

Blockchain Authentication and Data Protection for IoT Systems

Mahdi Mohammad Abdullah Al Momani¹ & Dr. P S Puttaswamy²

¹Research Scholar, PET Research Center, Mandya

²Prof. and Head, Adichunchagiri University, B G Nagar, Bellur

ABSTRACT

The growing applications of the Internet of Things lead to a constant rise in cyberattacks across the board. Identity management is one of the most common attack vectors since it enables impersonation and bypasses existing trusted procedures. The weak identity management approach undermines any attempt to create safe systems because identity is fundamental to every security mechanism, including authentication and access control. Although digital certificates are the most popular methods for authentication and identification, their widespread distribution is still unresolved. The procedure includes identity and key provision for devices which is typically a laborious undertaking. The human-made configuration might have mistakes and are frequently the root for many security and privacy problems. This operation should be made semi-autonomous to reduce incorrect setups while performing it. With suitable multi-key exchange authentication for user identification and a blockchain hash key, both the user and data providers can be ensure with authentication, authorization, and data validity so that the data is stored and validated each time when a user accesses it. This paper aims to demonstrate the implementation to prove that without releasing information like the public key there is a possibility of enhancing the anonymity of Blockchain by using Zero Knowledge proof to IoT systems.

Keywords: Internet of Things, Blockchain, authentication, secure communications

INTRODUCTION

The Internet of Things (IoT) extends internet connectivity with number of physical devices and with every object. The various devices are able to communicate and interact with others over the internet, and they can be remotely monitored and controlled. The present paper introduces the Blockchain concept, which is a digital record of transactions. The name comes from the structure

in which individual transactions/records, called as blocks which are linked to a single chain, together called as Blockchain. The Blockchain records transactions where each transactions added to the Blockchain is validated by multiple consumers. These systems are configured to monitor specific Blockchain transactions and to form a peer-peer network. They work together to ensure each transaction whether it is valid or not before it is added to the Blockchain. The decentralized network of computers provides a single system that 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 the contents of the previous block. This ensures that the chain is never broken and also each block is recorded properly.

IoT enables the devices across Internet to send data to private blockchain networks to create tamper-resistant records of shared transactions. Each IoT node can be registered and authenticated in the Blockchain network and they will have a unique ID and address, thus, it will help in the unique identification of the device. If any device that wants to connect with another device then it has to use its unique blockchain ID and local blockchain wallet to raise the request. IBM Blockchain allows the business partners to share and access IoT data without central control and management. Using a decentralized ledger to store data on IoT device that helps the enterprises to build secured information, thereby reducing the costs associated with IoT device maintenance, data transfer and data management.

1.1 IoT and its Security Challenges: IoT devices are becoming increasingly popular due to their ability to collect and analyze large amount of data. However, as the number of IoT device increase then the security challenges also increases. One of the most significant challenge is the authentication to access the network. For this purpose the IoT devices needs to verify the identity of all other devices with which they interact, and also to ensure that the data exchanged is genuine and has not got tampered. Additionally, since IoT devices stores the sensitive data, there is a need to ensure that the data is protected from unauthorized access.

1.2 Blockchain and its Potential in IoT

Blockchain technology is the recent technology which is a decentralized and distributed ledger which can be used to store and verify transactions. It has a unique structure that ensures data integrity, immutability, and transparency, thereby making it an excellent candidate for securing the IoT devices. The implementation of blockchain system in IoT does provides the scope for

authentication process automation, so that the data can be securely stored, shared, and accessed by only authorized parties.

The implementation of blockchain in IoT can also provide a more efficient way of handling transactions between the devices. In traditional centralized system, the authentication process is typically slow and resource-intensive. However, the use of blockchain technology makes the authentication process automated, thereby reducing the need for human intervention.

1.2.1 Authentication and Data Protection using Blockchain

To implement blockchain concept in IoT there is a need to create a network of nodes where each node has a copy of the blockchain. In this method each node is individually mainly responsible for validating and verifying transactions and also ensuring that they are legitimate and are not being tampered. When the new device wants to join the network, it needs to be authenticated and authorized by the other associated nodes of the network. Once the device is authenticated, then it can communicate with other devices on the network and data can be exchanged securely.

In blockchain-based IoT system, data is always stored on the blockchain, making it immutable and transparent. The data is encrypted and only authorized parties can be able to access it. The use of blockchain ensures that any changes made to the data are recorded on the ledger, thus making it easy to track and trace any changes.

1.2.2 Authentication and Authorization:

The network consists of three layers, they are device, gateway and cloud. The Blockchain technology is employed at the gateway layer where the data is stored and exchanged in the form of blocks of chain to support decentralization and overcome the problem of traditional centralized architecture.

Authentication and authorization are two vital information essential for security process where the administrators make use of them to protect the system and information. Authentication process verifies the user's or service's identity, determine authorization access rights. Authorization is a process by which a server determines the client has permission or not to use a resource or access a file. Authorization is usually coupled with authentication, where the server has a concept of the client request for the access. The authentication and authorization process is shown in Figure 1.

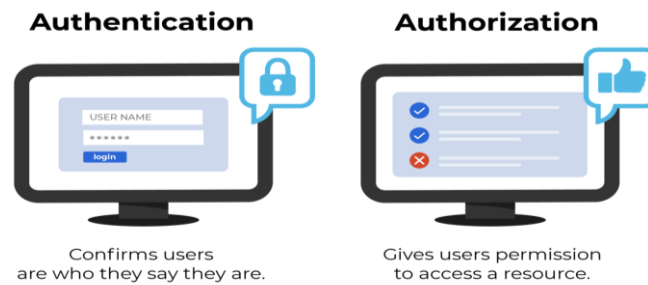


Figure 1: Authentication and Authorization

IoT system comprises of four basic building blocks and they are sensors, processors, gateways and applications. However, the complete IoT systems are also same in the way where they represent the integration of four distinct components such as sensors/devices, connectivity, data processing, and a user interface. The strong IoT device authentication is required to ensure the connected devices on the IoT that can be trusted for what they purport to be. Consequently, each IoT device needs a unique identity that can be authenticated when the device attempts to connect the gateway or central server. IT professionals are able to choose from many IoT authentication methods, including digital certificates, two-factor or token-based authentication, hardware root of trust (RoT), and trusted execution environment (TEE). Authentication factors can be classified into three groups: which may be something like a password or personal identification number (PIN), a token, bank card and biometrics, such as fingerprints and voice recognition. The authentication process involved is shown in Figure 2.

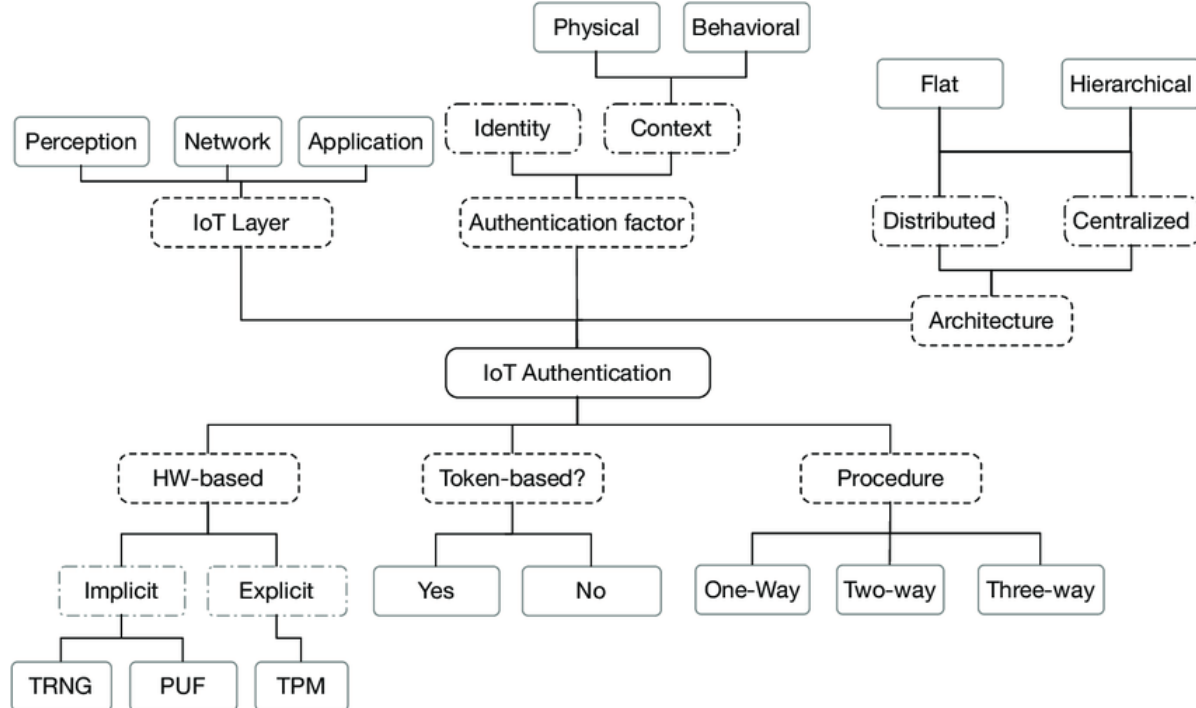


Figure 2: Schematic block diagram for IoT authentication

For IoT safety, the use of Blockchain can monitor the information collected by the sensors without allowing them to be duplicated by any wrong data. The Sensors can transfer data using Blockchain technology without needing a trusted third party.

The implementation of blockchain in IoT can provide a secure and efficient solution to the challenges of authentication and data protection. By creating a network of nodes and storing data on the blockchain, IoT devices can communicate and exchange data securely. Blockchain technology provides a decentralized and immutable ledger, ensuring data integrity and transparency. With the increasing number of IoT devices, the need for better security and data protection is more critical than ever. Implementation of a blockchain-based system can help to overcome these challenges and provide a more secure and efficient IoT ecosystem.

1.3 Proposed System

The proposed system contains three modules such as IoT, Blockchain Server and a Client application. Here, it is considered with the environment something like strong room in the police station. The Smart cards will be given to a few selected authorized staff working in the police station for their use. When the person swipes a card to enter the strong room then RFID Card

reader scans the value of that particular card, 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. The Clients, on the other hand in order to view the transaction for which they should get registered to the Blockchain server initially. During the registration, the Blockchain server shares a secret key with the client on request by encrypting it with the public key and share the private key. Once the client gets registered and obtains the private key from the Blockchain then 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. The Blockchain after receiving it decrypts with the public key and checks for the shared secret key which is same as the one given to the client while registering. Once the combination of the secret key is found to have been matched then 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 then that particular transaction will be removed from the Blockchain ledger, hence no security breach and data tampering will take place. In order to check the security breach the hacker application has been developed for, when a hacker modifies the transactions, then that particular transaction is viewed as a “bug” icon in the user block. This helps to provide better security.

1.4 System Requirements

In order to implement the secured authentication and authorization, the following components are required and are mentioned below

- (i) **A computer or laptop:** A computer or laptop with a processor Intel core i5 or equivalent with RAM 4 GB or higher, with a suitable operating system.
- (ii) **Blockchain Development Platform:** A blockchain development platform such as Ethereum, Hyperledger Fabric, or Corda is necessary to create a blockchain-based IoT system.
- (iii) **IoT hardware:** IoT devices such as sensors, actuators and gateways are necessary to connect to the blockchain-based system and exchange data securely.
- (iv) **IoT software:** IoT software such as firmware, operating systems and communication protocols are necessary to interact with the IoT hardware and connect it to the blockchain-based system.

- (v) **Authentication protocols:** Authentication protocols such as Public Key Infrastructure (PKI) and digital certificates are necessary to authenticate new devices joining the blockchain-based system.
- (vi) **Encryption software:** Encryption software such as AES, RSA, or Elliptic Curve Cryptography (ECC) is necessary to encrypt data exchanged between IoT devices and the blockchain-based system.
- (vii) **Development tools:** Development tools such as Integrated Development Environment (IDE) and software libraries are necessary to develop the blockchain-based system and IoT software.
- (viii) **Cloud infrastructure:** Cloud infrastructure such as Amazon Web Services (AWS), Google Cloud Platform (GCP), or Microsoft Azure is necessary to host and deploy the blockchain-based IoT system.
- (ix) **Testing tools:** Testing tools such as JMeter or Postman are necessary to test the functionality and performance of the blockchain-based IoT system.
- (x) **Security tools:** Security tools such as firewalls, intrusion detection, prevention systems and anti-malware software are necessary to protect the blockchain-based IoT system from cyber attacks.

It is also noted that the specific technology requirements may vary depending on the scope and complexity of the blockchain-based IoT system and the use case.

1.5 System Design and Architecture

The architectural design of the system used in the present study is shown in Figure 3 and its operation is explained in brief.

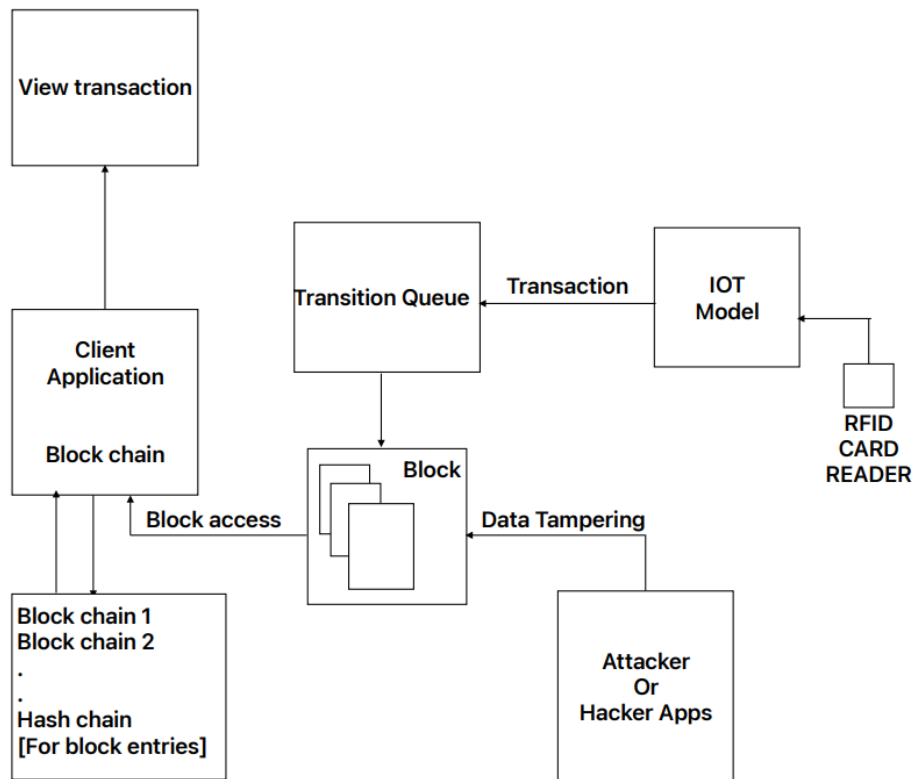


Figure 3: Architecture Diagram

The primary 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 users can keep track of transactions where the data might get tampered with it. The proposed system is in such a way that if the data is manipulated then the system capable of notifying the particular data that has been modified.

The functional requirements of **Blockchain Authentication and Data Protection** for IoT System includes the following steps and are explained below:

- (i) **Registration:** The first is that the client should register with the Blockchain server to view the transactions.
- (ii) **Approval/Rejection:** Blockchain server management gets recent client requests for registration, approval or rejection.
- (iii) **Transaction:** Only for few of the users will be given smart cards that they have to swipe the card in order to enter the strong room. As soon as they swipe, the value of the

smart card is swiped and the image is captured and then the tag ID + Image both are considered as a transaction.

- (iv) **Request for the data:** Clients who are already registered with the Blockchain server can request the server to send the recent transaction.
- (v) **Accept Request:** As soon as the client requests the Blockchain for transactions, then user gets the transactions from the transaction queue also gets the key from the key mapping module and then encrypts the transaction using the key and stores back the encrypted data in the Blockchain.
- (vi) **Transaction View:** The Blockchain verifies for the authorized client, if it finds they are authorized and moves the transaction to user blocks where the user can view recent transactions.

The process of implementation involves the following innovations and they are:

- (i) *Zero-Knowledge proof* is applied to a Strong room utilizing an RFID Smart card and camera to prevent data forgery and personal information infringement.
- (ii) Blockchain handles transactions carried inside the strong room and stores each transaction in a *blockchain ledger for privacy protection*.
- (iii) Blockchain also stores *symmetric keys* inside the server and these keys are not distributed to users who view the data hence security is preserved.
- (iv) Whenever a user needs to view the data they must be registered prior to the transaction with the Blockchain server so that *only authorized user can access* to the transactions, and only they can view the data by keys generated by the Blockchain.
- (v) A *hacker application* has been developed to check if the data has been modified by using a false timestamp, and if there is any modifications will be notified in the user blocks by a “*bug*” *icon* and the same will be reported.

1.5.1 Device Authentication and Data Transmission:

The following Figure 4 depicts the sequence diagram used for the device authentication and data transmission process involved in the present work.

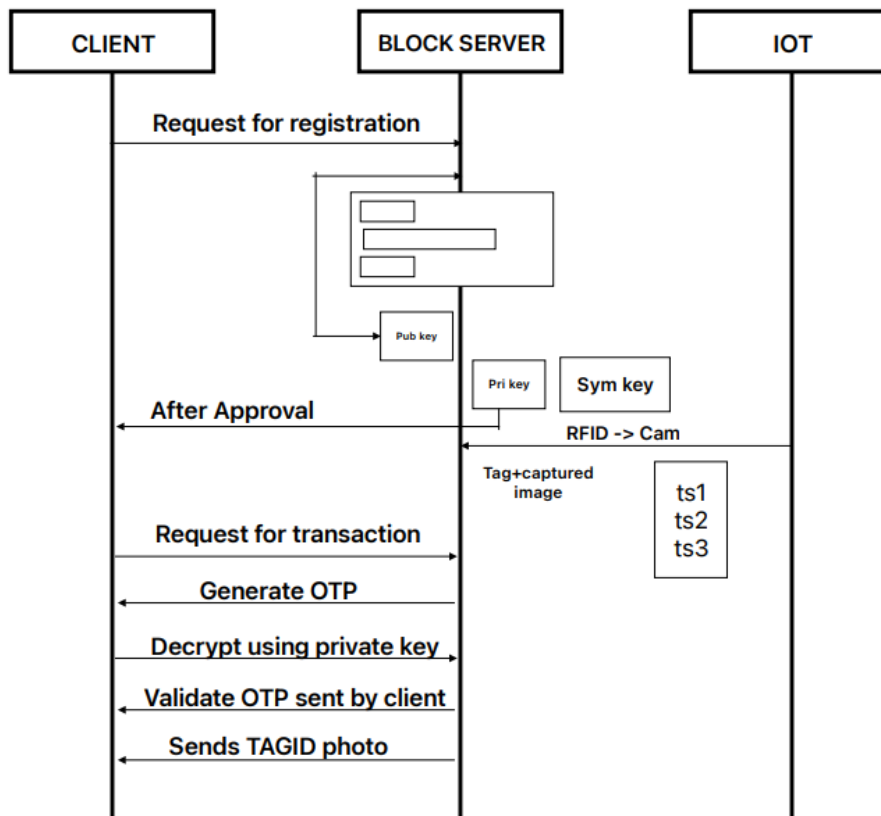


Figure 4: Sequence Diagram

The IoT Model stores the transactions using RFID Card Reader as well as an image captured by the camera in queue and sends those transactions to the Blockchain ledger. The next step is the Clients need to be registered to the Blockchain server first, in order to seek permission for transactions. The blockchain contains multi-key system and they are Private key, Public key and Secret key. During client registration, the private key along with the secret keys are provided to the client. The public key is retained in the Blockchain only. Once the registration is done, the client can request the recent transactions approved and then Request for the data view, which involves the regeneration of the shared secret key using the private key and sent to the server. The Blockchain should check the secret key which is the same one that hasd been sent to the client while registering. If the secret key mathches, then that particular client is said to have registered and right to access the server and found to be authorized person. The recent transactions are sent to user blocks where only the authenticated user can view them. As soon as the transaction is moved to blocks then only that particular block will be removed from the ledger in order to prevent security breaches and data tampering.

1.6 Literature Survey

Various researchers have suggested and implemented many security mechanisms. The following section, illustrates the review of the literature related on the topic chosen for the study.

"Blockchain-based System for Secure Data Storage with Private Keyword Search" was developed by **Hoang Giang Do and Wee Keong Ng [1]**. Blockchain technology is used to present a system that offers a secure distributed data storage system with keyword search functionality. These systems enable the users to spread data content across cloud nodes, upload data in encrypted form and employ cryptographic techniques to guarantee data availability. Once a particular file has been pulled from the data repository, it must be encrypted for the access. The aggregate key is only accessible to certain individuals, but the trapdoor key for a particular community is available to everyone.

"A Blockchain-Based Access Control System for Cloud Storage," presented by **Ilya Sukhodolskiy and Sergey Zapechnikov[2]**, suggested a blockchain-based user access framework for cloud storage. This gives a framework for recovering data stored in unsafe environments, such as cloud storage. For instance, the metadata identified the file will be accessible on the blockchain. In contrast, the data, such as multimedia files, documents, and other type, will be safely stored on the cloud. A blockchain will encrypt and restrict access to the anonymous data stored before processing it. The client who wishes to view a file must comply with the access policy and possess the key to unlock and decrypt it. The owner of the information provides the decryption keys. Blockchain and smart contracts ensure the adaptability of access policies, other stakeholders' ability to modify access policies without requiring additional security measures to keep user keys unchanged, security and privacy of all transaction data, facts that are accepted and rejected, and the impossibility of editing and modifying these data.

"Blockchain-based Secure Data Storage and Access Control System using Cloud" was published by **Shubham Desai and Omkar Deshmukh[3]**. They have described a multi-user access control system for databases that uses blockchain technology to deliver robust, distributed data processing. This proposes a more secured, blockchain-based data storage and access

management system to improve the security of cloud storage. The processing of the blockchain in the cloud with the technology promotes data privacy. retaining the blockchain's immutability.

“Evolutionary survey on data security in cloud computing using blockchain” was published by **S.Prianga, R. Sagana, and E. Sharon [4]**. They surveyed the security challenges, highlighting the effectiveness of security as it relates to cloud computing and blockchain technology. A detailed understanding of a PoW-based blockchain model leveraging blockchain technology is also included in this survey. Their aim was to provide a comprehensive overview of blockchain technology which is rapidly gaining popularity.

Rohini Pise and Sonali Patil [5] proposed the decentralized cloud storage which could be linked with blockchain technology for better data security and storage procedures in their paper "Enhancing Security of Data in Cloud Storage using Decentralized Blockchain," released in **2021**. The method proposed is capable of successfully preventing data from being changed or deleted in part. The data stored there is connected through the chain of blocks that makes up the blockchain, results in a lower chance of data manipulation, which is done using the SHA-512 hashing technique.

Farheen Shaik et al.[6] discussed the technologies which are rapidly increasing and depend on the Internet. The hardware will be embedded with software and interconnected to the Internet to send or receive data, termed as Internet of Things, resulting in Database shared between different devices. The technology of Distributed Databases is known as Blockchain. Using these latest technologies, the Internet of things (IoT), Blockchain, and Near Field Communication (NFC), can provide data protection. The authors aimed to develop a system for authentication on Android applications. In this paper, the authors use a Zero-knowledge authentication system to log into an Android application using Hashing Technique and NFC. The data is generated in Android application and transferred to a blockchain server, which converts the transaction details into ever-growing blocks stored in blockchain storage. With the help of all these technologies, the developed techniques provides a more secured environment that prevents data tampering, data modification and also restricts the data or blocks visibility with an unbreakable authentication system.

1.7 Implementation

The method proposed has been implemented for its validity and the flow chart of the implementation is shown in Figure 5.

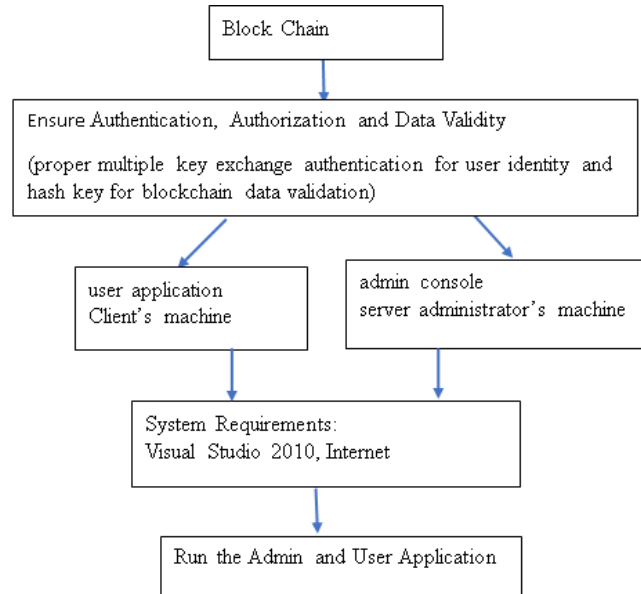


Figure 5: Implementation Flow chart

1.7.1 Role of the consoles: **Admin Console** will be used to start the connection service, approve/disapprove connection request from a user and moderate the connecting devices, whereas the **User Application** will be used by the client is mainly control the IOT device by connecting to the network, and also to make a connection request.

1.7.2 Running the Admin and User applications

1. In the present system where you want to run the Admin console, first open the 'AdminConsole' folder. Next open the 'AdminConsole.sln' file using Visual Studio. When this is executed, the following screen is opened and is displayed in Figure 6.

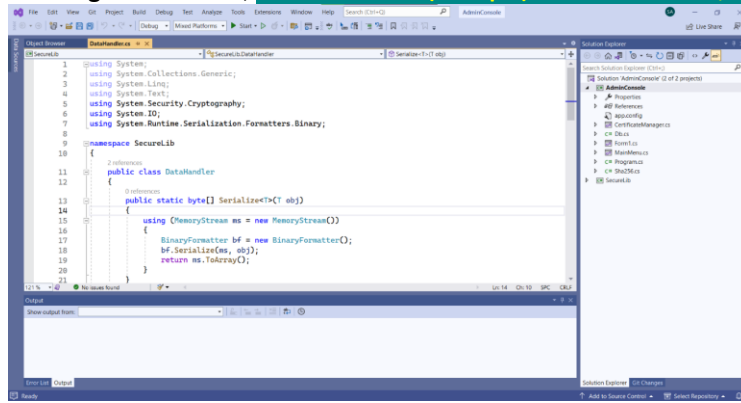


Figure 6: AdminConsole

- When the screen is opened, On the Menubar, click on ‘Build’, then select ‘Rebuild solution’ from the drop down, as shown in Figure 7.

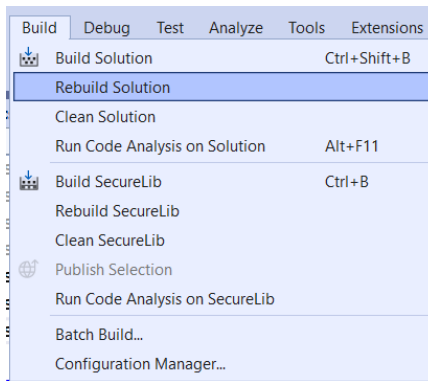


Figure 7: Rebuild Admin sln file

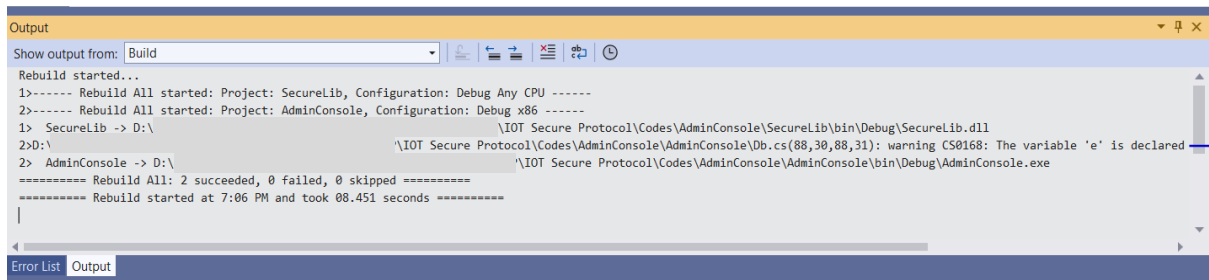
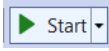


Figure 8: AdminConsole code rebuild

- Once the rebuild process is completed, click on the ‘Start’ button  on the toolbar or press F5 button to run the program and start the console.

A new admin console window is created. This is the window/console that distinguishes normal users from an administrator, since only administrator console has the options to

control the userbase of the IoT server, and also to start/stop the IoT server on the go. Admin Console window is displayed.

Perform the same steps to also the 'UserApp' code in the client machine, which will open a small window, as shown in Figure 9. Once the process is completed, then the app is available to use.



Figure 9: User Application preface screen

The window contains information regarding Internet of Things as a whole, for the user's basic knowledge. It also details the user about the risks and security concerns involving the IoT as a whole.

4. Click on the green coloured right arrow button to open the main User application window and then the is as shown in Figure 10.



Figure 10: User application window

1.7.3 The Flow Chart for Sending of Registration Request by the client

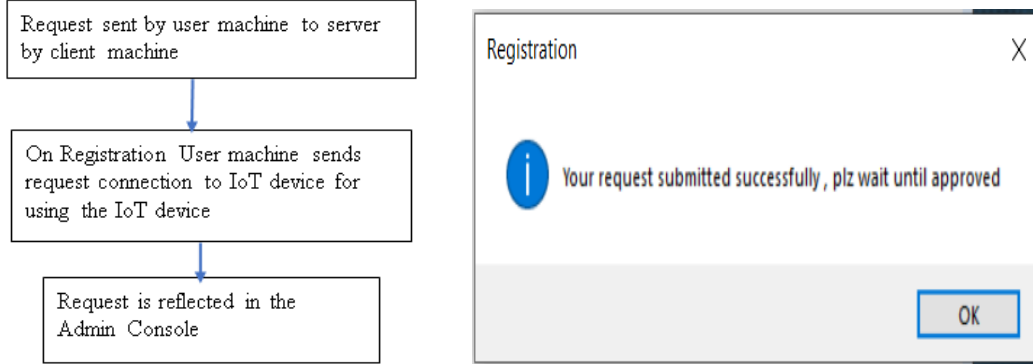


Figure 11: Registration Request

The opened dialog box with the display, then press OK to continue.

This request is reflected on the Admin console, where the further steps are carried out by the administrator of the IoT server, then he chooses whether to approve the registration from the particular user or to reject it.

1.7.4 Approving the User request by the Admin is shown below in the flow chart.

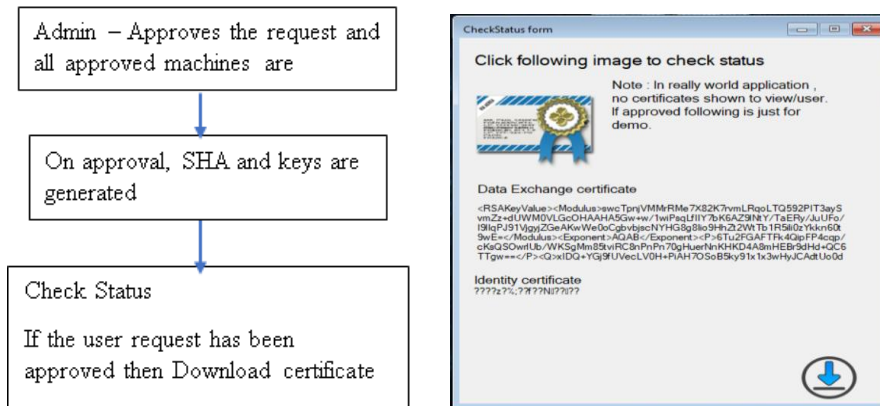


Figure 1: Download certificates dialog box

Accessor (get statement) is used to access the certificate and private key from the cloud database for the particular record, and are returned.

The further step to start the IOT server and establish the Client connection to the IOT server to control the IOT device is shown in the following flow chart. The implementation in the sequence provide the display as shown in Figures

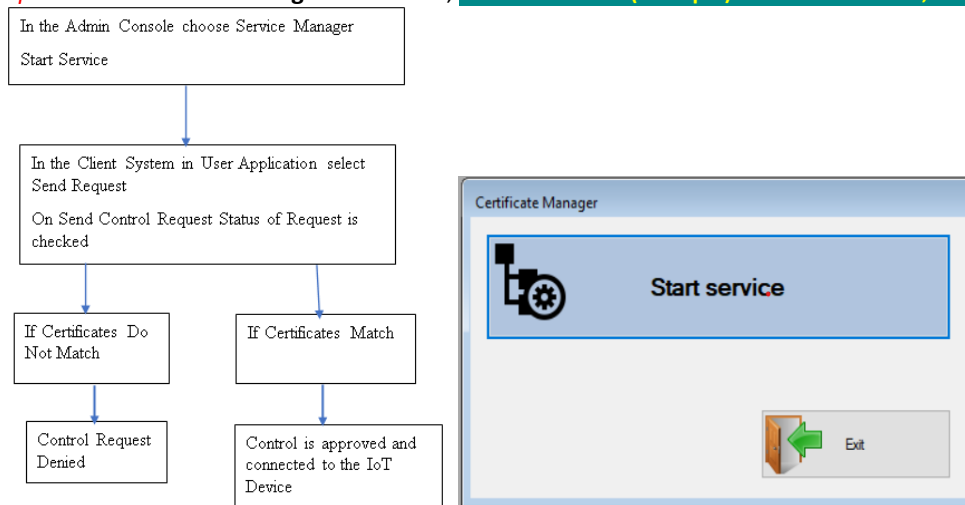


Figure 13: Start Service

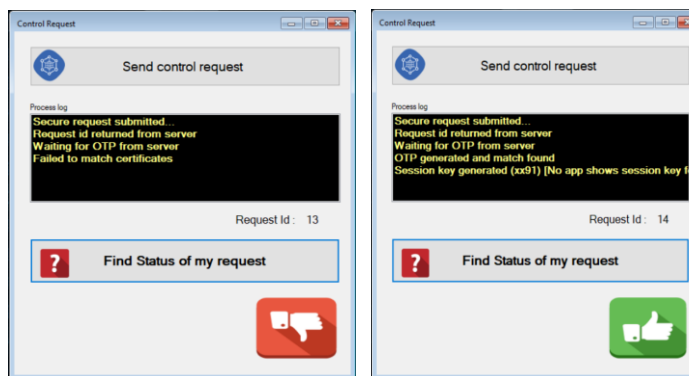


Figure 2: Control request denied

Figure 3: Control request Approved

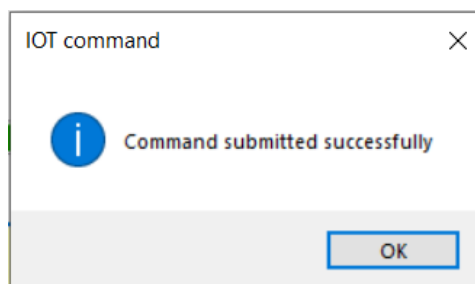
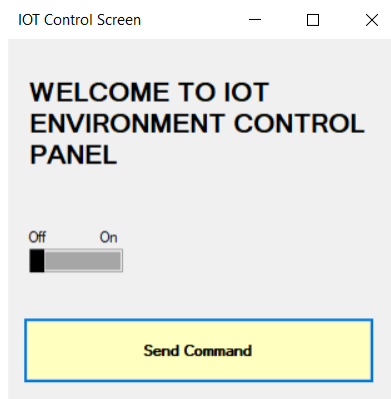


Figure 16: IOT device control panel Figure 17: Connection Successful

Now the user can notice that IoT device has been turned on with the display ‘Command submitted successfully’ as shown. In this process, through a secure environment, the client can control and access the IoT devices.

CONCLUSION

With the rise of IoT devices in various industries, there is a need for secure and efficient communication and data sharing is becoming increasingly important. The paper proposes a highly secured strong room like system using Zero-knowledge proof to protect data. IoT data is stored in the blockchain, which can prevent IoT device authentication and data tampering by the intruder. RFID card used in the present work monitors the modification and the theft of data done by others through blockchain because of the problems such as forgery and alteration of data.

The present research work includes the implementation of blockchain in IoT offers a secure and efficient solution to the challenges of authentication and data protection. The Blockchain used in the present work is capable of providing secure authentication and data storage, as well as enable the decentralized and secure communication networks. The conclusion is that by adopting blockchain in IoT, the improved security of information is achieved and also provide better service to their authenticated customers.

REFERENCES

- [1] Hoang Giang Do and Wee Keong Ng “Blockchain-based System for Secure Data Storage with Private Keyword Search”, IEEE 2017
- [2] Ilya Sukhodolskiy, Sergey Zapechnikov, “A BlockchainBased Access Control System for Cloud Storage,” IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus), 2018.
- [3] Shubham Desai and Omkar Deshmukh “Blockchain-based Secure Data Storage and Access Control System using Cloud”, IEEE 2019
- [4] S. Prianga R. Sagana and E. Sharon, “Evolutionary survey on data security in cloud computing using blockchain”, vol. 6, no. 4, pp. 4396–4401, 2020
- [5] Rohini Pise and Dr. Sonali Patil “Enhancing Security of Data in Cloud Storage using Decentralised Blockchain”, ICICV 2021
- [6] Farheen Shaik, Satish G.C, (2019). Implementation of IoT System using Blockchain with Authentication and Data Protection. *International Journal of Computer Sciences and Engineering*, 07(14), 171-175.
- [7] B. A. Alzahrani and K. Mahmood, “Provable privacy preserving authentication solution for

internet of things environment,” *IEEE Access*, vol. 9, 2021.

<https://github.com/hivemq/hivemq-community-edition>

[8] Trusit Shah and S. Venkatesan, "Authentication of IoT Device and IoT Server Using Secure Vaults," In Proceedings of 17th IEEE International Conference, New York, USA, pp. 819-824, 2018.

[9] Kalra S and Sood S. K, "Secure Authentication Scheme for IoT and Cloud Servers," *Journal of Pervasive and Mobile Computing*, Elsevier Publications, Vol. 24, pp. 210-233, 2015.

[10] Amazon.com. "Amazon Elastic Compute Cloud". URL <http://aws.amazon.com/ec2/>

[11] Amazon.com. "Amazon Elastic Block Store". URL <http://aws.amazon.com/ebs/>

[12] Microsoft Windows Azure Platform. URL <http://www.microsoft.com/azure/default.aspx>