Implementation of IoT System using BlockChain with Authentication and Data Protection

Sumana Bhat N M, Chaya P, Ashwini H C, Chithra S, Vaibhavi R

Department of ISE, GSSSIETW,mysuru

Abstract

Blockchain allows users and data providers to ensure authentication, authorization and data validity with proper multi-key exchange authentication for user identity and hash key for Blockchain so that the data is not just stored but also validated each time the user access. In this paper, we apply ZeroKnowledge proof to a Strong rooms using RFID Card reader and Camera module IoT systems to prove that a prover without disclosing information such as public key enhances the anonymity of Blockchain.

Keywords— *IoT; RFID Card Reader; Block Chain; Strong room; Zero Knowledge Proof*

1. INTRODUCTION

Internet Of Things (IoT) is the extension of internet connectivity into physical devices and everyday objects. These devices can communicate and interact with others over the internet, and they can be remotely monitored and controlled.

The paper introduces Blockchain which is a digital record of transactions. The name comes from the structure, in which indivisual transactions/records, called blocks are linked together to a single list called chain. Blockchain records transactions and each transaction added to the Blockchain is validated by multiple consumers. These systems are configured to monitor specific types of Blockchain transactions, form a peer-peer network. They work together to ensure each transaction is valid before it is added to the Blockchain. This decentralized network of computers ensures a single system cannot add invalid blocks to the chain.

When a new block is added to the Blockchain, it is linked to the previous blocks using a cryptographic hash generated from contents of previous block. This ensures that the chain is never broken and that each block is permanently recorded.

2. EARLY STAGE IDEAS FOR RESEARCH PAPER

[1] Gungor, V. Cagri, et al. "Block Chain Based Data Security Enhanced IoT Server Platform" Industrial Informatics, Vol.9, No.1, 2013, pp. 28-42.

The paper discuss about the Mobius MySQL platform and the storage of the sensor data. It also discuss about the configuration vulnerabilities and threats to security.

[2] Gangale, Flavia, Anna Mengolini, and IjeomaOnyeji., "The Use of Authentication Technology Blockchain Platform for the Marine Industry ", Energy Policy, Vol.60, 2013, pp.621-628.

The paper discuss about the combination of digital identities based on the blockchain which will allow to create automated security systems.

[3] Luan, Shang-Wen, et al, "Secured Data Storage Scheme Based On Blockchain for Agricultural Products Tracking" 2009. PEDS 2009. International Conference on. IEEE, 2009.

The paper ensures that the data of agricultural products is not maliciously tampered and destructed and enhances the anonymity of the Blockchain.

[4] Andreas "A Privacy-preserving Cross- organizational Authentication/ Authorization /Accounting System using Blockchain Technology", 2015.

The paper describes One-way hash chain which enforces the concept of one-time pad password, which can provide the unlinkability merit and also deals with accounting and unlinkability issues.

[5] Joseph A, "Variable Block-Size Image Authentication with Localization and Self Recovery" pp.49-68, O'REILLY, 2015.

The paper discuss about the image authentication and provides Attack localization which is less complexity.

[6] Prakash M Mainkar, Shreekant Ghorpade, "Secure Authentication For Data Protection In Cloud Computing Using Color Schemes" , 2015.

The paper discuss about the secured preprocessing and data segmentation by quick analysis of authentication thereby decreasing the complexity of users.

[7] Nicola Fabiano, "Internet of Things and Blockchain: legal issues and privacy", 2015.

The paper describes the low complexity data processing techniques which is installed on the mobile phone. The data processing technique is developed in a network, which operates in multiple levels.

[8] Dhananjay Sampath, "Strengthening Protocol For Wireless Networks Using Block Chaining With Variable Encrypting Function Mechanism", 2016.

A Classification system is presented that stores a 5-class classification. The 5 classes represent a data class and 4-storage classes. Security class is assigned one is the data class and 5 is the severely protected.

[9] Basin Sutticharya, Pattarasinee Bhattarakosol, "Chain Rule Protection Over the Internet using PUGGAD Algorithm", 2016.

The paper describes about the PUGGAD Algorithm where in hackers cannot decrypt back to the original plaintext.

[10] Less Stuurman, Irene Kanara, " IoT Standardization: The Approach In The Field of Data Protection as a Model for Ensuring Compliance of IoT Applications", 2017.

The paper provides the additional safeguard in ensuring adequate legal protection. The existing approach being the dominant regulatory model for applying standards in relation to EU product legislation has been criticized for lacking legitimacy of standard-setting procedures and lacking judicial review.

3. FRAMEWORK AND ARCHITECTURE

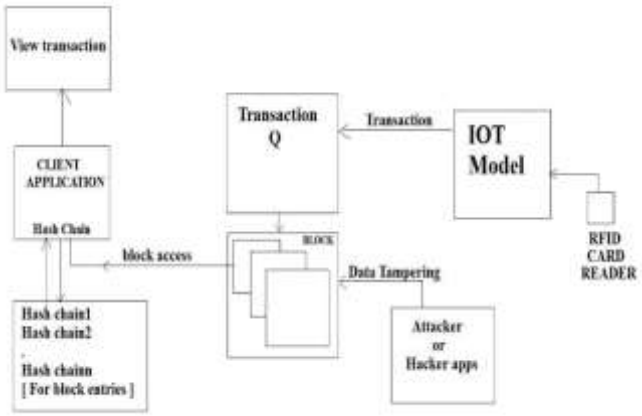


Figure 1: Architecture Diagram

The main purpose of Blockchain technology is to secure the digital identity reference. The concept of Blockchain in the existing system is that the data obtained from the IoT model gets stored in the server and authenticated user can keep track of transactions, where the data might get tampered. The proposed system is in such a way that, if the data is manipulated, the system notifies that the particular data has been modified.

The proposed system contains three modules: IoT, Blockchain Server and Client Application. We have taken the environment of strong room in police station. Smart cards will be given to few authorized staffs working in police station, and when the person swipes card to enter into the strong room, the RFID Card reader scans the value of that particular card swiped by the person, and the camera fixed at a place captures the image of the person swiping the card. The "RFID tag+image" is a transaction which gets stored in the Blockchain ledger. Client on the other hand, to view the transaction, should get registered to the Blockchain server initially. During the registration, Blockchain server shares a secret key to the client on request by encrypting it with the public key by providing the private key. Once the client gets registered and obtains the private key from the Blockchain, that client is said to have been authenticated and authorized. Again, when the client wants to view transactions, he has to regenerate the shared secret by encrypting it with the private key. Blockchain, upon receiving, decrypts it with the public key and checks if the shared secret key is the same given to the client while registering. Once the combination of the secret key is found to have been the same, Blockchain concludes that the client is an authorized person and allows the recent transaction to move to the respective user blocks. Once the transaction moves to user blocks, that particular transaction will be removed from the Blockchain ledger, hence no security breach and data tampering. In order to check the security breach, a hacker application has been developed where in, when a hacker modifies the transactions, then that particular transaction is viewed as a "bug" icon in the user block.

3.1 Innovations Presented in the Project

1. Zero Knowledge proof is applied to Strong room utilizing RFID Smart card and camera to prevent data forgery and personal information infringement.
2. Block chain handles transactions carried inside the strong room and stores each transaction in a block chain ledger for privacy protection.
3. Block chain also stores symmetric keys inside the server and these keys are not distributed to users who view the data and hence security is preserved.
4. Whenever a user needs to view data he must be registered in prior to the Block chain server so that only authorized user has access to the transactions, and he can view the data by keys generated by the Block chain.
5. A hacker application has been developed to check if the data has been modified by using false timestamp, and if any modifications, will be notified in the user blocks by a "bug" icon and reported.

3.2 Device Authentication and Data Transmission

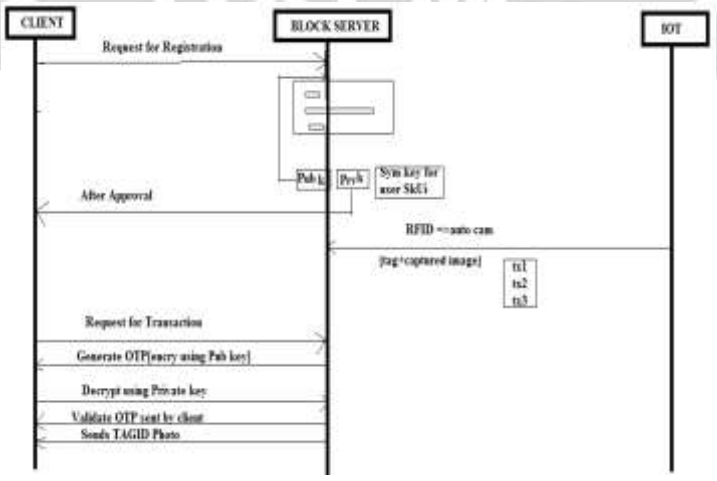


Figure 2: Sequence Diagram

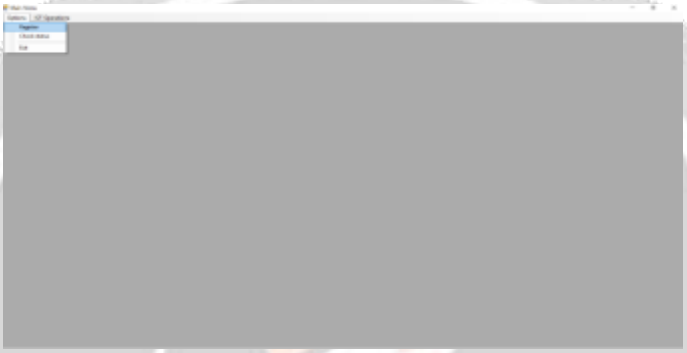
IoT Model stores the transactions i.e, RFID Card Reader as well as image captured by the camera in a queue and sends those transactions to the Blockchain ledger. Client need to be registered to the Blockchain server first, in order to seek transactions. Blockchain contains multi-key i.e, Private key, Public key and Secret key. During client registration, private key along with the secret key is given to the client. Public key is retained in

the Blockchain only. Once the registration is done, the client can request for the recent transactions. Request for the data view involves regeneration of the shared secret key using the private key and sent to the server. And the Blockchain should check if the secret key is the same that had been sent to the client while registering. If the secret key is the same, then that particular client is said to have registered to the server and found to be authorized. And the recent transactions are sent to user blocks where only the authenticated user can view. And as soon as the transaction is moved to blocks, that particular block will be removed from the ledger in order to prevent the security breach and data tampering.

4. IMPLEMENTATION

Blockchain allow the users and data provider to ensure authentication, authorization and data validity with proper multiple key exchange authentication for user identity and hash key for block chain data validation so that data is not just stored but also validated each time when user access.

4.1 Snapshots of the Project



Snapshot 1: Client Registration Page

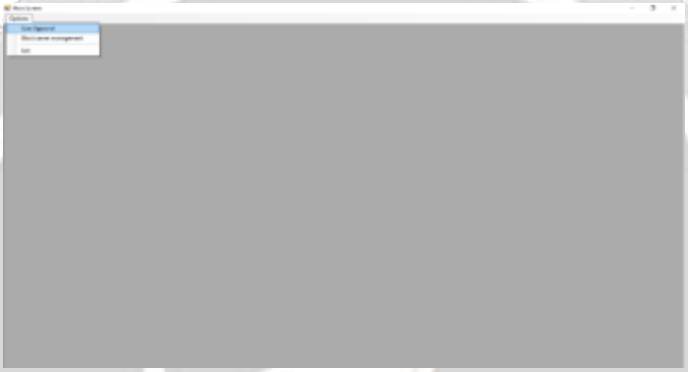
The above snapshot depicts the user registeration page , where the user sends the request to the block chain server from client application to get registered.

Snapshot 2: Confirming the User Request

The below snapshot depits the User request approval page where the request is sent to the server. The system automatically fetches the Mac Id, Username, Date and time.

Snapshot 3: Confirmation of the request sent

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



Snapshot 4: User Approval screen in the Blockchain Page

The above snapshot depicts the User approval screen in the block chain application, where the request sent by the client needs to be approved or reject.

Snapshot 5: Request Approval screen of the Blockchain admin

The above snapshot depicts the Request approval screen in the block chain application, where the list of request sent by the client is approved/rejected here.

Snapshot 6: Certificate Approval screen

The above snapshot depicts the check status screen, where it also includes the encrypted certificate option, it can be shown only when the status is approved by the block chain server.

Snapshot 7: Swiping of RFID card against the RFID Card reader

The above snapshot depicts the swipping of RFID card into the arudino board , scans the card number with the com port used.

Snapshot 8: A transaction

Scanning the card value as well as captures live image captured when the card is swiped against an Iot module (RFID Card reader) and the transaction is saved successfully.

Snapshot 9: Request form for the Recent Transaction

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

Snapshot 10: Blockchain server Page to allow the transactions to move to user blocks.

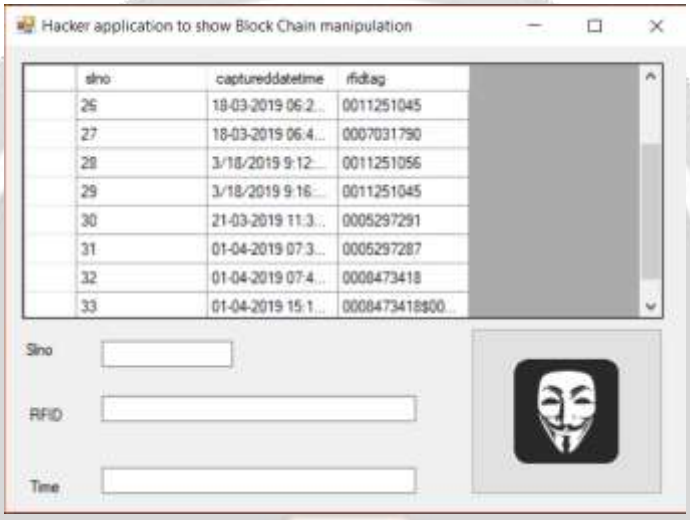
Blockchain accepts the request from the client and requests the client to decrypt the secret key using the private key.

Snapshot 11: Checks the secret key and moves transactions

The above snapshot depicts the checking of secret key and the movement of the transactions, here the recent transaction is moved to user blocks.

Snapshot 12: Transaction stored in user blocks

Once the Blockchain finds that the client is authorized, it allows transactions to move to respective user blocks.



Snapshot 13: Hacker application

The above snapshot depicts the hacker application, where in a hacker can modify any transaction stored in the user blocks.

Snapshot 14: View of the Hacked details

Any transaction modification can be easily identified in user blocks through the "bug" icon and can be reported. Blockchain hence, allows clients to identify the data tampering so no security breach.

5. CONCLUSION

The project propose strong room using Zero-knowledge proof to protect data. IoT data is stored in the block chain, which can prevent IoT device authentication and data tampering. RFID card monitors the modification of the data and the theft through block chain because of the problems such as forgery and alteration of data.

6. REFERENCES

[1] Gungor, V. Cagri, et al. "A survey on smart card potential applications and communication requirements." Industrial Informatics, Vol.9, No.1, 2013, pp. 28-42.

[2] Gangale, Flavia, Anna Mengolini, and Ijeoma Onyeji., "Consumer engagement: An insight from smart card projects in Europe.", Energy Policy, Vol.60, 2013, pp.621-628.

[3] Luan, Shang-Wen, et al. "Development of a smart power card for AMI based on ZigBee communication", Power Electronics and Drive Systems, 2009. PEDS 2009. International Conference on. IEEE, 2009.

[4] Common Criteria for Information Technology Security Evaluation, Version3.1, CCMB, Setp.2006.

[5] Youngu Lee, A Study for PKI Based Home Network System
Authentication and Access Control Protocol, KICS '10-04Vol.35No.4

[6] Kepco, Prosumer Power Trading, http://home.kepco.co.kr

[7] Andreas M, Masteing Bitcoin: Unlocking Digital Cryptocurrencies, pp.49-68, O'REILLY, 2015

[8] Sung-Hoon Lee, Device authentication in Smart card System using Blockchain, KAIST, 2016.

[9] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.

[10] Nick Szabo, Smart Contracts, 1994.

[11] Nick Szabo, The Idea of Smart Contracts, 1997.

[12] The Cointelegraph, A Brief History of Ethereum From Vitalik

[13] Buterin's Idea to Release, 2015

[14] Jean-Jacques Quisquater, How to Explain Zero-Knowledge Protocols to Your Children, 1989.

[15] KETI, Mobius IoT server platform, http://iotocean.com

[16] Ryan Cheu, An Implementation of Zero Knowledge Authentication, 2014

[17] Eli Ben-Sasson, Zerocash: Decentralized Anonymous Payments from Bitcoin, 2014

[18] Surae Noether, Review of Ctyptonote White Paper, 2016

[19] Charles RackoffDaniel R. Simon, Non-Interactive Zero-Knowledge Proof of Knowledge and Chosen Ciphertext Attack, Annual International Cryptology Conference, 1991

[20] Evan Duffield,Daniel Diaz ,Dash: A Privacy-Centric Crypto-Currency, 2015.