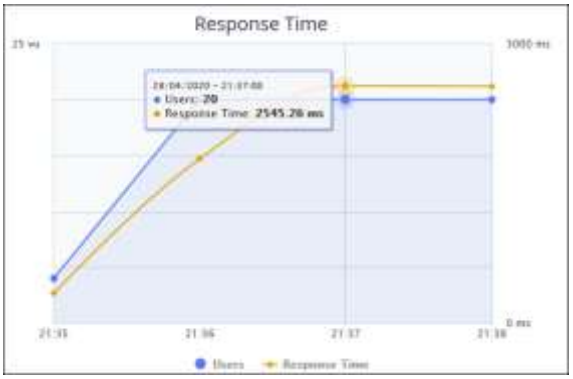
Fig.10.WebClientsendingaGETrequestand obtainingaresponsefromthewebserver.

In block chain heightincreasesaftereachwriteoperation.

Fig.11.block chainhashinformationbeforeup datingtheusagedetailsofUSER00 09

Fig.12.Block chainhashinformationafterup datingtheusagedetailsofUSER 0009

Performanceanalysis: The application wasproduced and examined forperformancebyPOST and GET requests. The performance examined on different platforms.



ig.13.sequentialtestresultsfor100POSTrequests within30secondsusingpostman.

Fig.16.LoadtestgraphforconcurrentGETrequest

Using Blazeter tool

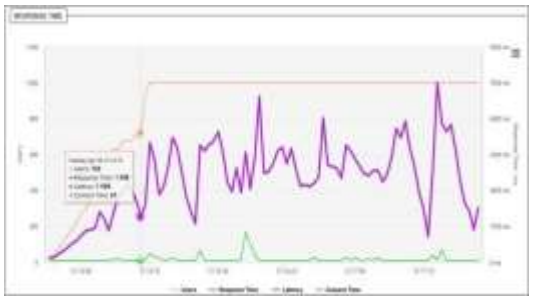


Fig.17.ResponsetimegraphforconcurrentGETrequestusingBlazemetertool

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

CONCLUSIONANDFUTURESCOPE

It provides the visualization of an IOTecosystemf o r trusted and non-trusted parties.The integrity of data is maintained across the ecosystemwithtamper-proofsystem.Theperformance test results shows the normal functioning andusability. 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 thissenddatafromArduino 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 manyIOTdevicesandapplications.

REFERENCES

1. ObaidUr-Rehman,NatasaZivic,ChristophRuland,“ Security issues insmart metering systems”, IEEE International Conference on Smart EnergyGridEngineering(SEGE),2015
2. Pardeep Kumar, Yun Lin ,Guangdong Bai,Andrew Paverd,Jin SongDong ,Andrew Martin, “Smart Grid Metering Networks: A Survey onSecurity,Privacyand Open Research Issues”,IEEE CommunicationsSurveys&Tutorials,Volume:21,Issue:3,2019.
3. MohsinKamal,MuhammadTariq,“Light-WeightSecurityandBlock chain Based Provenance for Advanced Metering Infrastructure”,IEEEAccess (Volume:7),2019,INSPECAccession Number:18826750
4. RuiguoYu,JianrongWang,TianyiXu,JieGao, YongliAn,GongZhang ,MeiYu,“AuthenticationWithBlock-ChainAlgorithmandTextEncryption Protocol in Calculation of Social Network ”, IEEE Access (Volume:5),09November2017
5. DinanFakhri, KusprasaptaMutijarsa, “Secure IoT Communication usingBlock chain Technology”, International Symposium on Electronics andSmart Devices(ISESD), 2018,INSPECAccessionNumber:18374691
6. PinLv,LichengWang,HuijunZhu,WenboDeng ,LizeGu, “AnIOT-OrientedPrivacy-PreservingPublish/SubscribeModelOverBlock chains”,IEEEAccess(Volume:7),march2019 ,INSPECAccessionNumber:18576298
7. Mary Subaja Christo, AnigoMerjora A, ParthaSarathy G, Priyanka C

andRajKumariM,"AnEfficientDataSecurityin Medical Report usingBlock Chain Technology", International Conference on CommunicationandSignalProcessing(ICCSP),2019

8. JinHyeongJeon;Ki-HyungKim;Jai-HoonKim,"Blockchainbaseddata security enhanced IoT server platform", International Conference onInformationNetworking (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,INSPECAccessionNumber:18392665.
10. Chan Hyeok Lee , Ki-Hyung Kim, "Implementation of IoT system usingblockchainwithauthenticationanddataprotection",InternationalConferenceonInformationNetworking(ICOIN),2018,INSPECAccessionNumber:17720922.
11. Han Liu ; Dezhi Han ; Dun Li, "Fabric-iot: A Block chain-Based AccessControlSysteminIoT",IEEEAccess(Volume: 8 Page(s): 18207 – 18218),January2020,ElectronicISSN:2169-3536.
12. Eman-YasserDaraghmi,Yousef-AwwadDaraghmi, Shyan-Ming Yuan,"MedChain: A Design of Block chain-Based System for Medical RecordsAccessandPermissionsManagement",IEEEAccess(Volume: 7,Page(s):164595-164613),November2019,INSPECAccessionNumber: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.html
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 andscalability of private ethereum Block chains", International conference onprocess Management,August2019, OnlineISBN 978-3-030-30429-4