Privacy Preserving Authentication Technique- Trust by Computation

Amruta Narayan Hegde[1] Prof. Padmashree T[2]
[1]M. Tech Student [2]Assistant Professor
[1,2]Department of Information Technology
[1,2]RV College of Engineering®, Bengaluru-59, India

Abstract— Internet is a revolution of modern world technology. It is becoming inseparable and integral part of every walk of life. In this world of new technology the risk of fraud is also constantly increasing. With the growing usage of internet by people, protection of important information has become the need of the hour. If computer is not having required security controls, the system can be easily infected with malicious logic and thus any type of necessary information can be accessed. As an aid to data privacy and security, the concepts of Zero-Knowledge Proof, Near Field Communication and Blockchain have now poised to redefine online privacy. This paper provides a framework for enabling secure data authentication and storage that helps in secure application development.

Keywords: Blockchain; Zero-Knowledge Proof (ZKP); Near Field Communication (NFC)

I. INTRODUCTION

Digital technologies are revolutionizing modern world. They are changing people's lives from almost all facets. They have become part of how people live, interact, socialize and involve in business. Internet and World Wide Web have made data to be available on demand and smart phones make data available wherever we go. It is estimated that already around 15 billion devices are online; and by 2020 it may go up to 26 to 50 billion. Data pool is increasing which entails need for storage. Thus technology is shifting to cloud. With increasing availability, usefulness, complexity of data maintenance and security is also increasing.

Many of the security protocols underpinning today's networks are not built with security in mind. As a result current security practices have some loopholes [1]. They lag behind the evidence-based engineering standards. This leaves the cyber space vulnerable to both known and unknown risks. Since the digital security has pivotal importance, the security tools need to overcome the vulnerabilities to keep up with and catch up the security demands.

Cyber security or information security aims to protect the data, networks, programs or applications from unauthorized and illegal access, damage or change. In other words it includes those activities or operations that are employed to reduce threats and all kind of susceptibilities. The main objective of cybernetics is to enforce necessary policies to prevent attacks, recovery, data assurance and other cyber security related activities. It covers all the mechanisms and processes that protect digital equipment, information and records from illegal or unintended access, manipulation or destruction. In computing context the system security consists cyber security and physical security- both of them are used to provide protection against unauthorized access to data stored and other computerized devices. Information security is the part of cybernetics which intends to maintain confidentiality, integrity and availability of data.

The number of technological inventions has made modern life much easier. Numbers of applications are touching different aspects of life. Most of the applications are characterized by data storage and transfer. In order to make them the most reliable means of communication, suitable authentication and privacy preserving policies must be employed. Extensive research in the field of information security has come up with new hope to enhance the security of the system. Combination of concepts like Zero-Knowledge Proof and Blockchain are paving way in designing new security measures.

The rest of the article is organized as follows: Section II gives some related works behind the proposed work. Section III describes Theory and Concepts that is used for providing secure data authentication and storage. Section IV Methodology and Section V give implementation and results. Section VI gives insight on security analysis of the proposed work. The article is concluded in section VII

II. RELATED WORK

This is the era of Near Field Communication (NFC) technology. It was jointly developed by Philips and Sony in 2002 for contact less communications. This short-range technology finds number of applications in digital world as they are designed exclusively for safe interaction between two devices. Currently NFC card are used in payment, social media, transportation and health care domains.

NFC provides anonymous end-to-end mutual authentication which helps in establishing mutual trust. Authors [2] use this principle to build a Near Field Communication (NFC) framework which can provide secure mutual authentication and attestation for mobile devices. The novel technique is lightweight and robust compared to other schemes.

The authors in paper [3], explained how to apply blockchain and Zero Knowledge Proof (ZKP) for data privacy and protection. They proposed smart meter system enables data authentication using ZKP and stores the data in database using the concept of blockchain. The proposed application can protect the data using ZKP as it does not allow third party to access data and prevent the data stored against data tampering with the usage of blockchain concept. The proposed Advanced Mitigation Infrastructure mitigates the risk of modifying the power data transmitted in smart grid environment to charge low or high. Through smart contract that have Zero Knowledge proof make transactions such as power trading in smart grid convenient and safe.

III. THEORY AND CONCEPTS

The blockchain technology has credited a new and exciting opportunity to financial industries through its decentralized ledger property. Today the most widely known blockchain application is Bitcoin. This is the world's first digital currency application, where transaction involving currency

requires no third party to establish trust between two parties. Though Bitcoin technology has not been legally recognized all over the world, it is finding its applications beyond the financial sectors. The concept of blockchain along with zero knowledge proof is evolving as the most promising combination to enhance the privacy of the data stored by the application.

A. Blockchain

Blockchain uses concept cryptography and hash values to enable a medium for secure transaction. It uses verification and validation technique to make application highly resistant against data forgery and data tampering. It uses mechanism that verifies hash values before confirming any transaction. Figure 1 shows how transaction is made using blockchain.

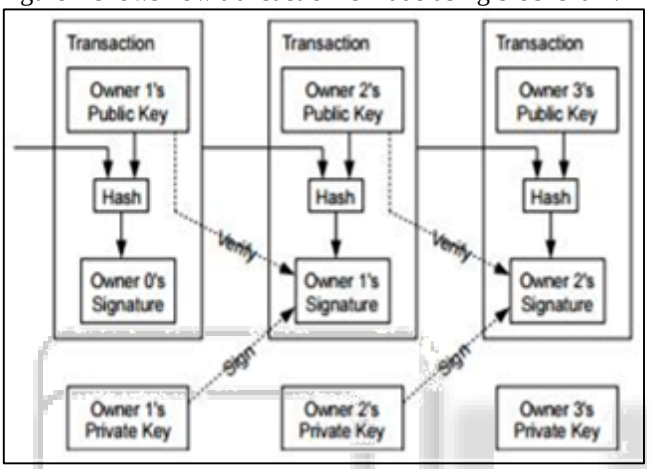

Fig. 1: Transaction in Blockchain

1) Near Field Communication Technology

Near Field Communication (NFC) is a short-range, wireless connectivity technology that uses magnetic field induction to enable communication between electronic devices in close proximity. NFC devices are gaining popularity day by day. World wide availability of NFC devices help in the creation of the secure applications as it provides small range communication between two devices. Figure 2 shows how NFC card communicates with mobile devices.

Fig. 2: Communication between NFC tag and smartphone

2) Zero Knowledge Proof

Zero Knowledge Proof protocol is one of the powerful tools that cryptographers have ever devised. It is the method by which one party (prover) can prove his credentials to another party (verifier) without revealing any information. Thus it serves as the important building block of an application to achieve privacy for the users, and enhance security of the system. Figure 3 shows Zero Knowledge proof interactive system.

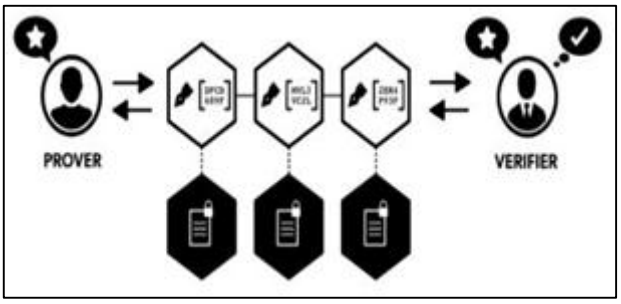

Fig. 3: Zero Knowledge Proof interactive systems

IV. METHODOLOGY

In the proposed system environment, the Privacy Preserving Authentication application is developed to demonstrate secure authentication and data storage using the concepts of Zero Knowledge Proof, Near Field Communication and Blockchain. The proposed application has several main modules like Admin module, NFC reading process, NFC writing process etc. User application uses NFC card to login, thus it help in providing secure authentication. Once the user enters into the application he/she can use it to store personal information. The details are stored using the concept of blockchain. Thus security threats and personal information infringement can be avoided. Also concept of cloud is used to enable distributed data storage. Figure 4 shows architecture diagram of the proposed mobile application system. It gives the overview of the application by depicting the communication between different modules.

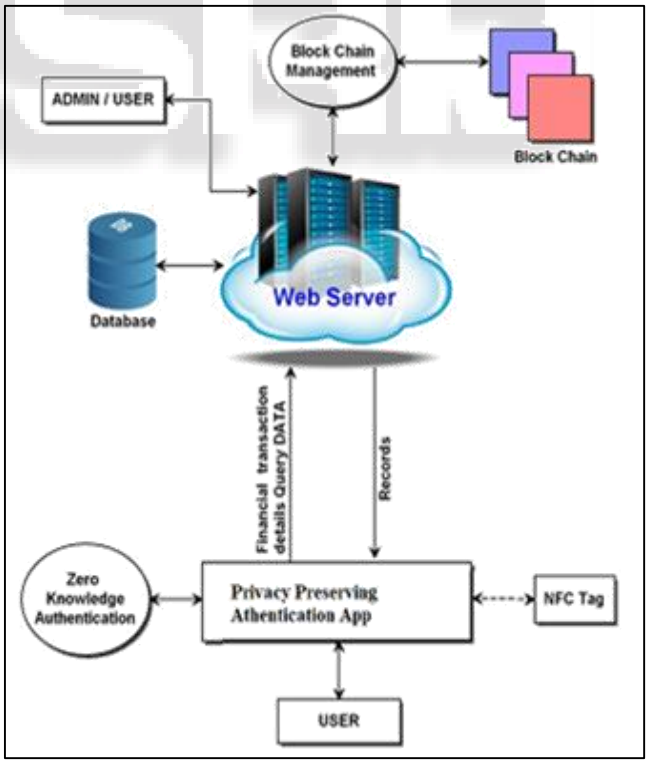

Fig. 4: System architecture

The admin can control the web server and Privacy Preserving Authentication application has to be installed in the user android mobile phone. Admin issues NFC card to user by writing secret hash code into it. User can login to the application through Zero Knowledge Proof using Near Field Communication (NFC) card. To enter into application user

has to give User Id and tap the NFC card. The mobile application fetches the hash code from user card and sends to web server. Based on the user ID and hash code (1) the web server fetches already stored hash code(2) and compares two hash codes. If the match is found correct home page is displayed to user. After logging in to application user can store his personal information using the application. The details are sent to cloud and stored using the concept of blockchain. Thus data is prevented from being modulated.

Digital world came up with new hope to secure user information by introducing passwords. But one has to make passwords more complex to protect it against hacking and keep remembering lot of passwords. This necessitated the need of novel technique that is more convenient to use as well as secure. However Near Field Communication (NFC) tags came up as ray of hope to be integrated with authentication techniques. This helps to transfer data between two devices by merely bringing them together. This technology has singled the death of passwords.

Once user logs into the application he/she will be able to store any sensitive information using the application. For example bank account details. User adds his account details, which will be encrypted and stored as file. The hash code of the file path is generated and stored into the database as the identifier of the data file. Each time the hash code of the previous data is fetched before storing the data file to cloud. Thus the chain of data blocks is created which makes it highly impossible for unauthorized user to fetch any specific or personal information.

V. EXPERIMENT AND IMPLEMENTATION

The proposed system consists of user authentication using NFC card. NFC devices are gaining popularity day by day. World wide availability of NFC devices help in the creation of the secure applications as it provides small range communication between two devices. Figure 5 shows user authentication using Near Field Communication (NFC) card.

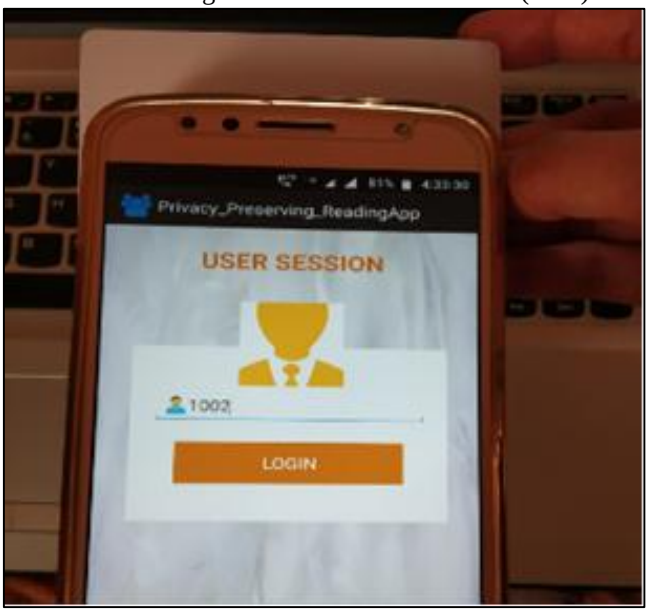

Fig. 5: User Authentication using NFC card

As shown in the figure, user has to give User ID and should tap NFC card. The application reads hash code from NFC card and checks with the already saved hash code for the corresponding user. If match is found user will able to enter into home page of the application.

This novel technique is the transition to new way of authentication by making passwords obsolete. In the current scenario, one has to remember secret information like passwords, PIN etc. which users usually do not prefer. Thus they try to keep such passwords, PIN or any other secret information that will be easy to remember. Such weak passwords will be highly vulnerable to cyber-attacks and results in data leakage. The proposed technique overcomes issues mentioned above. Here users need to carry only NFC card. There is no any additional burden of remembering passwords. Thus NFC finds its significant usage in developing smart authentication scheme.

Once the user gets access he/she can use the application to store personal information. For example if he wants to save banking details, he can use the application to store information like account number, deposits, bank name, deposit amount etc. The entire information is encrypted and stored as file before creation of chain of information blocks. Since the data is encrypted it is highly impossible for hackers to get unauthorized access and fetch the details.

Figure 6 shows user interface for adding personal information. User can store any kind of information like life insurance details, bank details, vehicle details etc.

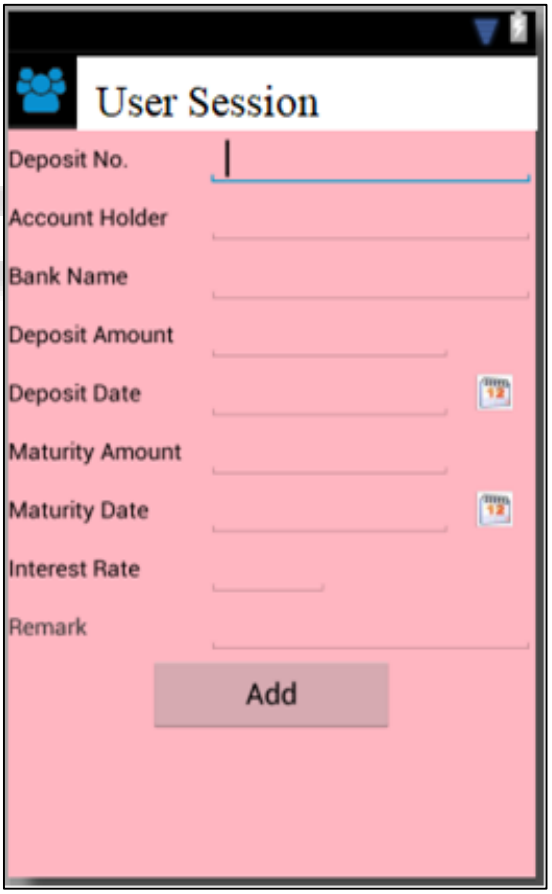

Fig. 6: User Interface for adding personal details

The data collected is saved in the form of a file as shown in the Figure 7. To protect the data from unauthorized access it is encoded using Advanced Encryption Standard (AES) algorithm. After encrypting the data the hash code of file path is generated.

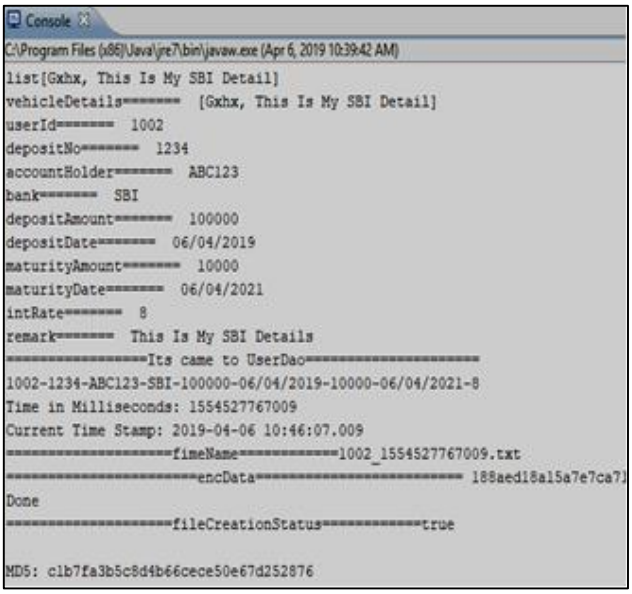

Fig. 7: Encryption and hash code generation

The hash code of the file path will be stored separately in database. Before storing the data, the hash code of the previous file is obtained to create chain of blocks. This paper demonstrates blockchain creation using cloud spaces by randomly choosing any block space available (i.e. the spaces already created like cloud 1, 2 etc) in the cloud. After saving data, user will be acknowledged with successful message. Figure 8 shows snapshot which depicts data storage into cloud.

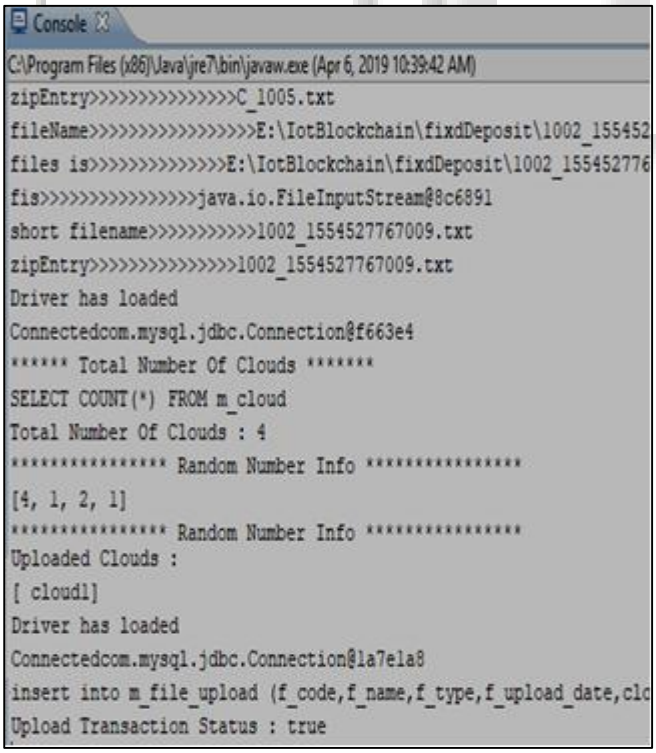

Fig. 8: Storing of data block into cloud

VI. Security Analysis

Near Field Communication (NFC) is based on contactless smartcard technology, helps in secure authentication by using hashing of authentication code, encryption and decryption. In addition to this, the wireless communication technology limits the communication between two devices to be within short distance. This reduces opportunities for an attacker to eavesdrop on communication and, adding security and privacy. Also NFC has following benefits:

- Ease of use: Since it enables contactless communication between two devices.
- Security: It uses secure channel for communication and uses data encryption for sending information.
- Versatility: NFC embraces number of applications ranging from data authentication to banking and other business services.

Also use of blockchain concept ensures that data is encrypted which makes it difficult to modify. The encrypted hash codes used to identify each data blocks and, separation of hash code and file data helps to provide anonymity to information stored.

VII. Conclusion and Future Work

This paper proposes secure data authentication using Near Field Communication technology. This smart card technology enables two devices to securely transfer data between to devices. It comes with the number of security features like proximity protection i.e. if unauthorized user wants to access it he/she must stand uncomfortably close to the device which brings out first level of defense. In addition to this, in includes features like user initiation i.e. user has to actively initiate its usage etc. But due less demand and popularity most of the devices are not supporting NFC. Thus in future more and more android applications have to come to support it. Similarly concept of blockchain is demonstrated using cloud. This also has to be developed so that this idea can be implemented use heterogeneous data storage environments.

Acknowledgment

Project work is supported as part of major project for M.Tech, Information Technology Post Graduate Program in the RV College of Engineering®, Bengaluru-560059.

References

[1] C C Sun, A Hahn and Chen-Ching Liu "Cyber Security of power grid: State of Art", International Journal of Electrical Power and Energy Systems 2018 Vol.99, pp. 45-56.

[2] L M Jalili, M Y Beh, " Double Authentication Locking System Using NFC Technology and Password", Journal of Computing Technologies and Creative Content 2018 Vol 3

[3] Chan Lee, Ki-Hyung Kim "Implementation of IoT System using Blockchain with Authentication and data protection", IEEE conference on Information Networking, Thailand 2018

[4] Tiago M, Paula Fraga-Lamas, "A Review on the Use of Blockchain for the Internet of Things" IEEE Access 2018 Volume 6

[5] Gungor, V. Cagri, et al. "A survey on smart grid potential applications and communication requirements." IEEE conference on Industrial Informatics, Vol.9, No.1, 2017, pp. 28-42.

[6] Gangale, Flavia, Anna Mengolini, and Ijeoma Onyeji., "Consumer engagement: An insight from smart grid projects in Europe.", Energy Policy, Vol.60, 2017, pp.621-628
[7] Luan, Shang-Wen, et al. "Development of a smart power meter for AMI based on ZigBee communication", Power Electronics and Drive Systems, 2017. International Conference on. IEEE, 2017.
[8] Huh, S., Cho, S., Kim, S., "Managing IoT devices using blockchain platform", in Proceedings of the 19th International Conference on Advanced Communication Technology (ICACT), Bongpyeong, South Korea, 19-22 Feb. 2017.
[9] Karafiloski, E., Mishev, A., "Blockchain solutions for big data challenges: A literature review", in Proceedings of the IEEE International Conference on Smart Technologies, Ohrid, Macedonia, 6-8 July 2017.
[10] Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., Amaba, B., "Blockchain technology innovations", in Proceedings of the IEEE Technology & Engineering Management Conference (TEMSCON), Santa Clara, United States, 8-10 June 2017
[11] Sung-Hoon Lee, Device authentication in Smart Grid System using Blockchain, KAIST, 2016.
[12] Tian, F., "An agri-food supply chain traceability system for China based on RFID & blockchain technology", in Proceedings of the 13th International Conference on Service Systems and Service Management (ICSSSM), Kunming, China, 24-26 June 2016.
[13] Tschorsch, F., Scheuermann, B. "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies", in IEEE Communications Surveys & Tutorials, vol. 18, no. 3, Mar. 2016, pp. 2084-2123.
[14] Andreas M, Masteing Bitcoin: Unlocking Digital Cryptocurrencies, pp.49-68, O' REILLY, 2015
[15] Youngu Lee, A Study for PKI Based Home Network System Authentication and Access Control Protocol, KICS '10-04Vol.35No.4
[16] Singh, S., Singh, N. "Blockchain: Future of financial and cyber security", in Proceedings of the 2nd International Conference on Contemporary Computing and Informatics (IC3I), Noida, India, 14-17 Dec. 2016, pp. 463-467.
[17] Tschorsch, F., Scheuermann, B. "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies", in IEEE Communications Surveys & Tutorials, vol. 18, no. 3, Mar. 2016, pp. 2084-2123.
[18] Tschorsch, F., Scheuermann, B. "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies", in IEEE Communications Surveys & Tutorials, vol. 18, no. 3, Mar. 2016, pp. 2084-2123.
[19] Christidis, K., Devetsikiotis, M., "Blockchains and Smart Contracts for the Internet of Things", in IEEE Access, vol. 4, pp. 2292-2303, May 2016.
[20] Swan, M. "Blockchain: blueprint for a new economy". First Edition, O'Reilly Media, Jan. 2015.

