Block pattern Based Information Storage with Security in Internet of Things

[1]Devarajugattu Ravi Kumar,[2]O.Bhulakshmi
Department of CSE
Dr.Samuel George Institute of Engineering& Technology, Markapur,India

Abstract

Block chain allowsusers anddataproviders toensureauthentication, authorizationanddatavaliditywithproper multi-key exchange authentication for user identity and hash key for Blockchain so that the data is not juststored but also validated each time the user access. In this paper, we apply ZeroKnowledge proof to Strong roomsusingRFIDCardreaderandCameramoduleIoTsystemstoprovethataproverwithoutdisclosinginformationsuch aspublic key enhancesthe anonymity ofBlockchain.

Keywords—*IoT;RFID CardReader;BlockChain;Strongroom;ZeroKnowledge Proof*

1. INTRODUCTION

Internet Of Things (IoT) is the extension of internet connectivity into physical devices and everyday objects. Thesedevicescancommunicateandinteractwithothersovertheinternet,andthey canberemotelymonitoredandcontrolled.

The paper introduces Blockchain which is a digital record of transactions. The name comes from the structure, inwhich indivisual transactions/records, called blocks are linked together to asingle list called chain. Blockchainrecords transactions and each transaction added to the Blockchain is validated by multiple consumers. These systemsare configured to monitor specific types of Blockchain transactions, form a peer-peer network. They work together toensure each transaction is valid before it is added to the Blockchain. This decentralized network of computers ensuresasingle systemcannotaddinvalid blockstothe chain.

When a new block is added to the Blockchain, it is linked to the previous blocks using a cryptographic hashgenerated from contents of previous block. This ensures that the chain is never brokenand that each block ispermanentlyrecorded.

2. FRAMEWORKANDARCHITECTURE

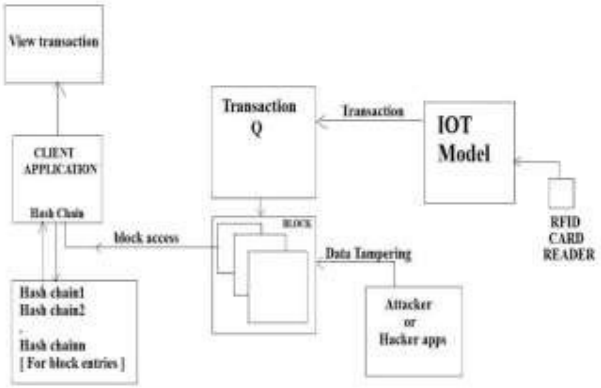


Figure1:ArchitectureDiagram

ThemainpurposeofBlockchaintechnologyistosecurethedigitalidentityreference.TheconceptofBlockchain in the existing system is that the data obtained from the IoT model gets stored in the server andauthenticated user can keep track of transactions, where the data might get tampered. The proposed system is insuchawaythat,ifthedatais manipulated,thesystemnotifiesthattheparticular datahasbeen modified.

The proposed system contains three modules: IoT, Blockchain Server and Client Application. We have takenthe environment of strong room in police station. Smart cards will be given to few authorized staffs working inpolice station, and when the person swipes card to enter into the strong room, the RFID Card reader scans thevalue of that particular card swiped by the person, and the camera fixed at a place captures the image of theperson swiping the card. The “RFID tag+image” is a transaction which gets stored in the Blockchain

ledger.Client on theotherhand,toview thetransaction,shouldget registeredtotheBlockchainserverinitially.During the registration, Blockchain server shares a secret key to the client on request by encrypting it with thepublic key by providing the private key. Once the client gets registered and obtains the private key from theBlockchain, that client is said to have been authenticated and authorized. Again, when the client wants to viewtransactions, he has to regenerate the shared secret by encrypting it with the private key. Blockchain, uponreceiving, decrypts it with the public key and checks if the shared secret key is the same given to the clientwhileregistering.Oncethecombinationofthesecretkeyisfoundtohavebeenthesame,Blockchainconcludes that the client is an authorized person and allows the recent transaction to move to the respective userblocks. Oncethe transactionmoves touserblocks, thatparticulartransactionwill be removedfrom theBlockchain ledger, hence no security breach and data tampering. In order to check the security breach, a hackerapplicationhasbeendevelopedwherein,whenahackermodifiesthetransactions,thenthatparticulartransactioni sviewedasa "bug"iconintheuserblock.

2.1 InnovationsPresentedinthe Project

1. Zero Knowledge proof is applied to Strong room utilizing RFID Smart card and camera to prevent dataforgeryandpersonal informationinfringement.
2. Block chain handles transactions carried inside the strong room and stores each transaction in a blockchainledgerfor privacyprotection.
3. Block chain also stores symmetric keys inside the server and these keys are not distributed to users whoviewthe dataandhence securityispreserved.
4. Whenever a user needs to view data he must be registered in prior to the Block chain server so that onlyauthorized user has access to the transactions, and he can view the data by keys generated by the Blockchain.
5. Ahackerapplicationhasbeendevelopedtocheckifthedatahasbeenmodifiedbyusingfalsetimestamp,and ifany modifications, willbenotified intheuserblocksbya"bug"iconandreported.

2.2 DeviceAuthenticationandDataTransmission

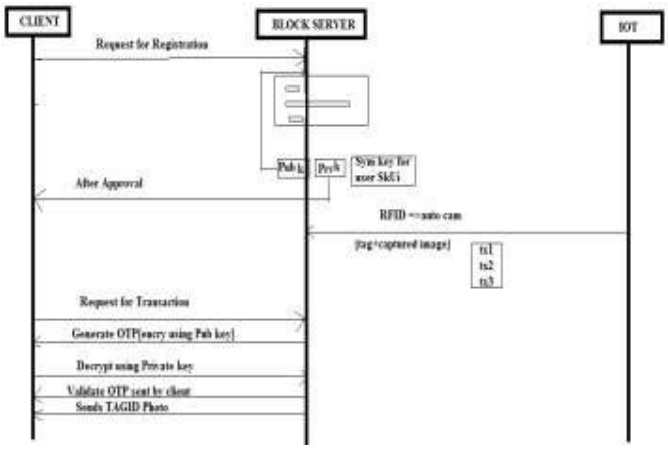


Figure2:SequenceDiagram

IoT Model stores the transactions i.e, RFID Card Reader as well as image captured by the camera in a queueand sends those transactions to the Blockchain ledger. Client need to be registered to the Blockchain serverfirst, in order to seek transactions. Blockchain contains multi-key i.e, Private key, Public key and Secret key.During clientregistration,privatekeyalongwiththesecretkeyisgiventotheclient.Publickeyisretainedin theBlockchain only. Once the registration is done, the client can request for the recent transactions. Requestfor the data view involves regeneration of the shared secret key using the private key and sent to the server.Andthe Blockchainshouldcheck if the secretkey is the same thathadbeen senttothe clientwhileregistering. If the secret key is the same, then that particular client is said to have registered to the server andfound to be authorized.And the recent transactions are sent to user blocks where only the authenticated usercan view. And as soon as the transaction is moved to blocks, that particular block will be removed from theledger inorderto preventthe securitybreachanddata tampering.

3. IMPLEMENTATION

Blockchain allow the users and data provider to ensure authentication, authorization and data validity withproper multiple key exchange authentication for user identity and hash key for block chain data validation sothatdata is notjuststoredbutalsovalidated eachtimewhenuser access.

3.1 SnapshotsoftheProject

Snapshot1:ClientRegistrationPage

The above snapshot depicts the user registerationpage , where the user sends the request to the block chainserver fromclientapplicationtogetregistered.

Snapshot2:ConfirmingtheUserRequest

The below snapshot depits the User request approval page where the request is sent to the server. The systemautomaticallyfetchesthe MacId, Username,Date and time.

Snapshot3:Confirmationoftherequestsent

The above snapshot depicts the confirmation of the request sent by the client application, The message ispopped saying that " Request sent successfully to the authentication server". The request is sent to the blockchain server.

Snapshot4: UserApprovalscreen intheBlockchainPage

TheabovesnapshotdepictstheUserapprovalscreenintheblockchainapplication,wheretherequestsentbytheclientneedst obe approvedor reject.

Snapshot5: RequestApprovalscreenoftheBlockchainadmin

TheabovesnapshotdepictstheRequestapprovalscreenintheblockchainapplication, wherethelistofrequestsentbythe clientisapproved/rejectedhere.

Snapshot6:CertificateApprovalscreen

Theabovesnapshotdepictsthecheckstatusscreen,whereitalsoincludestheencryptedcertificateoption,itcanbe shownonly whenthe statusisapprovedbythe blockchainserver.

Snapshot7: SwipingofRFIDcardagainsttheRFIDCardreader

Theabovesnapshotdepictstheswippingof RFIDcardintothearudinoboard,scansthecardnumberwiththecomportused.

Snapshot8: Atransaction

Scanningthecardvalueaswellascapturesliveimagecapturedwhenthecardisswipedagainst an Iotmodule(RFIDCardreader) and the transactionissaved successfully.

Snapshot9: RequestformfortheRecentTransaction

The above snapshot depicts the Request form for the Recent Transaction, when the client request the server fortherecenttranaction.

Snapshot10: BlockchainserverPagetoallowthetransactionstomovetouserblocks.

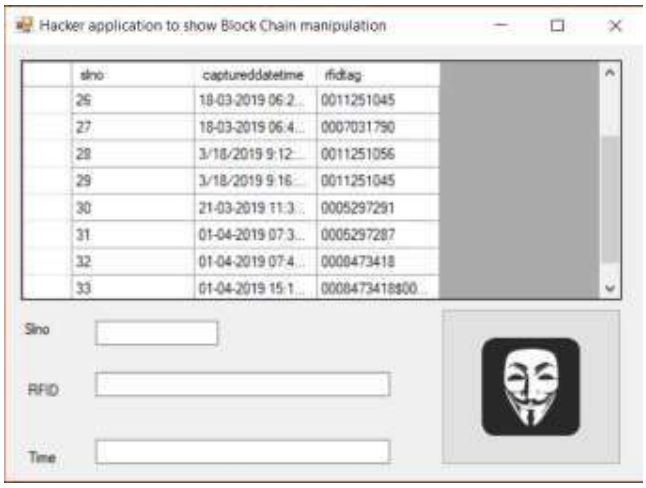
Blockchainacceptstherequestfromtheclientandrequeststheclienttodecrypt thesecret keyusingtheprivatekey.

Snapshot11: Checksthesecretkeyandmovestransactions

Theabovesnapshotdepictsthecheckingofsecretkeyandthemovementofthetransactions,heretherecenttransactionismovedtouserblocks.

Snapshot12: Transactionstoredinuserblocks

OncetheBlockchainfindsthattheclientisauthorized,itallowstransactionstomovetorespectiveuserblocks.



Snapshot13: Hackerapplication

Theabovesnapshotdepictsthehackerapplication,whereinahackercanmodifyanytransactionstoredintheuser blocks.

Snapshot14: ViewoftheHackeddetails

Anytransactionmodificationcanbeeasilyidentifiedinuserblocksthroughthe“bug”iconandcanbereported.Blockchainhe nce, allowsclientstoidentifythedata tamperingso nosecuritybreach.

4. CONCLUSION

The project propose strong room using Zero-knowledge proof to protect data. IoT data is stored in the blockchain, which can prevent IoT device authentication and data tampering. RFID card monitors themodificationofthedata and thetheftthrough blockchainbecauseoftheproblems suchasforgeryand alterationofdata.

5. REFERENCES

[1] Gungor,V.Cagri,etal."Asurveyonsmartcardpotentialapplicationsandcommunicationrequirements."IndustrialI nformatics, Vol.9, No.1, 2013,pp.28-42.

[2] Gangale, Flavia,AnnaMengolini, andIjeomaOnyeji., "Consumerengagement:Aninsight fromsmart cardprojectsinEurope.",EnergyPolicy, Vol.60, 2013,pp.621-628.

[3] Luan,Shang-Wen,etal."DevelopmentofasmartpowercardforAMIbasedonZigBeecommunication",PowerElectronicsand DriveSystems,2009.PEDS2009.InternationalConferenceon.IEEE,2009.

[4] CommonCriteriaforInformationTechnologySecurityEvaluation,Version3.1,CCMB,Setp.2006.

[5] Youngu Lee, A Study for PKI Based Home Network SystemAuthenticationandAccessControlProtocol,KICS'10-

04Vol.35No.4

[6] Kepco,ProsumerPowerTrading,http://home.kepco.co.kr

[7] AndreasM,MasteingBitcoin: UnlockingDigitalCryptocurrencies,pp.49-68,O'REILLY,2015

[8] Sung-HoonLee, DeviceauthenticationinSmartcardSystemusingBlockchain,KAIST,2016.

[9] SatoshiNakamoto,Bitcoin:APeer-to-PeerElectronicCashSystem,2008.

[10] NickSzabo,Smart Contracts, 1994.

[11] NickSzabo,TheIdeaofSmartContracts,1997.

[12] TheCointelegraph, ABriefHistoryofEthereumFromVitalik

[13] Buterin'sIdeatoRelease, 2015

[14] Jean-JacquesQuisquater,HowtoExplainZero-Knowledge ProtocolstoYourChildren,1989.

[15] KETI,MobiusIoT serverplatform,http://iotocean.com

[16] RyanCheu,AnImplementationofZeroKnowledgeAuthentication,2014

[17] EliBen-Sasson,Zerocash:Decentralized AnonymousPaymentsfromBitcoin,2014

[18] SuraeNoether,ReviewofCtyptonoteWhitePaper,2016

[19] CharlesRackoffDanielR.Simon,Non-InteractiveZero-KnowledgeProofofKnowledgeandChosenCiphertextAttack,AnnualInternationalCryptologyConference,1991

[20] EvanDuffield,DanielDiaz,Dash: APrivacy-CentricCrypto-Currency,2015.

Student details: Devarajugattu Ravi Kumar

Mail id: ravi.sharann@gmail.com

College :Dr.Samuel George Institute of Engineering & Technology, Markapur,PrakasamDistrict,Andhra Pradesh, India

Guide details:

O.Bhulakshmi received B.Tech (CSE) Degree from JNTUK Kakinada in 2012 and M.Tech (CSE) Degree from JNTUK Kakinada in 2016. She has 3 years of teaching experience. She joined as an Assistant Professor in Dr.Samuel George Institute of Engineering & Technology, Markapur,PrakasamDistrict,Andhra Pradesh, India in 2019. Presently she is working as Assistant Professor in CSE Dept. Her Interesting research areas are Image Processing and Computer Networks.She Attended Various National Workshops.