International Journal of Aquatic Science
ISSN: 2008-8019
Vol 12, Issue 02, 2021

Secure Healthcare System Based On Blockchain And Public Key Cryptography

P Arul[1], S Renuka[2]

[1]*Research Supervisor, Department of Computer Science, Government Arts College (Affiliated to Bharathidasan University, Trichy-24), Tiruchirappalli-620 022, India*
[2]*Assistant Professor, Department of Computer Science, Government Arts College (Affiliated to Bharathidasan University, Trichy-24), Tiruchirappalli-620 022, India*

Email: [1]phdarul2004@yahoo.co.in, [2]spkumarrenu@gmail.com

Abstract: Growing healthcare is very essentials nowadays. In the present situation, healthcare organizations are facing a serious problem in sharing medical information without giving up the privacy and integrity of information. Also an important research issue is to store large volume of health information and provide safety towards tampering and misuse of records. This paper aims to address the issues of information security and authentication in healthcare. Blockchain technology has the probable of immutability, integrity and decentralized architecture to manage records of the health sector. Here, we propose a blockchain based system using public key cryptography to be tamper resistant and secure the information. Our proposed architecture provides numerous opportunities for healthcare industry such as reduced transaction costs, increased transparency for regulatory reporting, effective healthcare data management and healthcare records universality.

Keyword: Blockchain, Public key cryptography, healthcare system.

1. INTRODUCTION

In the time of electronic framework patients are desirous of dealing with their data on the web. Most of the traditional healthcare management uses centralized ledger architecture. Thus, for managing and securing large amounts of medical records from unauthorized users is a challenge for any healthcare organization. Hence effective security mechanisms are needed for the healthcare sectors that are developing exponentially regarding medical data storage. The blockchain is the best approach to share and store the information of a healthcare organization securely with time-stamped [1]. In this work, we proposed the blockchain that gives decentralized, distributed and transparent architecture.

Usually, a patient visit more than one health professionals, e.g., general physicians , specialists, trained professionals, clinics, pharmacies, for different needs in the current health sectors, where users' health records that is issued by a health provider are stored in provider's data base system. Blockchain permits blocks to be get-together into blocked and the blocks are recorded in cryptographically chains in chronological order. In current healthcare organization used symmetric cryptography for data security hence it gives faster performance than asymmetric cryptography [2].

One of the major problem in symmetric cryptography is digital signature authentication, and the receiver can never identify that the information is coming from the authorized healthcare

providers. Another problem is sending private key every time using some secure channel and there is chance of security violation while sharing private key. Hence, the symmetric cryptography method in the blockchain is not given proper solution for authentication and data security in healthcare sector. To solve these difficulties, we propose public key cryptography (PKC) that use a digital signature and their associated keys as an authentication mechanism. Further, it is a way to reliably recognize the user claim to be the owner of a specific public key. In public key cryptography mechanism has public-private unique key pair for reliably recognize each and every user in healthcare system. Anyone can check the accuracy of an information using the public key and at the same time security of data is also not compromised due to the encryption of data by private key.

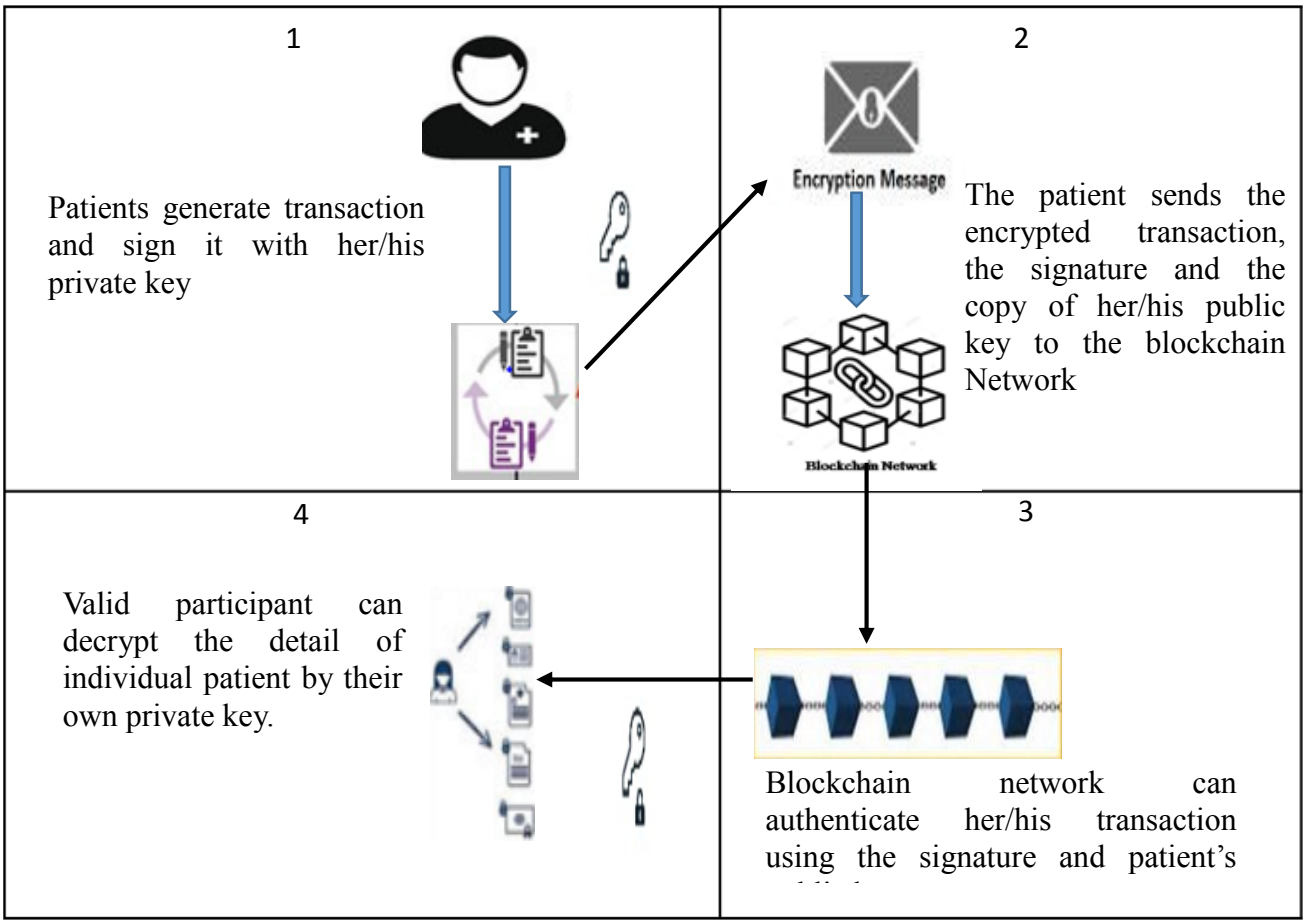

Fig .1. Authentication process for healthcare transactions on the Blockchain

Theodouli et al [3] presented the system that allows healthcare data sharing and permission managing in a secure, private and auditable way by unique properties of the Blockchain technology. This paper the author consider the frames of Patient Data Integrity, Patient pseudonymity, Workflow automation and Auditing and accountability. However this blockchain based healthcare system take more time of in verification for sharing the data. Brunner, Clemens et al [4] introduce and combine the most significant properties of blockchain and Public Key Infrastructures(PKI) and provide some directions for remove central trusted third parties with contemporary blockchain based PKI implementations. Zhang, Peng et al [5] addressed how interoperability of healthcare data should be maintained in blockchain. Here, patient Id is used for symmetric cryptography and the same is used for

the information sharing between participants. Esposito et al [6] provide the use of blockchain technology to protect the healthcare data hosted within cloud data and they have to give integrate access control with attribute-based encryption cryptographic methods. Srivastava, Gautam et al [7] gives an in depth look at blockchain technology in t
healthcare Internet of Things and proposed three

the healthcare frame work as Healthcare Blockchain System Using Smart Contracts for Patient Monitoring, Privacy-Preserving Blockchain Based IoT Ecosystem and a Decentralized Privacy-Preserving Healthcare Blockchain for IoT were presented and the security and their limitation were discussed.
Jiang, Shan et al [8] propose BlocHIE, a Blockchain-based platform for healthcare information exchange and provide two fairness-based packing algorithms to improve the system throughput and the fairness among users jointly. Mikula et al [9] proposed a framework for identity and access management using hyperledger Blockchain technology to support authentication and authorization of entities in Electronic Health Records (EHRs). Saxena, Aumreesh Ku et al [10] proposed an efficient symmetric cipher technique can encrypt any size and various types of files example .txt, .exe, .cpp, .com, .sys, etc.
While the study of literature, mostly discusses the symmetric key for data security in the healthcare system, thus work on public key cryptography in healthcare system is not concentrated. We have used a system which make sure data security by public key cryptography.

2. HEALTHCARE SYSTEM USING BLOCKCHAIN

A Blockchain is a chain of blocks that uses a distributed peer-peer network, and everyone is allowed to join. Blockchain network has the potential of immutability, integrity and decentralized architecture to manage the health records of the patient. This system proposed a blockchain based secure framework using public key cryptography. In healthcare system the providers give the medical data to the individual patient, who is a valid user of the following system and also validate the security key of the patient before the submission of the patient transaction. When any validate patient creates a new block, the new block is sent to all the users on the healthcare system network. The combined data will be encrypted using digital signature and hash functions. After all the verification Encrypted information are sequentially grouped into block. Each block is attached to the previous block and immutably recorded across a healthcare system using public key cryptographic mechanisms. When someone enters this network, it will get the full copy of the Blockchain. Likewise, blockchain of this healthcare network consists of a complete indexed history, patient's unique identifier and an encrypted link to the health record. Each record is time stamped. All patient records including their history are chained together. Patients have control over their health records. In this way, the history of all accesses is stored on the blockchain that provides a full view of all events that have happened to each record, and hence guarantees data integrity and prevents misuse of users' records. The valid participants like doctor, insurance organization and other hospital organization has to share their public key to get access of an individual patient record of the blockchain in the healthcare system otherwise they cannot get the complete details of the patient. That the valid participant can decrypt the detail of individual patient by their own private key.

4. PUBLIC KEY CRYPTOGRAPHY FOR BLOCKCHAIN

In Public Key Cryptography is to generate Public and Private Key pair for the authentic patient while sharing the data. Fig. 2 describes how the information will be encrypted by and stored as blocks in blockchain network for further communication of combined data among valid participants. A user has pair of keys: public key that are widely distributed, and private key is kept secret that are only known to the valid patient. With compare to symmetric cryptography, PKC provide data security and authentication. The sender encrypt data by the receiver public key, so that only authorized receiver can decrypt the message by the private key. The originality of message cannot be tempered owing to the secret key technique of PKC. However digital signature is created by the sender for authentication of the valid sender so that receiver can easily find whether the information has been changed by intermediate man or not. Similarly digital signature verification is done at the receiver end to verify the authentication of the sender by matching the message.

5. CONCLUSION

The proposed system has been used with Blockchain and Public Key Cryptography (PKC) for security and authentication in Healthcare data. This paper presented the healthcare system for data sharing using blockchain to access the data with all the valid user. The existing healthcare system is used the symmetric cryptography mechanism which is not very secure for valuable medical data. The proposed system is able to provide a valid participants and provide to an authorized one. The proposed system has been implemented using public key cryptography techniques which identified the valid participant and to provide data security as well as authentication.

6. REFERENCE

[1] Conti, Mauro, E. Sandeep Kumar, Chhagan Lal, and Sushmita Ruj. "A survey on security and privacy issues of bitcoin." IEEE Communications Surveys & Tutorials 20, no. 4 (2018): 3416-3452.

[2] Zhang, Xiaoshuai, and Stefan Poslad. "Blockchain support for flexible queries with granular access control to electronic medical records (EMR)." In 2018 IEEE International conference on communications (ICC), pp. 1-6. IEEE, 2018

[3] Theodouli, Anastasia, Stelios Arakliotis, Konstantinos Moschou, Konstantinos Votis, and Dimitrios Tzovaras. "On the design of a blockchain-based system to facilitate healthcare data sharing." In 2018 17th IEEE International Conference on Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), pp. 1374-1379. IEEE, 2018

[4] Brunner, Clemens, Fabian Knirsch, Andreas Unterweger, and Dominik Engel. "A Comparison of Blockchain-based PKI Implementations." In ICISSP, pp. 333-340. 2020.

[5] Zhang, Peng, Michael A. Walker, Jules White, Douglas C. Schmidt, and Gunther Lenz. "Metrics for assessing blockchain-based healthcare decentralized apps." In 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom), pp. 1-4. IEEE, 2017

[6] Esposito, Christian, Alfredo De Santis, Genny Tortora, Henry Chang, and Kim-Kwang Raymond Choo. "Blockchain: A panacea for healthcare cloud-based data security and privacy?" IEEE Cloud Computing 5, no. 1 (2018): 31-37

[7] Srivastava, Gautam, Reza M. Parizi, and Ali Dehghantanha. "The future of blockchain

technology in healthcare internet of things security." Blockchain Cybersecurity, Trust and Privacy (2020): 161-184

[8] Jiang, Shan, Jiannong Cao, Hanqing Wu, Yanni Yang, Mingyu Ma, and Jianfei He. "Blochie: a blockchain-based platform for healthcare information exchange." In 2018 ieee international conference on smart computing (smartcomp), pp. 49-56. IEEE, 2018

[9] Mikula, Tomas, and Rune Hylsberg Jacobsen. "Identity and access

[10] Management with blockchain in electronic healthcare records."In 21st Euromicro conference on digital system design (DSD), pp. 699-706.

[11] IEEE, 2018

[12] Saxena, Aumreesh Ku, Sitesh Sinha, and Piyush Shukla. "A new way to enhance efficiency & security by using symmetric cryptography." In 2017 International Conference on Recent Innovations in Signal processing and Embedded