A Zero-Proof Knowledge Based on NFC for Data Authentication/Protection using Blockchain for Mobile Edge Computing

Hanumantharaju R., Shreenath K. N., Srinivasa K. G., Swetha N.

Abstract: Mobile edge computing is a recent trend to complement the Internet of Things (IoT) ecosystem in the computing sector. IoT is the internet connected communications related to physical devices and everyday objects. The emergence of intelligent living spaces has been due to the rapid development of IoT technologies. Blockchain is one such technology that expands the list of information also referred to like records that are saved as blocks in the Blockchain which are connected using cryptographic algorithms. Within a Blockchain IoT environment, when data or device authentication information is stored in a Blockchain, authentication information can be displayed when verifying Block chain's transactions, which are also referred to as proof of work. A principle of Zero-knowledge proof (ZKF) is implemented in this paper which is a way of proving that knowledge is known without exposing any data to the user. The proposed model uses a Mobile application where users can prove without revealing users' passwords. Blockchain stores client information that can prevent data from being manipulated. The results of applying the ZKF theory for data security are shown through a web application and NFC.

Keywords: IoT; Security; Block Chain; NFC; Mobile edge.

I. INTRODUCTION

IoT incorporates and optimizes manual processes to make them part of the digital age, collecting volumes of data that provide unparalleled level of knowledge. This awareness promotes the creation of smart applications such as enhancing citizens ' management and quality of life by digitizing city services. Cloud computing technologies have contributed over the past few years to provide the IoT with the necessary functionality for analyzing and processing information and turning it into real-time actions and knowledge. The exponential IoT development has opened up new social possibilities such as connectivity and information sharing mechanisms. In these projects, the open data model is the cornerstone. Nonetheless, as has happened in many cases, one of the most significant drawbacks of these programs is the lack of trust. Centralized architectures such as those used in cloud computing have contributed significantly to IoT growth.

It has proved important to combine emerging innovations such as IoT and Cloud. They also understand that the IoT revolutionizes block chain's enormous potential. By providing a trustworthy share service, Blockchain can enrich the IoT with reliable information that can be traced. Data sources can always be established and data remains unchanged over time, thereby improving its protection. Where IoT data is to be exchanged safely among many participants, this implementation would be a major revolution. A major element in ensuring food safety, for instance, is robust traceability of different foodstuffs. The participation of many participants may require Food Traceability: growth, feeding, care, delivery, etc. A data leak throughout any part of the chain may lead to fraud and delay the infectious search processes, which can greatly affect the lives of people and, in the case of a foodborne outbreak, cause enormous financial costs for businesses, industries, and countries. Better control will improve the safety of food, improves data sharing among participants, and decrease search time in the event of foodborne outbreaks that can save people's lives. Moreover, the sharing of reliable data can contribute to the inclusion of new ecosystem participants in other fields, such as smart cities and smart cars. The use of Blockchain can therefore supplement the IoT with accurate and secure data, in which Blockchain technology is the key to solving IoT paradigm scalability, confidentiality, and reliability issues.

IoT which allows objects to exchange and control information between objects because it is connected to the Internet. Malicious attacks can be committed, such as data manipulation or privacy violations, while data is shared over the Internet. Blockchain is such a technology that can provide data manipulation/protection solutions. As the next revolutionary technology, Blockchain technology appeared. The use cases are growing to include finance, the Internet of Things and security.

Manuscript received on February 10, 2020.
Revised Manuscript received on February 20, 2020.
Manuscript published on March 30, 2020.

* Correspondence Author

Hanumantharaju R*., Assistant Professor**,** Department of Computer Science, M.S.Ramaiah Institute of Technology, Bangalore, Karnataka, India. E-mail:hmrcs@msrit.edu

Shreenath K. N., Associate Professor**,** Department of Computer Science, Siddaganga Institute of Technology, Tumkur, Karnataka, India. E-mail: shreenathk_n@sit.ac.in

Srinivasa K. G., Professor, Department of Computer Science, National Institute of Technical Teacher Training & Research, Chandigarh, India. E-mail: kgsrinivasa@gmail.com.

Swetha N., M.Tech Student, Department of Computer Science, M.S.Ramaiah Institute of Technology, Bangalore, Karnataka, India. E-mail:nalluriswetha01@gmail.com

Most private and public sectors are already interested in the technology. Blockchain is a distributed ledger containing linked transaction blocks, which are called blocks connected by crypto algorithms known as a Blockchain [1]. Blockchain is a distributed and decentralized ledger comprising related transaction blocks. The basic concept behind Blockchain is to store accepted transactions as deceptive basis.

Transactions are stored as block (transaction lists) linked to the previous row. The original or the genesis block begins with a Blockchain [3]. The hash value of the previous block is entered after creating a new one. Once a new block was created, any modifications to a preceding block would lead to different hash code, so that all the participants participating in the Blockchain would be immediately visible. Consequently, the distributed transaction ledgers shown in figure 1 are assumed to be tamper-proof. In this paper, we introduced a block chain mechanism that prevents security threats such as the use of mobile finance to counterfeit data. Zero-Knowledge proof, anonymity enhancement in the block chain and NFC technology, was introduced through block investigation to prevent the safety threats of personal data violation. Smart contracts are introduced to prevent the forgery and misuse of personal information that we use for Mobile Financial wallet information.

II. RELATED WORK

Monero, Dash, ZCASH and so on are the block chains with anonymity. An anonymous block chain is a Blockchain which prevents the tracing of an account and the content of transactions, like an account transaction details. It used different security technologies to implement an anonymous block chain. Monroe has used a system to prevent the identification of expired bit coins using the Crypto note protocol for digital assets. It used a particular encryption technique, known as one-time ring signatures. A third party is difficult to verify the quality of a transaction because the key is mixed in a community and the transaction involves a private key [2]. Information technology (ICT) is a fundamental part of smart grid growth and performance .In addition, a complex, efficient, fast communication network is required for connectingthe large volume of distributed elements such as generators, substations, energy storage systems and users, enabling the sharing of data and information needed to manage the system in real time to guarantee improvement in efficiency, reliability and flexibility.

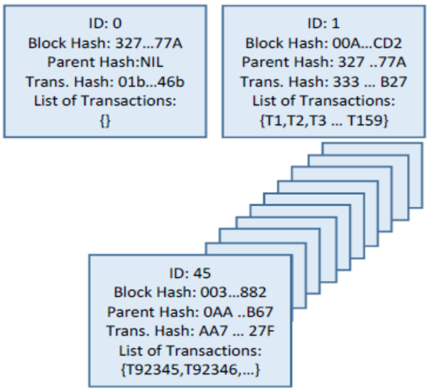


Fig. 1.Sample BlockChain

This paper discusses issues concerning the smart grid architecture in terms of potential applications and criteria for communication by providing or ensure of efficiency, flexible operation, reliability and economics [1]. The risk of fraud is constantly growing in a world full of new technology. This risk existed long before technology was used in the securities industry. Congress promulgated the 1933 Securities Act to combat the risk of fraud and misrepresentation in securities transactions. Investors may take informed decisions before investing by seeking full disclosure. Nonetheless, through the use of block chains and intellectual property contracts decentralized autonomous organizations (DAOs) conduct the selling of shares without disclosing completely the risks or meeting registration provisions under the 1933 Shares Act. However it would destroy this new technology and method of conducting business by compliance with the burdensome registration requirements. In order to prevent this change, Congress must amend the standards for registration to provide a DAO waiver. This exemption must still require that DAOs disclose certain data, whilst reducing current registration burdens, ensuring that investors are informed before investing. Furthermore, due to the unique nature of the Blockchain, smart contract, and DAOs, Congress must impose a fiduciary duty on the creators of DAOs to ensure compliance with the disclosure requirements. Moreover, after the initial crowd sale [3], Congress should consider allowances for burden shifts.

Several governments implement an omnipresent IT project that combines the latest broadband and wireless network technologies to implement an omnipresent wireless network. For Advanced Metering Infra-(AMI) structure, the all-round wireless communication network can be used. This article is therefore directed at the development and implementation of the Zig Bee-based smart power meter through new wireless communications technologies. An error feature is also designed and built into the intelligent meter. For the design of the proposed smart power meter the microcontroller dsPIC30F series is used. A module from ZigBee will then be designed and incorporated into the proposed power meter and transmitted into the rear-end system the detailed data on energy consumption and event discharge. Not only for data collection of energy consumption, but also for data recording of events, can the proposed smart power meter be used. There is great potential for the proposed system for the creation of the AMI in the area. The validity of the proposed system is shown by experimental results. Therefore, ZigBee communication can probably contribute to an omnipresent IT project [2] in the power sector.

III. PROPOSED DATA AUTHENTICATION AND PROTECTION SCHEME USING BLOCKCHAIN

The system architecture defines the layout of the web application's general hypermedia framework. The design of the architecture is linked to the goals set for a Web app, the content presented to the visiting users and the established navigation philosophy. The architecture of the app focuses on the way data and organized objects are viewed and navigated.

The WebApp architecture deals with the design of the software for user interface management, internal storage, results navigation and current content management. In the context of the development environment in the application to be implemented, the WebApp architecture is described as shown in Figure 2.

Figure 3 shows that admin can register, write and read near field interaction system, view a user list and admin can add to, remove or modifying the user information the web application. User may login via the mobile application, tap on the contact card, and upload their vehicle details and/or fixed deposit details etc. Figure 3 shows that admin may access this software.

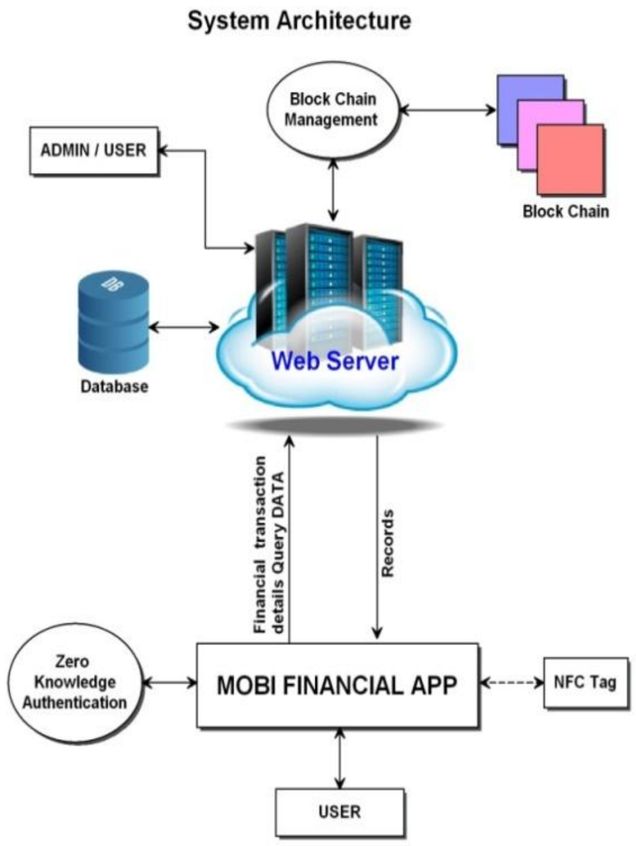


Fig. 2.System Architecture

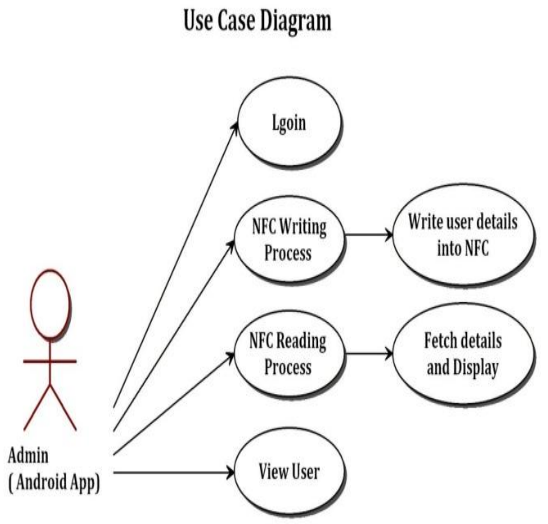


Fig. 3. Use case of admin using mobile application

The user provides his user id and taps near field communication which has hash code stored in it in an encrypted format. The hash code is sent to the server, based on the user Id the hash code is fetched from the databases. The user is checked by the hash code database, the hash code is checked with the hash code database. If this hash code is matched, the user is allowed to login else the user will display the error messages as shown in figure 4.

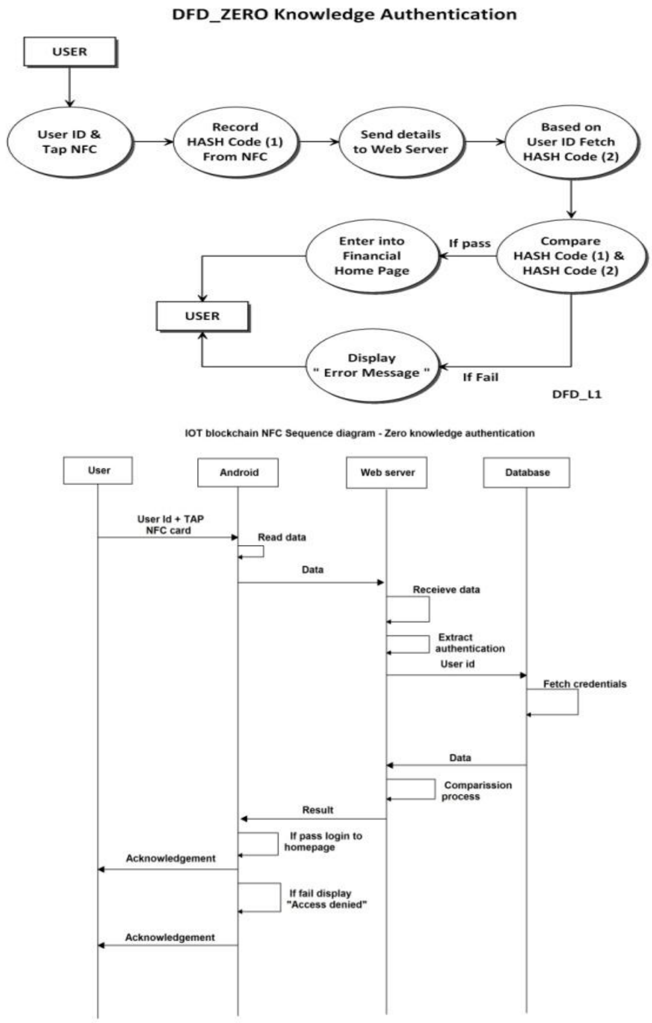

DFD_ZERO Knowledge Authentication
USER
User ID & Tap NFC
Record HASH Code (1) From NFC
Send details to Web Server
Based on User ID Fetch HASH Code (2)
Compare HASH Code (1) & HASH Code (2)
If pass
Enter into Financial Home Page
USER
Display " Error Message "
If Fail
DFD_L1
IOT blockchain NFC Sequence diagram - Zero knowledge authentication
User
Android
Web server
Database
User Id + TAP NFC card
Read data
Data
Receieve data
Extract authentication
User id
Fetch credentials
Data
Comparission process
Result
If pass login to homepage
Acknowledgement
If fail display "Access denied"
Acknowledgement

Fig. 4.Data Flow and Sequence diagram of user authentication.

Modules Description

In this section different modules that constituted to build a system has been identified and showcased their significance namely the use of NFC writing & reading Process, Working of Admin module, use of Zero knowledge authentication in integration with the Blockchain.

- *NFC Writing Algorithm (Tag):*

In this module the User details like NFC Card no., Vehicle No, Date of Registration, Vehicle Type, Vehicle Model and Card Expiry Date will be encrypted using Encryption key and dumped into the NFC tag, before dumping into the card first data is Declare an Intent Filter to announce to the system that it's enabled to work on NFC.

Have a method that Android will call when NFC is detected. Create a method to build a NDEF message. Create a method to write the NDEF (NFC Data Exchange Format) message.

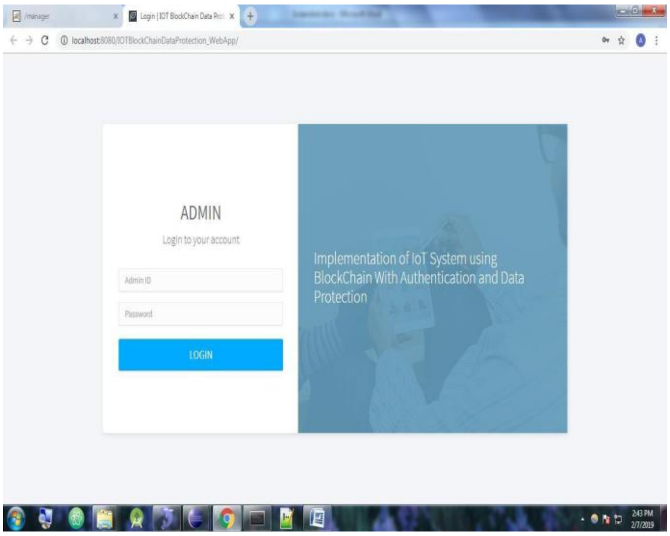
- *NFC Reading Algorithm (Tag):*

When the vehicle owner taps on the card to the android application, first encrypted data is converted into original data with key and reading NFC Data Exchange Format data from a Near Field.
Communication tag with language convention English

- **Admin Module:** Admin can login with his admin id and password. 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.
- **ZERO Knowledge Authentication:** In this module 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 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.

IV. RESULTS AND IMPLEMENTATION

The result is the final result of qualitative or quantitative actions or events taken place. Performance analysis is an operational analysis, constitutes a fundamental quantitative connection between the quantities of performance [19]. Figure 5 shows that admin may link to or delete a user by using admin I d and the administrative key. Figure 6 shows that admin can add user by entering details such as user identity, name, email, dob, gender etc. The list of users added by admin is shown as in Figure 7. Figure 8 shows that administrators can also edit user data such as address, user identification, etc. The following is shown in Figure 9 that a user can be deleted by the user ID and name. Figure 10 shows that you can access the NFC code via the mobile app. Figure 11 demonstrates that the user can provide the necessary information on his vehicle. Figure 12 demonstrates that once the details are applied, the client will access his vehicle details.



/manager
Login | IOT BlockChain Data Pro
localhost:8080/IOTBlockChainDataProtection_WebApp/

ADMIN

Login to your account

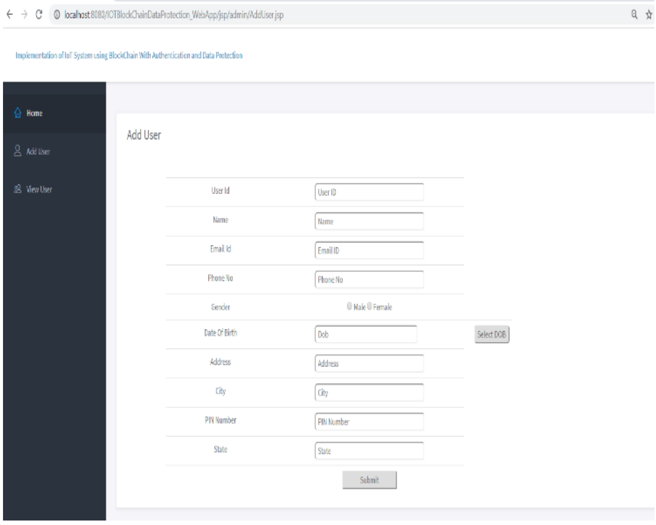
Admin ID

Password

LOGIN

Implementation of IoT System using BlockChain With Authentication and Data Protection

Fig.5.Admin Login



localhost:8080/IOTBlockChainDataProtection_WebApp/jsp/admin/AddUser.jsp
Implementation of IoT System using BlockChain With Authentication and Data Protection
Home
Add User
View User

Add User

User Id: User ID

Name: Name

Email Id: Email ID

Phone No: Phone No

Gender: ○ Male ○ Female

Date Of Birth: Dob [Select DOB]

Address: Address

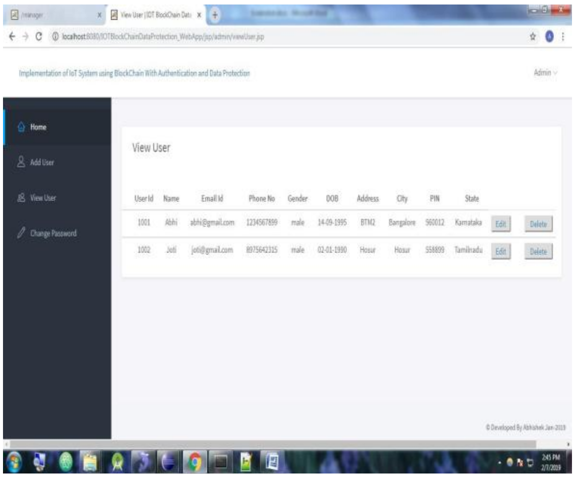
City: City

PIN Number: PIN Number

State: State

Submit

Fig.6.Add User

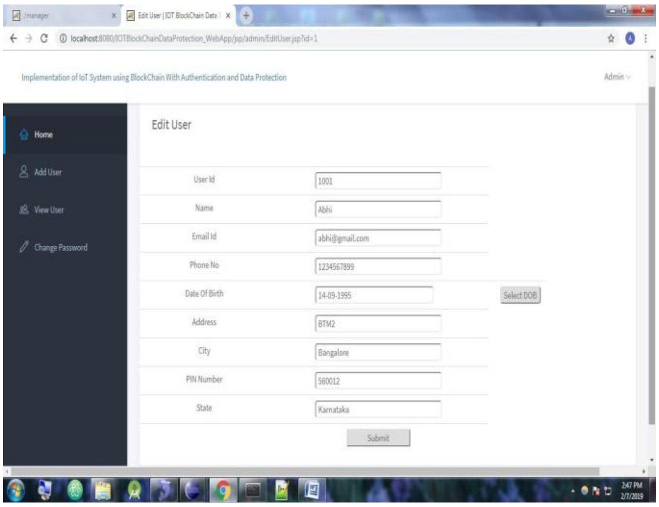


/manager
View User | IOT BlockChain Data
localhost:8080/IOTBlockChainDataProtection_WebApp/jsp/admin/viewUser.jsp
Implementation of IoT System using BlockChain With Authentication and Data Protection
Admin
Home
Add User
View User
Change Password
© Developed By Abhishek Jan 2019
2:45 PM
2/7/2019

View User

User Id	Name	Email Id	Phone No	Gender	DOB	Address	City	PIN	State		
1001	Abhi	abhi@gmail.com	1234567899	male	14-09-1995	BTM2	Bangalore	560012	Karnataka	Edit	Delete
1002	Joti	joti@gmail.com	8975642315	male	02-01-1990	Hosur	Hosur	558899	Tamilnadu	Edit	Delete

Fig. 7.View User



/manager
Edit User | IOT BlockChain Data
localhost:8080/IOTBlockChainDataProtection_WebApp/jsp/admin/EditUser.jsp?id=1
Implementation of IoT System using BlockChain With Authentication and Data Protection
Admin
Home
Add User
View User
Change Password
2:47 PM
2/7/2019

Edit User

User Id: 1001

Name: Abhi

Email Id: abhi@gmail.com

Phone No: 1234567899

Date Of Birth: 14-09-1995 [Select DOB]

Address: BTM2

City: Bangalore

PIN Number: 560012

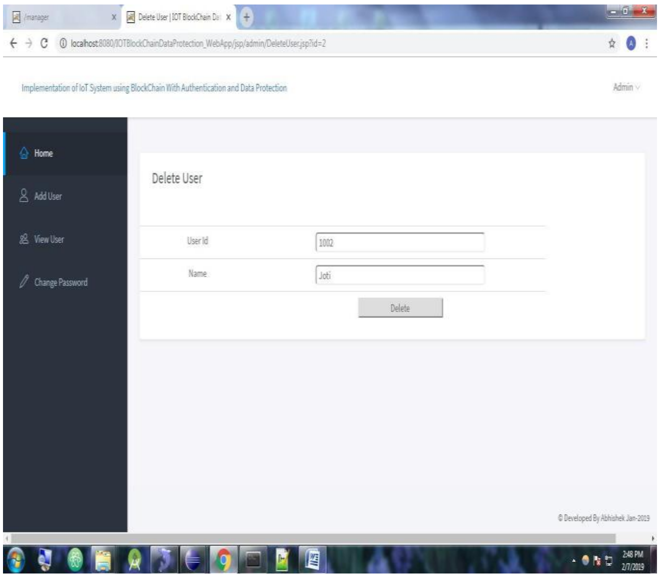
State: Karnataka

Submit

Fig. 8. Edit User

Retrieval Number: F8520038620/2020©BEIESP
DOI:10.35940/ijrte.F8520.038620
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication


/manager
Delete User | IOT BlockChain Da
localhost:8080/IOTBlockChainDataProtection_WebApp/jsp/admin/DeleteUser.jsp?id=2
Admin
Home
Add User
View User
Change Password
Delete
© Developed By Abhishek Jan-2019
2:48 PM
2/7/2019

Implementation of IoT System using BlockChain With Authentication and Data Protection

Delete User

User Id	1002
Name	Joti

Fig. 9.Delete User

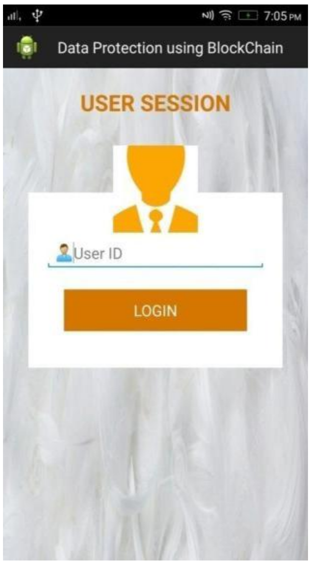


Fig. 10.User Login

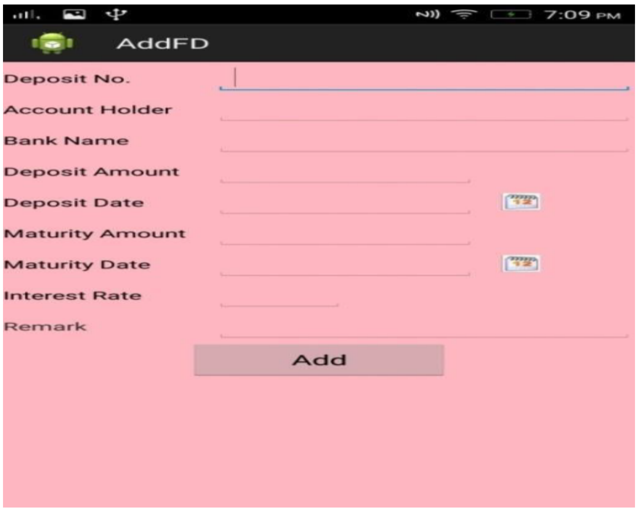
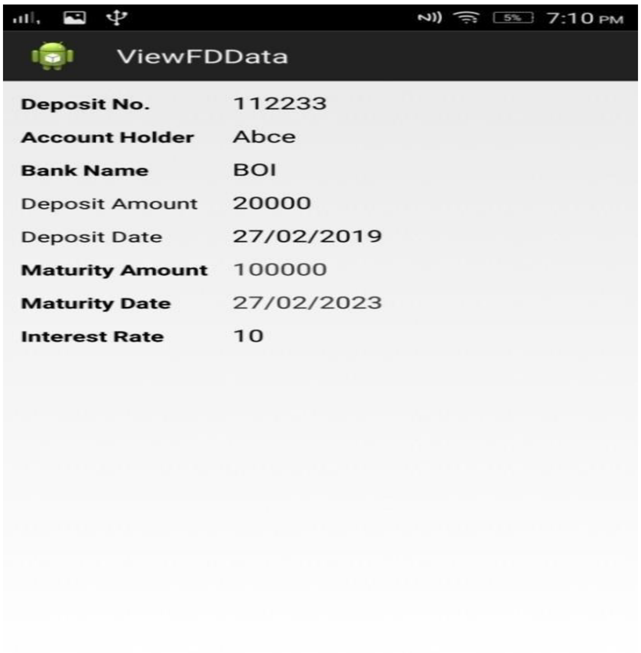


Fig. 11. Add Details



Deposit No.	112233
Account Holder	Abce
Bank Name	BOI
Deposit Amount	20000
Deposit Date	27/02/2019
Maturity Amount	100000
Maturity Date	27/02/2023
Interest Rate	10

Fig. 12.View Details

V. CONCLUSION

We use a mobile application in this project to use a protocol for authentication of users via NFC using zero information evidence. NFC hash code serves as a user's password and also a public key which will be stored in the block chain without the original data being stored in the block chain thus not revealing the actual data. Where the original data is stored in the server database. Here the user can login only by typing the authenticated NFC, and the user's data stored is encrypted by block chain format with a zero information protocol. The key to decrypting user data is with in Blockchain.

REFERENCES

1. J. Demuro, *Here Are the Ten Sectors That BlockChain Will Disrupt Forever*,TechRadarPro,16Jan2018,https://www.techradar.com/news/here-are-the-10-sectors-that-blockchain-will-disrupt-forever.
2. B. Dickson, *Blockchain Tech Could Fight Voter Frau-dand These Countries Are Testing It*, VentureBeat, 22 Oct. 2016; https://venturebeat .com/2016/10/22/blockchaintech-could-fight-voter-fraud-andthese-countries-are-testing-it.
3. J. Hall, *Can Blockchain Technology Solve Voting Issues?, Bitcoin Magazine*,7 Mar. 2018; https://www.nasdaq.com/article/can-blockchain technology-solve-voting-issuescm931347.
4. A. Sandre, *Blockchain for Voting and Elections, Hack- ernoon*, 14 Jan. 2018;https://hackernoon.com/blockchain-for-voting-and-elections-9888f3c8bf72.
5. G. Prico, *Sierra Leone Pilots Blockchain- Based Voting for Political Elections*, 22 Mar. 2018;
6. B. Miller, "*Blockchain Voting Startup Raises $2.2M*," *Government Technology*,8Jan.2018;http://www.govtech.com/biz/Blockchain-Voting-Startup-Raises-22M.html.
7. A. Perala, "*Voatz Raises $2.2 Million in Seed Funding*," Mobile ID World,9Jan.2018;https://mobileidworld.com/voatz-seed-funding-901093.

8. M. Hochstein, "*Moscow's Blockchain Voting Platform, Adds Service forHigh-RiseNeighbors*,"CoinDesk,15Mar.2018;https://www.coindesk.com/moscows-blockchain-voting platform-adds-service-for-high-rise neighbors.
9. "*Digital Home Blockchain Voting System, Active Citizen in MoscowOpens*,"BitccoinExchangeGuide.com; https://bitcoinexchangeguide.com/digital-home-blockchain-voting-system-active-citizen-in-moscow-opens .Nick Szabo, The Idea of Smart Contracts, 1997.
10. The Cointelegraph, *A Brief History of Ethereum From Vitalik*.Buterin's Idea to Release, 2015.
11. Ryan Cheu, an *Implementation of Zero Knowledge Authentication*, 2014.
12. Eli Ben-Sasson, *Zerocash: Decentralized Anonymous Payments from Bitcoin*, 2014.
13. Surae Noether, Review of Cytptonote White Paper, 2016. Charles RackoffDaniel R. Simon, *Non-Interactive Zero-Knowledge Proof of Knowledge and Chosen Ciphertext Attack*, Annual International Cryptology Conference, 19.

AUTHORS PROFILE

Hanumantharaju R, is Assistant professor in Dept. of CSE, M.S.Ramaiah Institute of Technology, Bangalore. He is currently a Research Scholar pursing Ph.D. from VTU. His area of interest is Internet of Things, Edge Computing, embedded systems and distributed systems.

Shreenath KN, is Associate professor in Dept. of CSE, Siddaganga Institute of Technology, Tumkur. He has completed Ph.D. from Jawaharlal Nehru Technology University, Ananthapur, His area of interest are Distributed systems, Theory of computation and Wireless sensor networks.

Srinivasa K G, is Professor at National Institute of Technical Teacher Training & Research, Chandigarh, He received his PhD in Computer Science and Engineering from Bangalore University in 2007. He is the recipient of All India Council for Technical Education – Career Award for Young Teachers, Indian Society of Technical Education. His research areas include Data Mining, Machine Learning and Cloud Computing

Swetha N. is currently pursuing M.Tech in Computer Science from M.S.Ramaiah Institute of Technology. She is working as Intern in Unisys, Bangalore.

Retrieval Number: F8520038620/2020©BEIESP
DOI:10.35940/ijrte.F8520.038620
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication