International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 08 | Aug 2021 www.irjet.net p-ISSN: 2395-0072

RFID Card Reader & IoT System using Blockchain with Authentication and Data Protection

Gayathri S[1]
Student
Department of Computer Science and Engineering
National Institute of Engineering
Karnataka, India

Dr. C Vidyaraj[2]
Professor
Department of Computer Science and Engineering
National Institute of Engineering
Karnataka, India

Abstract - *The IoT is that the abbreviation of the Online of Things, which enables objects to share and control data between objects because things are connected to the Online. The Blockchain is "distributed ledger" technology, make sure appeared as an object of intense interest in the interior the tech industry also out there. As soon as a person desires to characteristic of transaction to the chain, the whole thing of the contributors within the community will validate it. They try this via way of worth of making use of a set of rules to the transaction to affirm its validity. A set of permitted transactions is then bundled at some point of a block, which receives dispatched to any or the entire item of the nodes inside the community. Now validate the brand new block. For each successive block add in a hash, which may possibly too be a completely unique fingerprint of the preceding block.*

Key Words*: *IoT, RFID Card Reader, Blockchain, Strong room, Zero Knowledge Proof.

1. INTRODUCTION

A Blockchain may be a dispersed database that keep up a dynamic list of records, secured against damaging and modification. Blockchain can be present used such as distributed ledgers that agree to transactions on the way to be recorded as well as verified cryptographically without the requirement. Now a Blockchain IoT environment, when the transactions are stored in the ledger once the user requests for his transaction it sends to block and delete from the ledger. As soon as data or device authentication information is placed on a Blockchain, personal information may possibly leaked through the proof-of-work process or address search. We apply Zero-knowledge proof to a robust room by means of RFID Card reader as well as Camera module IoT systems in the way of prove that a prover devoid of disclosing specifics enhances the secrecy of Blockchain.

2. LITERATURE SURVEY

In [1] "The Incremental Hash Function Established on Pair Block chaining", the paper consist of Incremental Hash Function such as XOR Scheme and PCIHF Scheme established on Pair Blockchaining. The paper as well make available of data integrity, message authentication, digital signature, as well as password protection.

In [2] "A privacy Detection and Authorization/Accounting System using Blockchain Technology", the paper describes hash functionality with long accounting and control issues with protection and authorization. This also helps in storing data for a longer time and privacy policies are improved Deals with accounting and unlikability issues.

In [3] "Survey on Multicast Data Origin Authentication", the paper focuses on the methodology of Convolutional neural network. The trained model achieves an accuracy of 99.35%. The data set taken under different conditions still achieves an accuracy greater than when selected at random. This needs a more diverse set of training data to improve the general accuracy.

In [4] "World of empowered IoT users" The paper presents the view of challenges and opportunities for design automation of cyber-physical systems. The design challenges significantly high ability in the direction of

control to access the data. The paper also includes Limited to the database. It should be expanded to the storage variety of data.

In [5] "A Novel Biometric-Based Authentication Scheme with Privacy Protection" the paper presents the integration of embedded systems with global networks such as the internet and the paper also deals with the Transfer learning approach to train a deep convolution storage capacity. This method avoids the complex and virus step of feature extraction to maintain the storage.

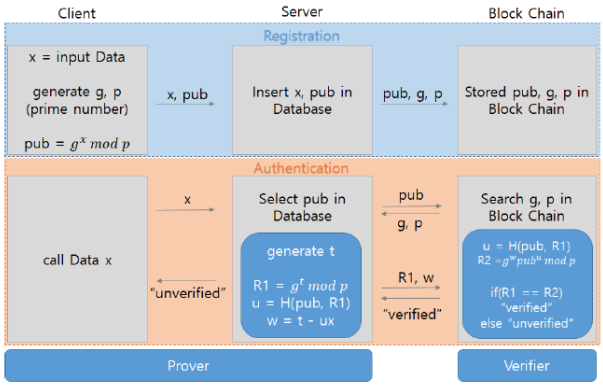
3. METHODOLOGY

Registration module

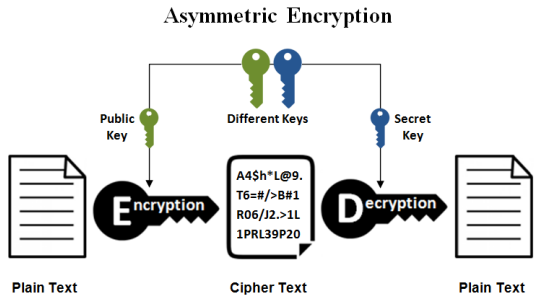
In this module, we should allow the user of the system to register for data communication with the IoT model. During registration technical information about the machine is collected and the same will be submitted to the Blockchain server for further process.

Authentication module

Module works as follows



Digital Certificate generating module



Asymmetric or else public-key cryptography is a cryptographic system that uses a pair of keys-a public key and private key. A piece of mail or client will send a first encrypted using a public key, which is available to anyone and can be passed around freely. On the other hand, to encrypt the message, the recipient will need a private key, which is something must have.

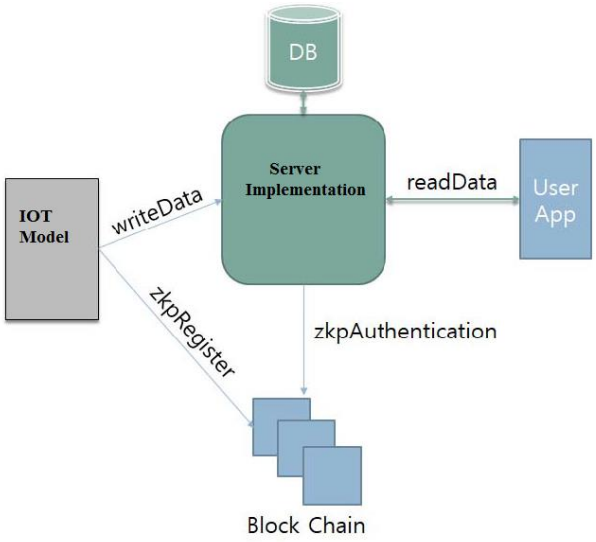
This worth, as long as the private key remains hidden, no one but the intended recipient will be able to open the email that send them for you. In the meantime this one is impossible to figure out the private key from the public key, this makes asymmetric cryptography extremely important to secure your email. Email by default is not very secure. Sure, your email will for the most part and be protected on its way between the client and email server, making it hard for some intercept your sensitive documents.

IoT module

We should develop an IoT module with sensors [not yet decided] to read live data and store same in Blockchain controlled database (MySQL), which will be secured from the user layer so that user can't access IoT data directly

Blockchain server implementation

Server implementation sits between IoT module and user for managing User profile, Certificates, Request, Storing and Read Data from the Blockchain blocks to deliver to the user. The outline sketch of the implementation is shown below



Data distributing Module from IoT to Blockchain

In this module based on the user request, The Blockchain server identifies the user & matches the certificate to

deliver data. The server accepts the request and performs Authentication with Blockchain & response data using thin layer data communication such as XML or JSON.

User application to get data after authentication & authorization

User requires apps to register, check register status, data request and get data based on request.

4. IMPLEMENTATION

Arduino IDE:

The Arduino IDE is a cross-platform application based on Windows, machos, Linux. This is on paper with inside the programming language Java. This one is wont to write down and improve applications to Arduino well matched boards, on the other hand additionally, by way of the help of third celebration cores, not the same dealer improvement boards. The Arduino IDE is the program that used to write some code, then get some form. The Arduino board that stores and performs some code then uploaded. It is based on C or C++ programming language. The Arduino IDE is an open source platform. It is based going on easy to use hardware as well as software. It is software based on processing. The Arduino boards are able to read inputs like light on a sensor, a finger on a button, a Twitter message and turn it into an output than activating a motor, turning on an LED and so on.

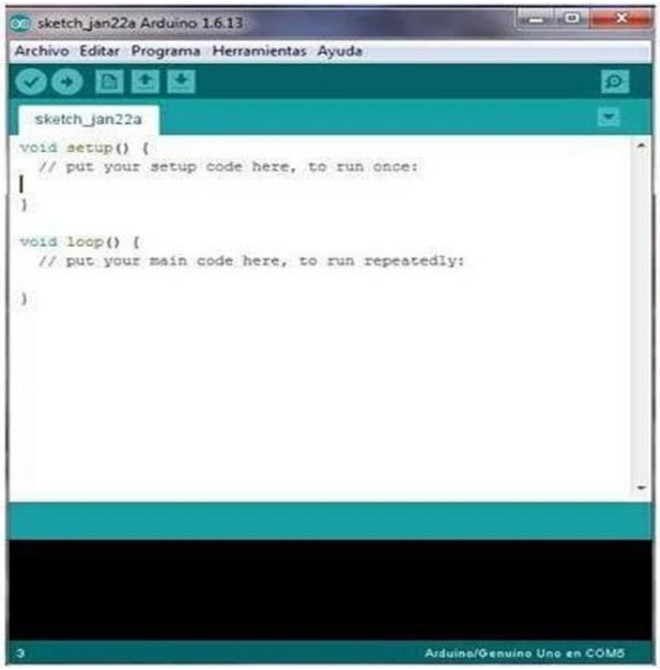


Fig: Arduino IDE is within functions

5. RESULT AND DISCUSSION

Blockchain agree to the consumers as well as data provider to make sure Authentication, Authorization, too Data validity by way of proper multiple key exchange authentication for user identity as well as Hash key for Blockchain data validation in future that data is not just stored but also validated each time when end user right to use.

Fig 1: User Register in the Client Page

Fig 1 depicts the user registration, where the user sends the request to the Blockchain server from the client application to be registered.

Fig 2: Confirming the Request for the approval

Fig 2 depicts the Confirmation of the request approval, once the client application requests to get registered, the system automatically fetches the Mac Id, Username, Date, and time.

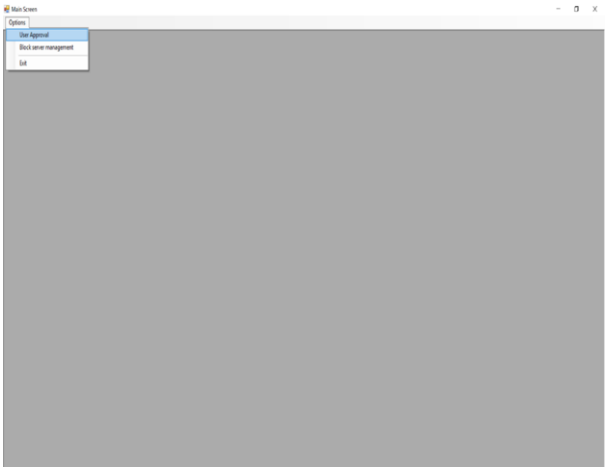


Fig 3: User Approval screen in the Blockchain Page

Fig 3 depicts the User approval screen in the Blockchain application, where the request sent by the client needs to be approved or rejected.

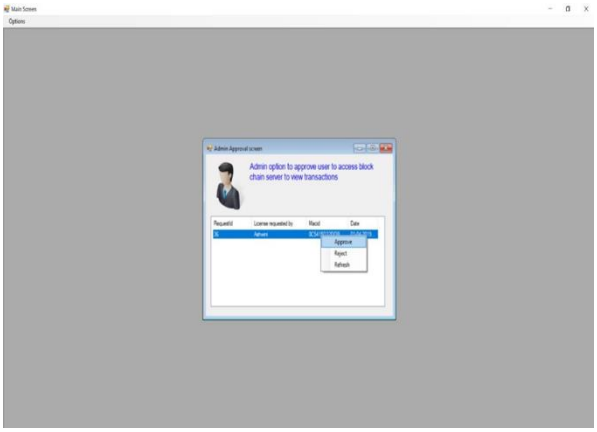


Fig 4: Request Approval/reject screen of the Blockchain admin

Fig 4 depicts the Request approval screen in the Blockchain application, where the list of requests sent by the client is approved/rejected here.

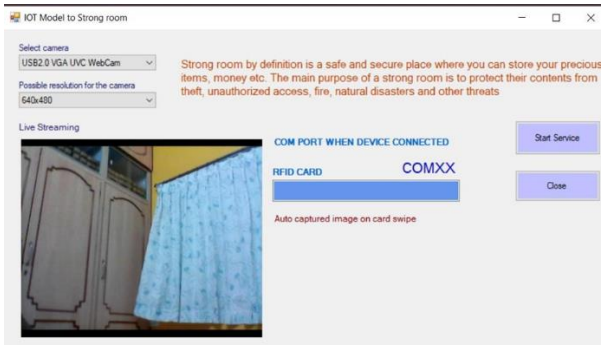


Fig 5: IoT screen connected to the Camera

Fig 5 depicts the IoT screen connected to the camera where it fetches the type of camera and also the resolution of the camera.

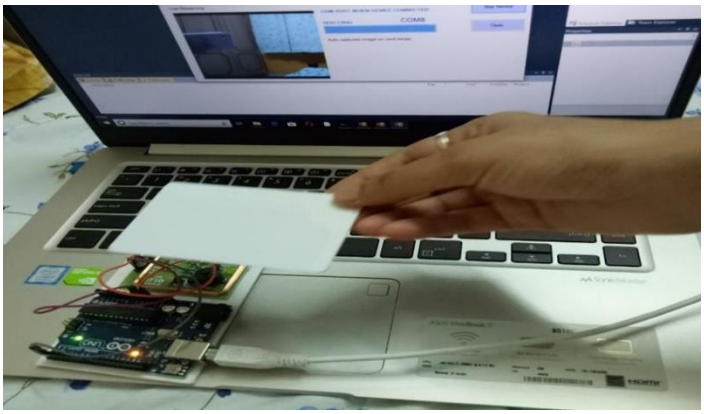


Fig 6: Swiping RFID card in the IoT screen

Fig 6 depicts the swiping of an RFID card into the Arduino board in the IoT screen, fetches the card number with the com port used.

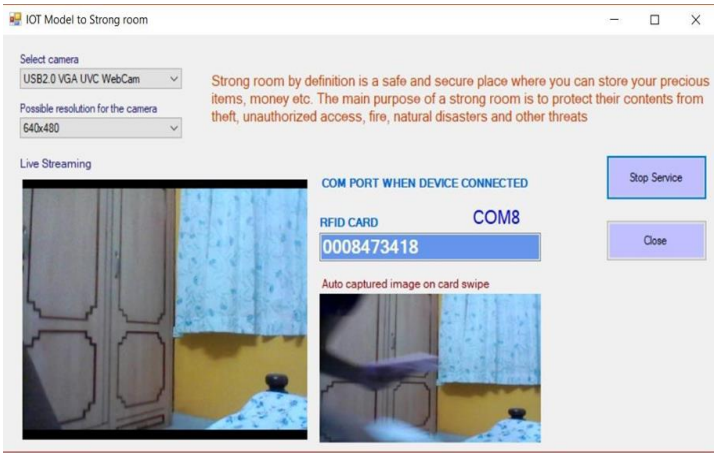


Fig 7: Live image is captured

Fig 7 depicts that whenever the card is swiped against the RFID Card reader, the card value is scanned and the live image is captured and the tag ID and image is saved as a transaction

Fig 8: Check the secret key and move the transaction

Fig 8 depicts the checking of the secret key and the movement of the transactions, here the resent transaction can check by the secret key and can move
that transaction.

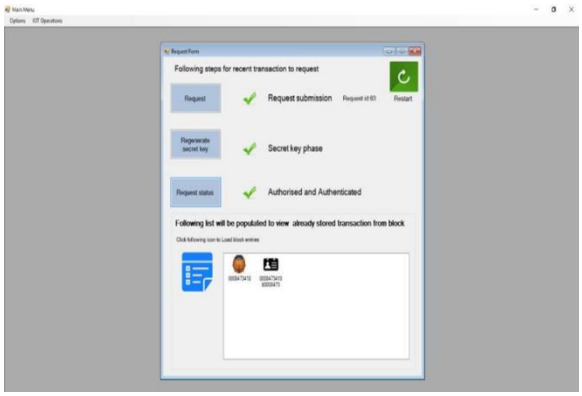


Fig 9: Transaction stored in the client screen

Fig 9 depicts the transactions stored in the client screen, here the transaction stored are from the blocks of Blockchain to the user block.

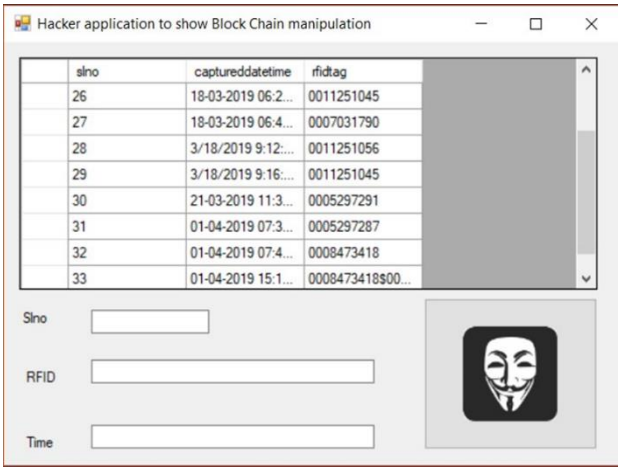


Fig 10: Hacker application

Fig 10 depicts the Hacker application, where all the transactions are listed and the hacker can modify any transactions. He can modify the RFID number, time of transaction too.

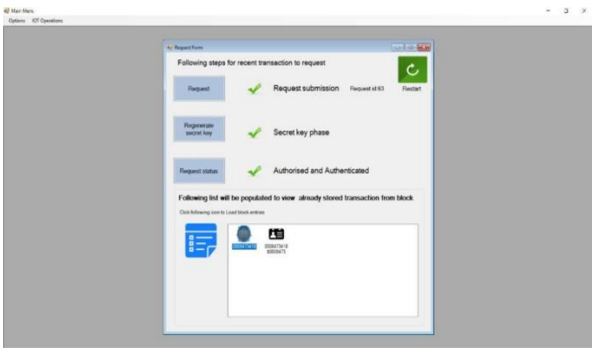


Fig 11: Hacked Transaction in the user block

Fig 11 depicts Hacked transaction in the user block, here the BUG li icon is shown for the modified transaction so that the user can identify easily that the transaction has been hacked.

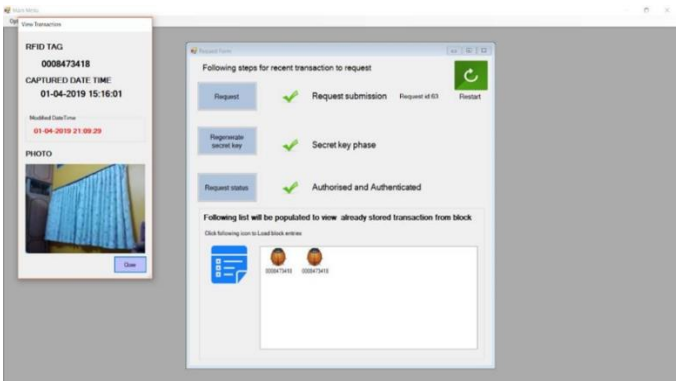


Fig 12: View of the Hacked details

Fig 12 depicts the view of the Hacked details, the details like the time of the modification, RFID number any changes or modification is done by the hacker can be viewed here.

6. CONCLUSIONS

Equally Internet of things as well as Blockchain be present in their nascent stages, by way of the promise of a future anywhere machine-to-machine communication are going to be located effortless. At present, companies are putting efforts into merging the 2 technology powers. As soon as mutual, Internet of things as well as Blockchain technology will hire agreement several industries grow well by easily monitoring, tracking, as well as securing data.

ACKNOWLEDGEMENT

I personally prompt our thanks to the National Institute of Engineering in place of provided that and chance in the direction of comprehensive this effort. Myself be present as well glad to the authors whose papers have been referred.

REFERENCES

[1] Madhusudhan Singh, Abhiraj Singh, Shiho Kim, "Blockchain: A game Changer for Securing IOT Data", IEEE 4th World Forum on Internet of Things (WF-IoT), 2018.

[2] Randa Almadhoun, Maha Kadadha, Maya Alhemeiri, Maryam Alshehhi, Khaled Salah, "A User Authentication Scheme of IoT Devices using Blockchain-enabled Fog Nodes", IEEE/ACS 15th International Conference on Computer Systems and Applications,2018.

[3] M. Alblooshi, K. Salah, Y. Alhammadi," Blockchain-based Ownership Management for Medical IoT (MIT IoT) Devices", 13th International Conference on Innovations in Information Technology (IIT),2018.

[4] Beini Zhou, Hui Li, and Li Xu," An Authentication Scheme Using Identity-based Encryption & Blockchain", IEEE Symposium on Computers and Communications (ISCC),2018.

[5] Mary Subaja Christo, Anigo Merjora A, Partha Sarathy G, Priyanka C, and Raj Kumari M," An Efficient Data Security in Medical Report using Blockchain Technology", International Conference on Communication and Signal Processing, April 4-6, 2019.

[6] Oksana Lukmanova, Elena Volkova, Anton Zabolotnyi, Aleksandr Gorelik," Blockchain Technology for Public Utilities", IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering,2019.

BIOGRAPHIES

Gayathri S MTECH IT, Department of Computer Science and Engineering, The National Institute of Engineering, Mysuru, Karnataka, India.

Dr. C VidyaRaj Professor, Department of Computer Science and Engineering, The National Institute of Engineering, Mysuru, Karnataka, India.