International Journal of Applied Engineering and Technology ISSN: 2277-212X
An Open Access, Online International Journal Available at http://www.cibtech.org/jet.htm
2022, Vol.12, pp.145-148/Rajakani et al.
Research Article

BLOCK CHAIN BASED SECURE ACCESS OF USER DATA IN IOT

***Rajakani V[1], Balamurugan L [2], Krishnapriyan S [3], Keerthivasan R [4] and Praveen M [5]**
[1]Department of Electronics & Communication Engineering, Anjalai Ammal MahalingamEngineering College, Kovilvenni, Thiruvarur-District
[2, 3, 4,5] UG student, Department of Electronics & Communication Engineering,
Anjalai Ammal MahalingamEngineering College,
Kovilvenni, Thiruvarur-Dist.
**Author for Correspondence: rajakani.v@gmail.com*

ABSTRACT

Net-banking user datas are electronically-stored account transaction information in a digital format. Blockchain is the revolutionary invention of the twentieth century that offers a distributed and decentralized setting to communicate among nodes in a list of networks without a central authority. Three categories of blockchain-based potential solutions have been proposed by researchers to handle EHRs: conceptual, prototype, and implemented.

INTRODUCTION

Blockchain has been a buzzword in Information and Communication Technology industry in recent years. The rise of this new technology has greater potentials to solve data privacy, security, and integrity issues. The word blockchain came in the front line after the publication of the Bit coin white paper by Satoshi Nakamoto in 2008 [1]. The fundamental mechanism behind Bit coin is to make financial transactions possible without the intervention of a trusted third party. The technology is mainly considered a distributed Peer to Peer (P2P) network where digital data may publicly or privately be allocated to all users on the web in a secure and verifiable way. In traditional financial transactions, both sender and receiver need to depend on a Trusted Third Party (TTP), e.g., bank. It involves a few security issues and operational difficulties. For instance, a TTP gets access to a user’s financial data, which indicates the lack of user privacy. Moreover, the time involved in a TTP transaction is lengthy as there are many steps in between the operation. Furthermore, users need to pay the TTP for their service. Bit coin solves the above limitations and makes the TTP vanish for a successful transaction between two users.

In practical Bit coin crypto currency came into the market in 2009. However, since the code for Bit coin was open source, other programmers could edit and improve Bit coin. The blockchain technology has evolved in different phases.1 • Blockchain 1.0: The use of Distributed Ledger Technology (DLT) contributed to the first and most noticeable use of the technology: crypto currencies. Blockchain 1.0 is the first crypto currency that uses a transparent mechanism to monitor bit coin transactions on a shared ledger. • Blockchain 2.0: Doing transactions through some legally binding policies, also called Smart Contracts, which are generated from a set of small computer programs, is considered blockchain 2.0. The most prominent blockchain in phase 2.0 is Ethereum. • Blockchain 3.0: The next incarnation in this technology is blockchain 3.0, which focuses on Decentralized Applications (DApps) by avoiding centralized infrastructure. Unlike traditional apps, DApps store and communicate through decentralized storage and decentralized server. The aim of blockchain 3.0 was to popularize blockchain among conventional sectors, government, health, and education. • Blockchain 4.0: It provides solutions and methods that can meet several business demands of Industry 4.0, which involves automation, resource planning, and integration of various execution programs. It requires enhanced trust and privacy which can be met by blockchain. Many surveys have been published on the application of blockchain in various areas.

BLOCKCHAIN FRAMEWORKS

Blockchain technology is an association of two technologies, cryptography, and P2P. A blockchain is a series of time stamped blocks connected through a cryptographic hash. Typically each block contains transaction records verified by the peers, called miners. The chain is increased continuously, and each new block is added to the end. However, each new block contains a reference, basically a cryptographic hash (e.g., SHA-256), of the previous block's header. The creation of each block ensures anonymity, transparency, and immutability [15]. The whole operation of blockchain is held in a P2P network. The basic structure of a blockchain is shown in Fig. 1. Each block except the genesis block (first block of the network) has the hash value of data from the previous hash. Besides, each block has a difficulty value called Nonce, a Timestamp, and other attributes (e.g., the list of transactions)

1) P2P NETWORK

A P2P network works more or less like a Bit Torrent network,4 where a peer, commonly known as a node, not only deploys the system for its benefit but also contributes to the whole system with its resources like storage, bandwidth, and processing power. Depending on the blockchain network type (discussed in a later section), the network node is restricted to fewer people or open for all. The bright side for nodes in the blockchain is that their identity is kept safe, as only the user's public key is shown to the other peers of the network. Nodes also work as miners, who validate a transaction to be added to the chain

TYPES OF BLOCKCHAIN

This section contains a description of different types of blockchain. Depending on the network size, application, and kind of consensus algorithms (seen below), blockchain has various kinds. Commonly, three types of blockchain exist in the market, mentioned below. • Public • Private • Consortium (Hybrid)

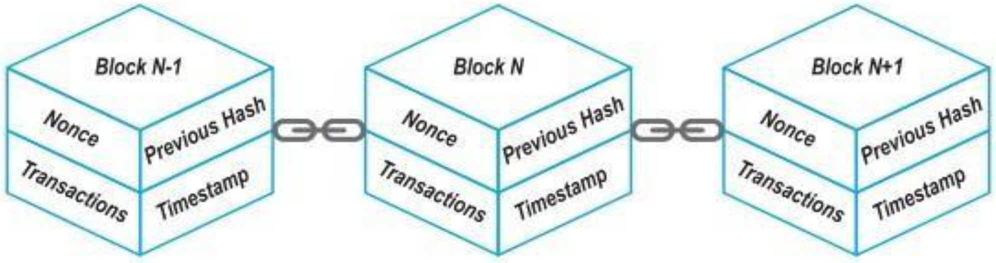

Figure 1: A standard structure of a blockchain.

***Consensus Algorithms*:**

Consensus algorithm is the heart of Blockchain technology since they maintain the integrity and security of the blockchain network. It is a protocol by which network nodes of the blockchain arrive to a standard agreement on current records state of the ledger. Different blockchain platforms use different algorithms to reach the consensus and of course all of them differ in their operation and execution. Figure 3 shows the list of most popular consensus algorithms used in different blockchain platforms. Basic working principle behind these algorithms is as given below: i. Proof of Work (PoW) In PoW, nodes with more computing power administers the network. ii. Proof of Stake (PoS) In PoS, nodes with more money administers the network. iii. Proof of Authority (PoA) In PoA, arbitrary chosen trustworthy nodes administers the network. iv. Proof of Elapsed Time (PoET) In PoET, nodes who have finished specific waiting period administers the network. v. Delegated Proof of Stake (DPoS) In DPoS, Nodes elected by delegates through voting administers the network

Proposed Methodology:

- The proposed model is a face recognized & data analysis management system in the sense that user canenter the name.
- And take images is confirmed before the transaction is accepted in the main database.
- Using these system customers of that particular bank can make their transactions through net banking facerecognition without visiting bank.
- A centralized database is maintained by particular bank of India where user information is maintainedwhenever user is using face recognition net banking system

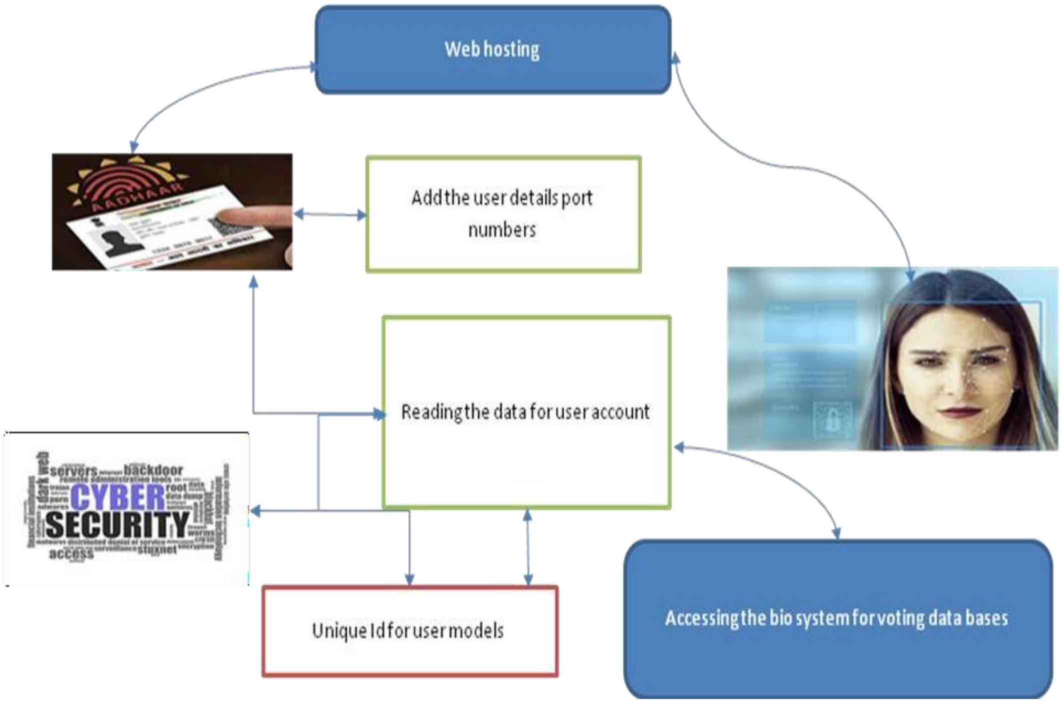
Web hosting
AADHAAR
Add the user details port numbers
Reading the data for user account
CYBER SECURITY
Unique Id for user models
Accessing the bio system for voting data bases

Figure 2: **Work Flow diagram**

***Linear Regression for Face Recognition*:**

- LRC approach segments a given occluded image and reaches individual decisions for each block. These intermediate decisions are combined using a novel Distance-based Evidence Fusion (DEF) algorithm to reach the final decision.
- The LRC algorithm works really well on faces without any rotation and under nominal lightning conditions (i.e. accuracy above 99%).
- Conclusions and Future Works :

The issues related to the security and privacy of the IoT system are immense and require careful consideration. There are some pros and cons to both centralized and decentralized solutions. Centralized solutions are constrained by scalability, while decentralized approaches are bound by delays, computational overheads and energy constraints. We proposed a multi-agent system to provide lightweight, decentralized IoT access control security mechanisms. Blockchain Managers (BCMs) are responsible for providing the necessary security for access control, securing communication between local IoT devices, fog nodes, core fog nodes and cloud computing. The proposed architecture is a generalizable solution that can be applied to various IoT applications. Furthermore, IoT's issues are not fully addressed in prior studies, as most studies focus on addressing access control issues in a specific IoT application such as a smart home. The authors understand that research evaluation is must be based on implementation and testing phases that specify the solution's applicability and effectiveness compared to related research. However, this research is still in progress and the authors believe that the results of these two phases should be published in a separate paper due to the expectation that a great number of details will need to be discussed, as well as new contributions. In future research, the proposed framework will be implemented in a real environment to measure the achievement of the fundamental security goals in relation to integrity by applying the digital signature, authentication via shared secret keys, authorization via the MAC policyand confidentiality via public key encryption. We will examine various solutions to solve the big header size problem in the blockchain. A possible solution is to separate the header block access control policy from the blockstructure in the blockchain and place the access control policy in a separate policy file blockchain or in a separate encrypted text file. The proposed architecture will be enhanced in this domain and we will apply a case study for IoT applications that requires a high level of security. The Raspberry PI IoT device will be used for thedeployment of the solution and we will use a private blockchain platform in its deployment. Further details will be included in future works. Author Contributions: Conceptualization, S.A., F.E. and K.A. (Khalid Almarhabi).

REFERENCES

Ouaddah, A.; Mousannif, H.; Elkalam, AA.; Ouahman, AA. Access control in the Internet of Things: Big challenges and new opportunities. Comput. Netw. (2017), 112, 237–262. [CrossRef]

Aldowah, H.; Rehman, SU.; Umar, I. Security in Internet of Things: Issues, Challenges and Solutions. In International Conference of Reliable Information and Communication Technology; Springer: Cham, Switzerland,(2018); pp. 396–405.

Ourad, AZ.; Belgacem, B.; Salah, K. Using blockchain for IOT access control and authentication management. In International Conference on Internet of Things 2018 June; Springer: Cham, Switzerland, (2018); pp. 150–164.

Ravidas, S.; Lekidis, A.; Paci, F.; Zannone, N. Access control in Internet-of-Things: A survey. J. Netw. Comput. Appl. (2019), 144, 79–101. [CrossRef]

Ouaddah, A.; Mousannif, H.; Ouahman, AA. Access control models in loT: The road ahead. In Proceedings of the (2015) IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA), Marrakech, Morocco, 17–20 November(2016); pp. 272–277.

Jia, J.; Qiu, X.; Cheng, C. Access control method for web of things based on role and SNS. In Proceedings of the (2012) IEEE 12th International Conference on Computer and Information Technology, Chengdu, China, 27–29 October 2012; pp. 316–321. [CrossRef]

Xu, R.; Chen, Y.; Blasch, E.; Chen, G. Blendcac: A blockchain-enabled decentralized capability-based access control for iots. In Proceedings of the (2018) IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August (2018); pp. 1027–1034. [CrossRef]

Novo, O. Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. IEEE Internet Things J.(2018), 5, 1184–1195. [CrossRef]

Dorri, A.; Kanhere, SS.; Jurdak, R. Blockchain in Internet of Things: Challenges and Solutions. Yingyong Kexue Xuebao/J. Appl. Sci.(2020), 38, 22–33. [CrossRef]

Gao, W.; Hatcher, WG.; Yu, W. A survey of blockchain: Techniques, applications, and challenges. In Proceedings of the (2018) 27th International Conference on Computer Communication and Networks (ICCCN), Hangzhou, China, 30 July–2 August (2018). [CrossRef]

Dorri, A.; Kanhere, SS.; Jurdak, R.; Gauravaram, P. Blockchain for IoT security and privacy: The case study of a smart home.