Implementation of Secure Data Storage in Blockchain with Near-Field Communication Authentication

Niranjan S
Department of Computer Science and Engineering
Bapuji Institute of Engineering and Technology
Davanagere, Karnataka, India.

Pramod C Poojar
Department of Computer Science and Engineering
Bapuji Institute of Engineering and Technology
Davanagere, Karnataka, India

Punith B N
Department of Computer Science and Engineering
Bapuji Institute of Engineering and Technology
Davanagere, Karnataka, India

Vadiraj K
Department of Computer Science and Engineering
Bapuji Institute of Engineering and Technology
Davanagere, Karnataka, India.

Project Guide:
Dr.Ashoka K
Department of Computer Science and Engineering
Bapuji Institute of Engineering and Technology
Davanagere, Karnataka, India

***Abstract*--Blockchain secures a variety of IoT circumstance, when information or system validation information is placed on a blockchain, personal data might be spilled through the affirmation of working system. This paper observes a Zero-Knowledge proof for an awesome meter framework to illustrate the effectiveness of uncovered information as an instance. This research work has pondered a way to enhance the obscurity of blockchain for safety insurance. [2] In addition to that, device Near-field communication (NFC) generation is used as a mobile platform application. The fundamental idea of this research is to provide a secure service to a consumer through mobile application using the near field communication card and Zero knowledge authentication system.**

Keywords— ***IOT, Blockchain, NFC, Zero Knowledge Proof.***

I. INTRODUCTION

Blockchain is a top security system in this jiffy. Internet of Things (IOT) is a fast growing and essential technology for the human. There are several chances for leakage of data which are generated and stored in cloud storage by IOT device. Cryptography technique is not enough the safeguard the data in cloud storage. To overcome this issue, this research work come up with a new mechanism where blockchain technology is used to store the data generated by IoT devices. IOT allows gadgets to share and manage data between objects which are connected through Internet [1]. It is possible to commit malicious attacks, inclusive of records tampering, or privateness infringement, while sharing facts on items over the Internet. This paper introduced a block chain module to provide protection against threats including data counterfeiting, that can arise the usage of clever meters [5]. Zero-Knowledge proof is a block chain anonymity enhancement generation which is added to prevent security threats together with personal statistics infringement through block inquiry. The proposed project is aimed to prevent smart meter facts forgery and personal data infringement in IoT environment.

II. RELATED WORK

Blockchain

A block chain, to begin with block chain, is a growing rundown of records, referred to as blocks, which might be related utilizing cryptography. Each block incorporates a cryptographic hash of the past block, a time stamp, and alternate records (for the most component spoke to as a Merkle tree root hash).

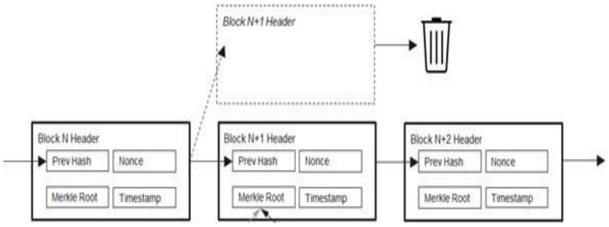

Fig 1: Block Chain Structure

Structure: A Blockchain is a decentralized, disseminated and open superior report this is applied to report exchanges crosswise over several PCs so the file can't be modified retroactively without the modification of each single consequent block and the accord of the system. This enables the individuals to verify and assessment exchanges in lavishly. [8] A Blockchain database is overseen self-sufficiently using a shared gadget and a circulated time stepping server. They are confirmed records safety is negligible. The use of a Blockchain clears the typical for boundless reproducibility from a propelled asset. [10] It affirms that every unit of considerable really worth become exchanged simply once, tackling the lengthy-standing trouble of twofold spending. Blockchain had been portrayed as an esteem exchange conference. This Blockchain- primarily based exchange of substantial worth may be finished snappier, greater relaxed and less luxurious than with traditional frameworks A Blockchain can relegate identify rights seeing that, whilst legitimately set up to detail the alternate information, it gives a file that urges provide and acknowledgment.

Peer to Peer in Block chain

A peer-to-peer network consists of a group of devices that collectively store and share files. Long back there was client server architecture in that for server clients are connected so in that process client sends response to server and in back server sends response to client. So, if a server stops working suddenly then clients cannot do work as server is not working and all clients are connected to server. To overcome this problem, this research work introduces a peer to peer in this every node acts as server (where every computer can have a copy of data) and if one system stops working then the remaining can work. In blockchain, peer to peer network is used in such a way that a blockchain protocol operates on top of internet, so in peer to peer every computer can send the information from one computer to other as there will be no intermediate consensus like client server architecture.

NFC (Near-field communication)

NFC) innovation is pretty regular in recent times and highlights in most pinnacle of the line superior cells. Just as Just as telephone-to-telephone communication, little NFC labels can likewise be applied to store and change records.[11] You will possibly have seen little NFC labels by means of promotions near transport stops, stickers in shops, or may additionally have even run over the smart concept of making use of NFC empowered commercial enterprise cards.

These tags can keep huge scopes of facts, from brief strains of content material, as an example, an internet address or touch information, to connections to applications inside the Google Play Store. It's a snappy and proficient approach to unexpectedly push data to your smartphone and those little labels can supplant bar and QI codes, and could also be applied instead of Bluetooth at times. So right here's the way by means of which it really works. [12]

Fig 2: 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. There will be no extensive specializations, yet the essential guideline is that loops of wire canbe utilized to deliver electromagnetic waves, which would then be able to be grabbed and transformed once more into current by 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 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.[11]

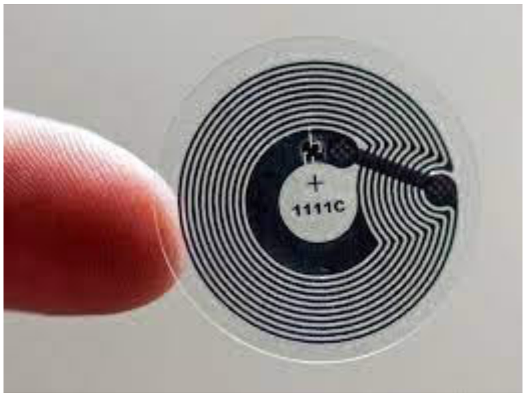

Fig 3: NFC tag

- **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, information will be dumped, 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.

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 has to set block chain storage details and user information in web server application. There is another responsibility of admin he has to write credentials into user NFC card using separate android app. The NFC card has to reach corresponding user safely.

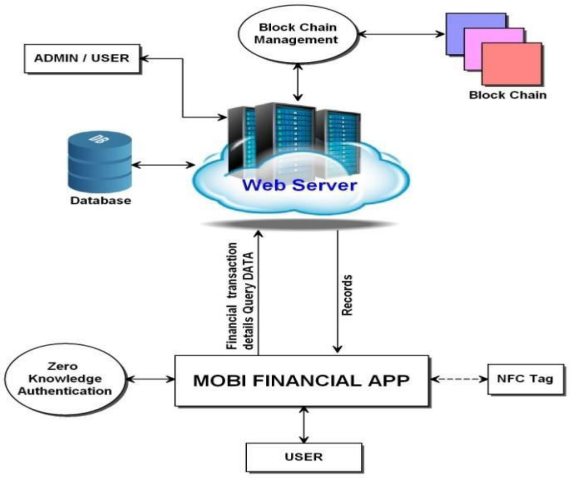

Fig 4: System Architecture

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 particular user same or not. Based on the test result it will take decision whether to allow the user into the home page or not.

With help of NFC user can logged in into mobile financial app he can able to give transactions related request to web server, database connected with web server, all meta data details are stored. All the financial transaction are 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, admin will generate hash code of that user also.

- **NFC card writing process**
  This admin android application is to write user information into 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, the user personal details will be obtained.
- **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.

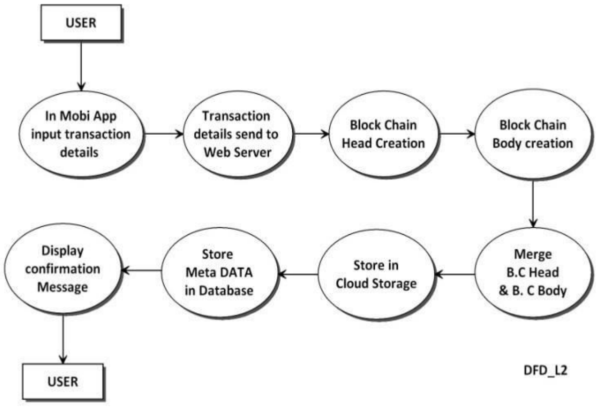
USER
In Mobi App input transaction details
Transaction details send to Web Server
Block Chain Head Creation
Block Chain Body creation
Merge B.C Head & B. C Body
Store in Cloud Storage
Store Meta DATA in Database
Display confirmation Message
USER
DFD_L2

Fig 5: Transaction Block Chain Storage Process

Once transactions are stored in block chain it becomes highly secure and no one can tamper it. This process is shown in Figure 5.

CONCLUSION AND FUTURE SCOPE

A secure mobile application-based data mining is proposed in the research work through block chain technology. To ensure the security the IoT devices, the generated data are stored in cloud storage through block chain which provides better security. Similarly, the data collected through mobile application retrieved from cloud through zero knowledge proof technique which is achieved using near field communication cards. To illustrate the proposed project, financial application is used as an example in the experimentation process. The proposed project achieves better security over IoT data which is suitable for various applications.

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] S. Profis, "Everything you need to know about NFC and mobile payments", CNET, 2014, [online] Available: http://www.cnet.com/how-to/how-nfc-works-and-mobile-payments.

[12] E. Haselsteiner and K. Breitfuß, "Security in near field communication (NFC)", Workshop on RFID security, pp. 12-14, 2006.

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

[14] The Cointelegraph, A Brief History of Ethereum from Vitalik

[15] Buterin's Idea to Release, 2015

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

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

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

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

[20] urae Noether, Review of Ctyptonote White Paper, 2016

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