IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Special Issue-14, May 2019 E-ISSN: 2347-2693

Implementation of IoT System using Blockchain with Authentication and Data Protection

Farheen Shaik[1*], Satish G.C[2]

[1,2]School of Computing and Information Technology, Reva University, Bangalore, India

Corresponding Author: farheen406@hotmail.com, Tel.: +91-7032434657

DOI: https://doi.org/10.26438/ijcse/v7si14.171175 | Available online at: www.ijcseonline.org

***Abstract*—** Technologies are rapidly increasing and dependent on the Internet. In near future, Hardware will be embedded with software and interconnected to the Internet to send or receive data, which is termed as Internet of Things. Resulting to Database shared between different devices, technology of Distributed Database is Blockchain. Using these latest technologies, Internet of things (IOT), block chain, and Near Field Communication (NFC) for providing data protection, we are developing a system for authentication on Android applications.

In this paper, we are using Zero knowledge authentication system to login into Android application using Hashing Technique along with NFC. The data generated in Android Application and transferred to block chain server which convert the transaction details into blocks, which ever growing and store it in blockchain storage. With the help of all these technologies we are providing more Secure environment which prevent data tampering and modification. As well restricted data or block visibility. With unbreakable authentication system.

***Keywords*—**IOT, Blockchain, NFC, Android Application.

I. INTRODUCTION

The Near Field Communication (NFC) is a wireless technology that facilitates conducting daily tasks through communication between NFC-enabled devices. Nowadays, the NFC technology is playing a major role in different fields of our daily life. It has been successfully applied in various fields such as healthcare, education, location-based services, access control, financial transactions, social applications and entertainment. In the financial sector, the NFC technology is expected to gain popularity especially in mobile-based payments, mobile authentication, etc. In this paper we are using NFC for zero knowledge authentication system for mobile login.

IOT is the abbreviation of internet of things which enables objects to share and control data between objects. In this system Android mobile is communicating with block chain server for data sharing.

It is possible to commit malicious attacks, such as data tampering, or privacy infringement, while sharing data on objects over the Internet. This paper introduced a block chain to prevent security threats such as data counterfeiting, which could occur using smart meters. Zero-Knowledge proof, a block chain anonymity enhancement technology, was introduced to prevent security threats such as personal information infringement through block inquiry. It was proposed to use smart contracts to prevent smart meter data forgery and personal information infringement we suggest. Internet of Things enables objects to share and control data between objects because things are connected to the Internet. It is possible to commit malicious attacks, such as data tampering, or privacy infringement, while sharing data on objects over the Internet.

Block chain server is running on web server, authorized android mobile can able to communicate with blockchain web server and store the data or retrieve the data. Block chain servers have the functionality for creating block and retrieving the block from block chain storage.

II. RELATED WORK

Blockchain

A block chain, initially block chain, is a developing rundown of records, called blocks, which are connected utilizing cryptography. Each block contains a cryptographic hash of the past block, a time stamp, and exchange information (for the most part spoke to as a merkle tree root hash).

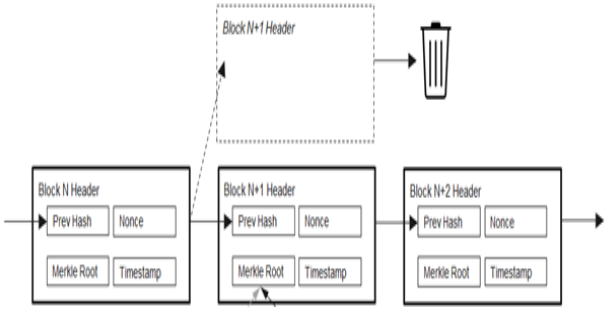


Fig 1: Block Chain Structure

Structure:
A Blockchain is a decentralized, disseminated and open advanced record that is utilized to record exchanges crosswise over numerous PCs so the record can't be modified retroactively without the modification of every single consequent block and the accord of the system. This enables the members to confirm and review exchanges in lavishly. A Blockchain database is overseen self-sufficiently utilizing a shared system and a circulated time stepping server. They are confirmed by mass cooperation fueled by aggregate personal circumstances. The outcome is a powerful work process where members' vulnerability with respect to information security is negligible. The use of a Blockchain clears the typical for boundless reproducibility from a propelled asset. It affirms that every unit of significant worth was exchanged just once, tackling the long-standing issue of twofold spending. Blockchain have been portrayed as an esteem trade convention. This Blockchain-based trade of significant worth can be finished snappier, more secure and less expensive than with conventional frameworks A Blockchain can relegate title rights since, when legitimately set up to detail the trade understanding, it gives a record that urges offer and acknowledgment.

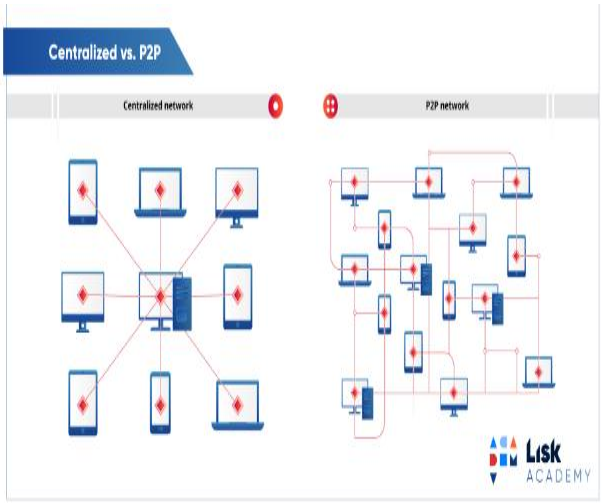


Fig 2: Centralized Vs P2P

In a P2P network, the "peers" are PC frameworks which are associated with one another by means of the Internet. Documents can be shared straightforwardly between frameworks on the system without the need of a central server. At the end of the day, every PC on a P2P network turns into a record server just as a client.

Kinds of blockchains
Right now, there are three sorts of blockchain systems - public blockchains, private blockchains and consortium blockchains.

Public blockchain
A public blockchain has positively no entrance limitations. Anybody with a web association can send exchanges to it just as become a validate (i.e., take an interest in the execution of an accord convention). Typically, such systems offer financial motivating forces for the individuals who secure them and use a Proof of Stake or Proof of Work calculation.

Near field communication
NFC (Near-field communication) innovation is quite regular nowadays and highlights in most top of the line advanced cells. Just as telephone to telephone communication, little NFC labels can likewise be utilized to store and exchange data. You will presumably have seen little NFC labels by promotions close transport stops, stickers in shops, or may have even run over the smart thought of utilizing NFC empowered business cards.

These tags can store wide scopes of data, from short lines of content, for example, a web address or contact details, to connections to applications in the Google Play Store. It's a snappy and proficient approach to rapidly push data to your telephone and these little labels can supplant bar and QI codes, and could even be utilized rather than Bluetooth at times. So here's the manner by which it works.


Fig 3: NFC Reading / Writing Process

How it works:
NFC tags are latent gadgets, which imply that they work without their very own power supply and are dependent on a functioning gadget to come into range before they are actuated. The exchange off here is that these gadgets can't generally do any preparing of their own, rather they are just used to exchange data to a functioning gadget, for example, a PDA.

So as to control these NFC tags, electromagnetic acceptance is utilized to make a current in the aloof gadget. We won't get excessively specialized on this, yet the essential guideline is that loops of wire can be utilized to deliver electromagnetic waves, which would then be able to be grabbed and transformed once more into current by an another curl of wire. This is fundamentally the same as the systems utilized for remote charging advancements, though significantly less amazing.

The dynamic gadgets, for example, your advanced cell, are in charge of creating the attractive field. This is finished with a straightforward loop of wire, which produces attractive fields opposite to the stream of the exchanging current in the wire. The quality of the attractive field can be balanced by fluctuating the quantity of turns in the wire loop, or expanding the present coursing through the wire. Be that as it may, increasingly current clearly requires more vitality, and exceptionally high power necessities would not be alluring for use in battery fueled portable advances. Subsequently why NFC works over only a couple of inches, as opposed to the numerous meters that we're utilized to with different sorts of remote communication.

- **NFC Writing Algorithm (Tag):**

NFC expands upon Radio-frequency identification (RFID) frameworks by permitting two-route communication between endpoints, where prior frameworks, for example, contactless shrewd cards were single direction as it were. Since unpowered NFC tags can likewise be perused by NFC gadgets, it is additionally equipped for supplanting prior single direction applications. In this NFC tag we are dumping the information, for example, name, telephone, address anything as a scrambled configuration utilizing Encryption key and dumped into the NFC tag, before dumping into the card first information is Declare an Intent Filter to report to the framework that it's empowered to take a shot at NFC. Have a strategy that Android will call when NFC is recognized. Make a strategy to fabricate a NDEF message. Make a technique to compose the NDEF (NFC Data Exchange Format) message.

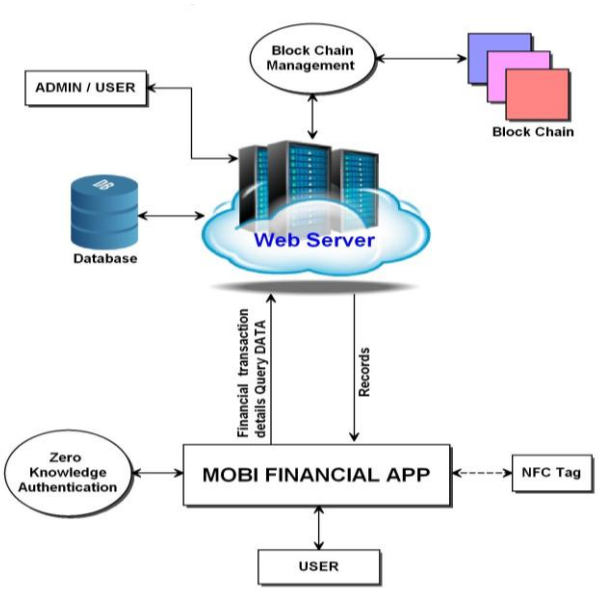
- **NFC Reading Algorithm (Tag):**

When the card owner taps the card to NFC device, first encrypted data will read and it will decrypt the data and converted into original data with key and reading NDEF data from an NFC tag with language convention English.

III. METHODOLOGY

This system has two applications one is mobile financial app. And another is web server application which manages block chain process.

There are two actors one is admin another one is end user. Admin must set block chain storage details and user information in web server application. There is another responsibility of admin he must write credentials into user NFC card using separate android app. The NFC card must reach corresponding user safely.



.
Fig 4: System Architecture

Once user receives NFC card then only he can able to login into mobile financial app. While user trying login, he has to provide his user id and tap NFC card on NFC sensor in the mobile. NFC sensor read the credentials from NFC card and give to zero knowledge authentication protocol. It is

responsible of zero knowledge authentication system to validate the credential from NFC card and the credential stored in block chain for the user same or not. Based on the test result it will take decision whether to allow the user into the home page or not.

Once user logged in into mobile app he can able to create transactions related to financial details. All the financial transaction is converted into blocks and store in block chain server.

Main Modules in the System

- **Admin Module**
  Admin has to login using id and password. After login admin can add users and display the user details, admin can modify also. While adding user we admin is making hash code of that user.

- **NFC Writing Process**
  This admin android application is to write user information in to NFC tag.

- **NFC Reading Process**
  In this user module user has to login using user id, if authentication is correct it has to navigate to the home page, after that user can store their personal details.

- **ZERO Knowledge Authentication**
  In this section when user is storing their personal details that time it will create metadata and it will store in to database, based on that metadata only we can find the user personal details.

- **Creating Block-chain**
  In this module user personal data will be store in to cloud as encrypted format, when user want to download that data it has to decrypt and it will display to the user.

Block chain Storing Process

Once the user logged in into android App he can able to create his transaction, all the transactions which are occurred in android mobile has to transfer to web server, in web server block chain head, block chain body created using encryption technique, hashing technique and compression technique. Once block is created it will be stored in block chain storage and there should be a meta data record to retrieve the block.

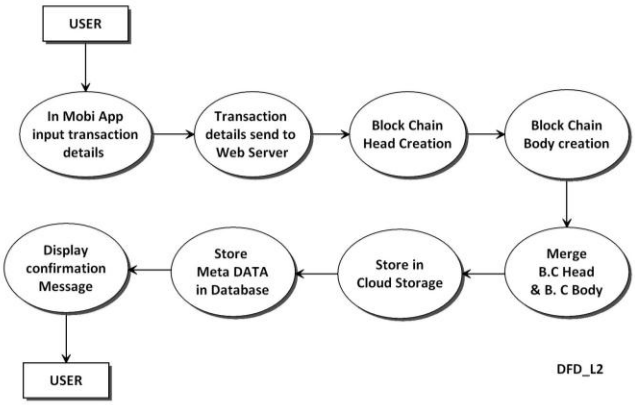


Fig 4: Transaction Block Chain Stroage Process

Once transactions are stored in block chain it becomes highly secure and no one can tamper it. This process is shown in Figure 4.

IV. RESULTS AND DISCUSSION

IOT, Blockchain and NFC techniques are upcoming trends in present scenario. This system involved all these three techniques which makes highly securable easy to use and user can view and retrieve transaction using android App.
For high security zero knowledge protocol and block chain are used. For user friendliness android App and NFC are used.

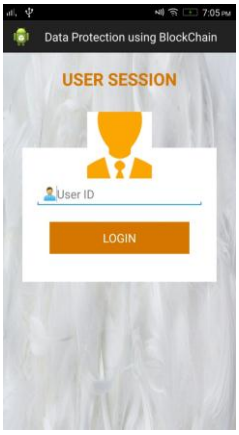


Fig:1

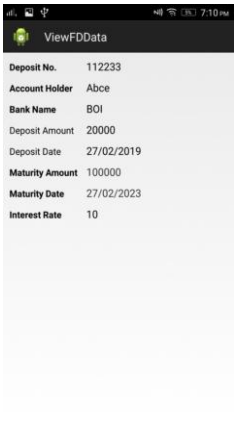


Fig:2

Fig:1- In this user android application user has to enter their userId, then it has to communicate with web server and it has to validate the userId. If it is valid then it will thake the hashcode of that user and then user has to tap the NFC card, from the NFC card it will read the hashcode. If both the hashcode is matching it will navigate to the user home page.
Fig:2- Here it has to display user financial data which user already stored into the Blockchain. When user wants to read his personal details, user has to request to the server and it

will check every details of user and from the blockchain file has to download then it has to decrypt, then from the server data will send to user android application.

V. CONCLUSION AND FUTURE SCOPE

This system uses financial android App, the transactions which are generated by android App are not stored in the same mobile instead it will be transferred to block chain server and stored securely.
The experimental result shows this system functions meet all the requirements specified in design phase.
At present the system is generated Android mobile App in future we can develop mobile App for Apple iOS.

REFERENCES

[1] Gungor, V. Cagri, et al. "A survey on smart grid 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 grid projects in Europe.", Energy Policy, Vol.60, 2013, pp.621-628.
[3] Luan, Shang-Wen, et al. "Development of a smart power meter forAMI 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 Grid System using Blockchai, 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.

Authors Profile

Ms. Farheen Shaik pursued her Bachelor of Technology from Jawaharlal Nehru Technological University,Anantapur-India in 2017 and pursuing Masters of Tecnology from Reva Univeristy in Data Engineering and Cloud Computing – Department of Computer and Information Technology and currently working as Associate Software Engineer at CGI,Inc - India. She is Microsoft Technology Associate – Introduction to Cloud Computing and also did her course in Introduction to Internet of Things and Cyber Security from Cisco Networking Academy

