International Journal of Future Generation Communication and Networking
Vol. 13, No. 4, (2020), pp. 1911–1919

A Smart Decentralised Framework To Track Patients Health Information Using Electronic Health Record With Block Chain Technology

Dr.R.Priscilla[1],Dr.S.Geetha[2]
[1]*Professor*,[2]*Professor*
[1,]*St.Joseph's Institute of technology, Shollinganallur, Chennai, Tamil Nadu, India.*
[2,] *School of Computing Science and Engg. VIT University Chennai Campus Chennai, Tamil Nadu, India*
[1]*prisci.christa@gmail.com*,[2] *geethabaalan@gmail.com*

ABSTRACT

Cyber world with health care system gradually increased when compared with the last decades. A technology innovation on the health care system plays vital role in the medical industries. The patient's details were manipulated in the cloud environment with various types of application which may leads to high risk in protecting the data from the hackers or the intruders. This paper proposed a decentralized framework which used to track and monitor the patient's information in the medical industries using a electronic health record with new innovated block chain technology. This paper classified into two strategies, first consist of proposed a block chain technology with decentralized system to control the mechanism using smart contract with electronic health record. The second strategies with high security in the form hash value creation, privacy preserving and cryptocurrency with middleware. This paper provide an effective and efficient decentralized framework to track and secured the patients' health record with block technology

Keyword *:Electronic Health Record; Patient Health Information* ***;****Cryptocurrency*

I. INTRODUCTION

Block chains have attracted interest as an innovative technology designed to lower transaction costs by securely enabling direct transactions among an indeterminate number of mutually untreated users.

BLOCK CHAIN MINERS

The newly created block in the block chain needs to be mined before it is added to the block chain. A peer-to-peer computer process, Block chain mining is used to secure and verify bit coin transactions. Mining involves Block chain miners who add bit coin transaction data to Bit coin's global public ledger of past transactions. In the ledgers, blocks are secured by Block chain miners and are connected to each other forming a chain.Miners validate new transactions and record them on the global ledger (block chain). On average, a block is mined every ten minutes. Miners compete to solve a difficult mathematical problem based on a cryptographic hash algorithm. The solution found is called the Proof-Of-Work. This proof proves that a miner did spend a lot of time and resources to solve the problem. When a block is 'solved', the transactions contained are considered confirmed, and the ethereum concerned in the transactions can be spent.

Miners receive a reward when a single transaction in carried out in the block chain. Bit coin mining is the process of adding transaction records to Bit coin's public ledger of past transactions or block chain. This ledger of past transactions is called the block chain as it is a chain of blocks. Mining requires high computational power. The miners in the block chain network get rewards for performing the mining.

DISTRIBUTED LEDGER

Distributed Ledger Technology (DLT) is a digital system for recording the transaction of assets in which the transactions and their details are recorded in multiple places at the same time. Unlike traditional databases, distributed ledgers have no central data store or administration functionality. In a distributed ledger, each node processes and verifies every item, thereby generating a record of each item and creating a consensus on each item's veracity. A distributed ledger can be used to record static data, such as a registry, and dynamic data, i.e., transactions.

ISSN: 2233-7857 IJFGCN

Ledgers which are essentially a record of transactions and similar data have existed for millennia in paper form. They became digitized with the rise of computers in the late 20th century, although computerized ledgers generally mirrored what once existed on paper. However, throughout history, a central authority needed to validate the authenticity of the transactions recorded in the ledgers. For example, banks need to verify financial transactions. Block chain, which bundles transactions into blocks that are chained together, and then broadcasts them to the nodes in the network, is probably the best-known type of distributed ledger technology.

ELECTRONIC HEALTH RECORD

Electronic Health Record (EHR) contains sensitive information of the patients that are managed by the healthcare providers. The attackers steal the EHR from the health applications and demand for ransom or bit coins. Loss of health record leads to wrong medication of patient that may result in loss of life.

Blockchain is a shared, immutable transaction record between nodes without an intermediator. Blocks in the block chain are linked to each other and stored in a distributed ledger. Each block in the blockchain possesses a timestamp, data, hash, previous hash, nonce, and difficulty, private and public keys. Timestamp is used to identify the block creation time. Hash is created from the data using a secure hashing algorithm. Previous hash references the hash of the block immediately ahead of the current block. Nonce is an arbitrary value to ensure the uniqueness of the block in a block chain and secure the block from a replay attack. Difficulty is a value used to prefix zeros in the hash value that is adjusted each time according to the duration required for the mining process. The public key and the private key is used to create and send digital signature during the transaction.

The blockchain is a decentralized and distributed system, in that all the nodes must verify a transaction. Validation of the transaction is termed as mining process. Adding the block to the blockchain is done by anyone in the network. Before adding a block to the blockchain, it is necessary to perform a Proof-of-Work (PoW). PoW is a mathematical puzzle that uses nonce and difficulty value to ensure the difficulty of the block mining process. The first block in blockchain is referred as a genesis block. Data and the hash value together used to create the digital signature that is verified by the miners.

CRYPTOGRAPHIC HASH FUNCTION

A Cryptographic Hash Function (CHF) is a hash function that is suitable for use in cryptography. It is a mathematical algorithm that maps data of arbitrary size to a bit string of a fixed size (the "hash value", "hash",) and is a one-way function, that is, a function which is practically infeasible to invert. The only way to find a message that produces a given hash is to attempt a brute-force search of possible inputs to see if they produce a match, or use a rainbow table of matched hashes. Cryptographic hash functions are a basic tool of modern cryptography. Cryptographic hash functions add security features to typical hash functions, making it more difficult to detect the contents of a message or information about recipients and senders.

Hashing is a method of cryptography that converts any form of data into a unique string of text. Any piece of data can be hashed, no matter its size or type. In traditional hashing, regardless of the data's size, type, or length, the hash that any data produces is always the same length. A hash is designed to act as a one-way function you can put data into a hashing algorithm and get a unique string, but if you come upon a new hash, you cannot decipher the input data it represents. A unique piece of data will always produce the same hash. Hashing is a mathematical operation that is easy to perform, but extremely difficult to reverse. (The difference between hashing and encryption is that encryption can be reversed, or decrypted, using a specific key.) The most widely used hashing functions are MD5, SHA1 and SHA-256.

II. RELATED WORK

This section explains the various researches related to the existing blockchain protocols for the Internet of Things (IoT) networks.

In this paper Q E Abbas describes blockchain is one of the technologies which appeared in the last decade and brought a lot of promise with it. Many researches are being conducted actively to explore the full capabilities of Blockchain. Some believe that Blockchain is key for a decentralized

ISSN: 2233-7857 IJFGCN

society. Especially, we are considering blockchain as the security scheme to protect the privacies of the objects to be augmented in Intelligent Mobile Augmented Reality (IMAR) project.

In BL Radhakrishnan describes the use of Electronic health records in possessing the patient's medication details and their health history. The health records attract the attention of the attackers' as it possesses invaluable information. Loss of electronic health record leads to a wrong medication or surgery. Healthcare systems provide fewer security measures to secure the health records. Blockchain is a distributed and decentralized ledger that plays a vital role in securing the data and transactions. Introduction of blockchain in the healthcare systems protects the health records from the attackers. However, the blockchain faces phishing, dictionary-based, cold wallets, and hot wallets attacks. This paper proposes a multilevel authentication-based scheme to protect the blockchain from the attacks. Electronic Health Record (EHR) contains sensitive information of the patients that are managed by the healthcare providers. The attackers steal the EHR from the health applications and demand for ransom or bitcoins. Loss of health record leads to wrong medication of patient that may result in loss of life.

S. Vyas work proved the power of machine learning in understanding the patterns in data, analyzing and making decisions, its importance in various sectors. Machine Learning requires reasonable amount of data to make accurate decisions. Data sharing and reliability of data is very crucial in machine learning in order to improve its accuracy. The decentralized database in Blockchain Technology emphasizes on data sharing. The consensus in Blockchain technology makes sure that data is legitimate and secured. The convergence of these two technologies can give highly accurate results in terms of machine learning with the security and reliability of Blockchain Technology. This paper gives an overview of how combining these two technologies can help in healthcare sectors. Data is a very important resource in machine learning. The data can also be used in preprocessing techniques for improving research environments [6]. The data can be gathered from interviews, questionnaire, surveys, and studies or generated electronically over the internet. The quality as well as quantity of data improves efficiency, classification and prediction rate in machine learning. Machine Learning models have proved their significance in various sectors like healthcare, transportation, e-commerce, and marketing.

F. M. Enescu discussed about the notion of block technology how they can be applied in the health sector. This system is decentralized and cannot be controlled, and records cannot be modified. Blockchain technology offers efficiency and low health costs. In this way, the health of the population is monitored worldwide, by using an encryption program for the storage of patients' databases in diagnosis, laboratory analysis, medical imaging, medicine etc. Users are encouraged to use such a platform in a peer-to- peer market to have permanent access to medical history, and last but not least, to support the medical act for a correct diagnosis, research system and pharmaceutical industry. The objective of this paper is to achieving a technology that will make the medical system more efficient by decentralization, faster access to information and the creation of a solid database that will bring essential predictability to the system.

The existing system is a centralized distribution system; hence medical data intrusion is always possible. In existing system, there is no data privacy, lack of network security, very less reliability of electronic health record sharing among cloud servers. Also in the existing system, single point of failure can happen any time thus raising data non-availability. The current healthcare system faces high storage issue and thus leads to much time in data retrieval performance.

The proposed blockchain technology based EHR, thus providing decentralized system. We design a trustworthy access control mechanism using smart contracts to achieve secure EHRs sharing among different patients and medical providers involving hospitals and pharmacist as well. In the proposed system the patient can register and provide the patient health information which would be converted into a single has value using SHA 256 algorithm and embed into a QR code. The doctor, hospital can view the patient permitted information using the hash value. The doctor can prescribe the medicine which would be converted into another block and this block can be viewed by the pharmacist and automatically respective invoice would be prepared. Then, finally we integrate machine learning technique to analyze the patient disease and recommend medicine to the patients. Also we integrate crypto currency i.e, Ethereum preserving sensitive health information against

ISSN: 2233-7857 IJFGCN

potential threats. The crypto currency can be used to book and pay for obtaining a respective doctor appointment.

III PROBLEM STATEMENT

The Fig1 Block Chain design for E-Health Systemdescribes the overall structure of the system and complete overview is obtained from its view.

In Fig.1, an E-health scenario on a mobile cloud platform where patient records are gathered from a network of local gateways and stored on a public cloud for sharing with health care providers as showing in Fig.1 E-health records may include personal information and medical history which are provided by patients. Patients have their own patient ID and are classified based on their current living area with an area ID. It is infeasible to store medical data on blockchain, we suggest to only keep addresses of patients on blockchain, while large medical records are stored on decentralized cloud storage. Further, to manage medical records, a cloud EHRs manager is proposed.

Thus, in order to retrieve a certain health record on cloud, a participating entity needs to know patient addresses which are visible on the blockchain network. The data flow of the proposed mobile cloud blockchain system. Next, we assume that each health provider (such as a doctor, physician or a nurse) has a mobile phone to retrieve EHRs on the cloud with their ID. By this way, they can acquire medical history on cloud storage for the medical analysis. For example, a doctor can access EHRs of a patient to analyze medical records and diagnose health problems for providing proper healthcare services. We also develop a cloud blockchain network for EHRs sharing.

The system authenticates whether the person logging in is an authorized user or not. If the authentication was successful then the patients can register their details and the unique hash value will be generated for each patients. The user requests are handled by request handler. The patients can convey their diseases as user request to request handler. Once the patient conveys their diseases as request, the doctors are able to view the respective patient's disease and can suggest the prescribed medicines from the data storage. The type of disease is identified from various similar data present in the data storage.

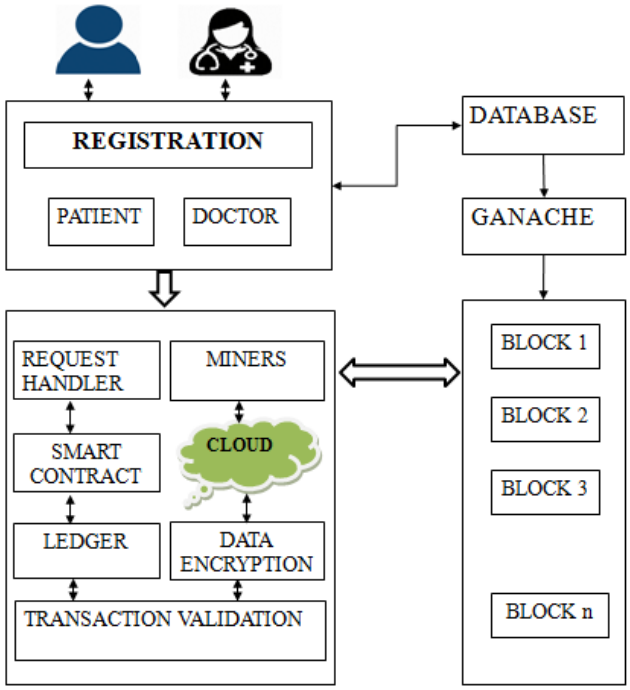

Fig.1 Block Chain design for E-Health System

REGISTRATION

Users of the system (doctors and patients) register their details using a registration module. Registration module collects details of the user. Doctor need to submit the name, mobile number, email id, date of birth, address, and registration number. Every doctor in the system belongs to one of the associated healthcare providers. Patient needs to submit the name, mobile number, Email id, date

ISSN: 2233-7857 IJFGCN

of birth, address and health insurance details. Besides, doctors and patients need to provide a valid password.

SMART CONTRACT CREATION

A smart contract is a kind of self-operating computer program, which can be executed automatically when specific conditions are met. In the Ethereum blockchain, a smart contract is a special account, which contains data and code with multiple programmable functions. Users can use their Ethereum account to interact with smart contracts via Application Binary Interfaces (ABI). Functions defined in smart contracts can be triggered by a new transaction sent from an account. This property allows entities to implement their job functionalities such as data transmission, request handling or access management.

A smart contract is a stand-alone script usually written in Solidity and compiled into binary or JSON and deployed to a specific address on the block chain shown in Fig.2. In the same way that we can call a specific URL endpoint of a RESTful API to execute some logic through an HttpRequest, we can similarly execute the deployed smart contract at a specific address by submitting the correct data along with the necessary Ethereum to call the deployed and compiled Solidity function.

From a business standpoint, it means that smart contract functions can be inherently monetized. Importantly, smart contract functions don't have to cost Ethereum to be run. In simple terms, we can see a smart contract as a collection of code stored in the block chain network that defines conditions to which all parties using the contract agree upon.

Fig.2 Smart Contract Operation

BLOCK CREATION

Patient has to approve the EHR notification received. EHR verification by the patient avoids double-spending types of attacks. After the successful verification of EHR, the Block Generator module in Fig.3 generates a block containing the EHR details. Each block in a blockchain contains the hash of the block data. The EHR is hashed using the key provided by the Key Generator Module.

The hash of the previous block is, so to speak, the chain of blockchains. Because the hash of the previous block is contained in the hash of the new block, the blocks of the blockchain all build on each other. Without this component, there would be no connection and chronology between each block. All transactions contained in a block can be aggregated in a hash. This is the root hash of the Merkle tree.

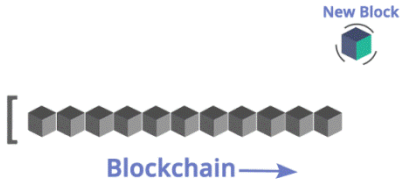

Fig.3 Block Creation

HASH VALUE CREATION

A cryptographic hash is an algorithm that takes an input as shown in Fig.4 and turns it into an output of a fixed size. It looks like a mix up of numbers and letters. There are many types of cryptographic hashes. Bit coin, for example, uses a hashing algorithm called SHA-256. A hashing algorithm is a computational function that condenses input data into a fixed size, the result of which is the output called a hash or a hash value. Hashes are used to identify, compare or run calculations

ISSN: 2233-7857 IJFGCN

against files and strings of data. Typically, the program first computes a hash and then compares the values to the original files.

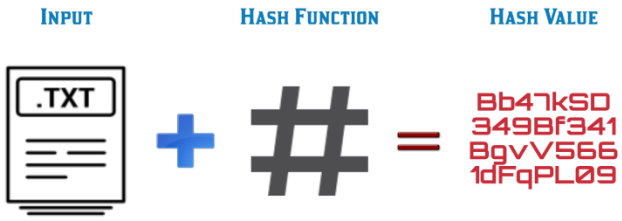

Fig.4 Hash Value Creation

PRIVACY PRESERVING

The solution for data privacy and security could and should very well be blockchain technology. The blocks relate to each other in the form of a chain. The first block of the chain is known as Genesis. Each block consists of a Block Header, Transaction Counter and Transaction. Also the patient data privacy is preserved using patient public address. The patient can share the public address rather than patient details to other members like doctors, hospitals etc.

As blockchain technology expanded and developed in recent years, manyhave pressed to shift health record storage onto the blockchain. Rather than having both physical and electronic copies of records, blockchains could allow the shift to Electronic Health Records (EHR). Medical records on the blockchain would be in the control of the patient rather than a third party, through the patients' private and public keys. Patients could then control access to their health records, making transferring information less cumbersome. Because blockchain ledgers are immutable, health information could not be deleted or tampered with. Blockchain transactions would be accompanied by a timestamp, allowing those with access to have updated information.

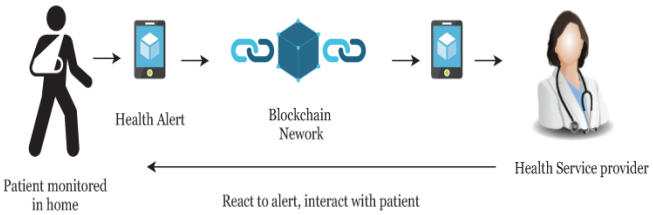

Fig.5 Privacy Preserving

CRYPTOCURRENCY

A cryptocurrency is a digital asset that can be used as a medium of exchange. The blockchain technology provides cryptocurrencies with the required level of security needed to withstand attacks on the state of the system and from preventing double spending. When a user sends cryptocurrency as shown in Fig.6, there is no physical exchange of coins. Instead what happens is a signing off of ownership in the sender's address to the receiver's address.

In order to be able to access the coins being sent the receiver must hold the private key which unlocks the sender's public key. If the keys match, the transaction is recorded on the blockchain and simultaneously the balance is altered in the sender's and receiver's address. Through crytocurrency the patient can pay the bills, pharmacy bills, appointment fee, doctor fee etc. To use cryptocurrency, buy some from an online exchange and choose a digital wallet to keep it secure. You can save it, or use it to purchase goods and services by exchanging your secret codes.

ISSN: 2233-7857 IJFGCN

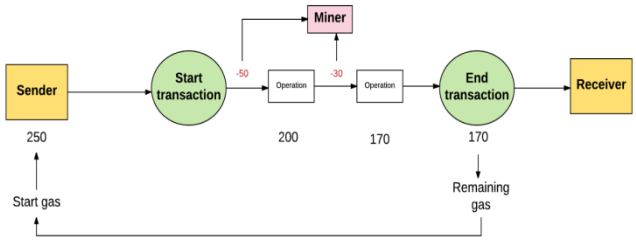

Fig.6Cryptocurrency Operation

MIDDLEWARE

This dependency is a personal blockchain, which is a local development blockchain that can be used to act as a public blockchain. Ganache is used to deploy smart contracts and for running tests. Here you have a personal blockchain network running. Ganache provides 10 accounts with 100Ether to test our smart contracts on local blockchain bases.

IV EXPERIMENTS AND RESULTS

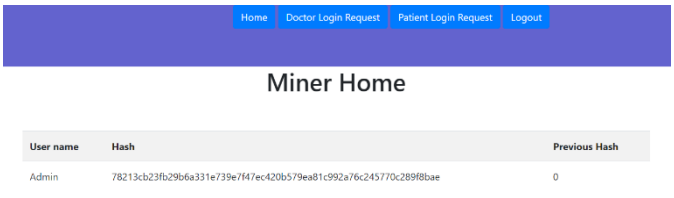

Fig.6 Admin home page

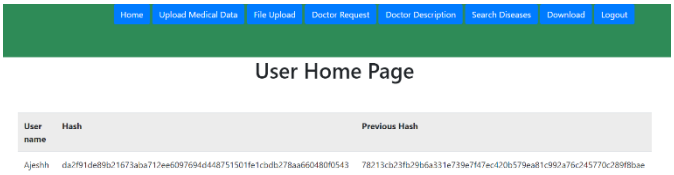

Fig.7 Patient home page

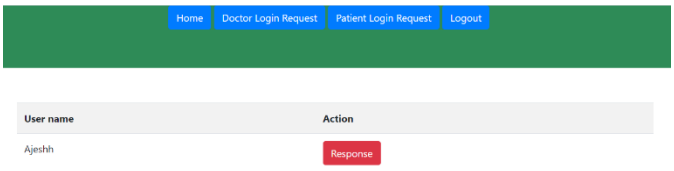

Fig.8 Granting permission for Patient

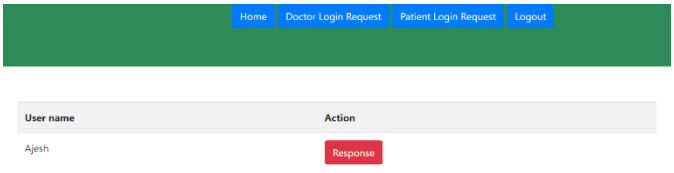

Fig.9 Granting permission for doctor

ISSN: 2233-7857 IJFGCN

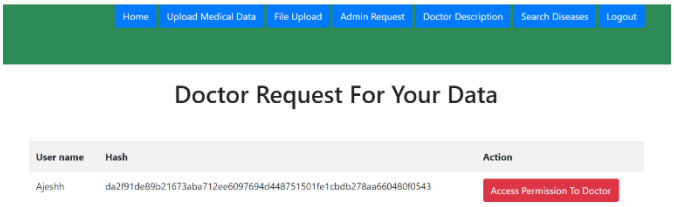

Fig.10Doctor requesting for patient data

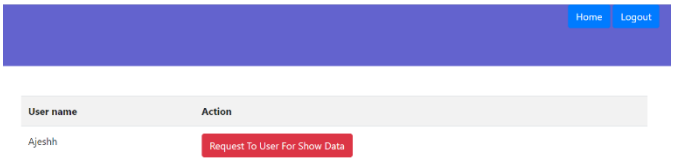

Fig.11 Patient giving permission to view the data

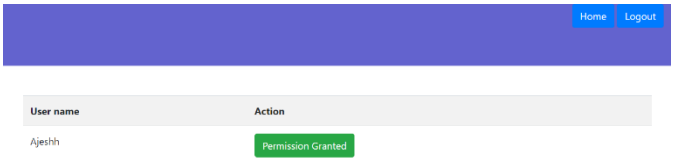

Fig.12 After patient gave permission

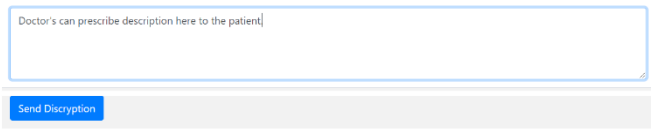

Fig.13 Doctor Prescription

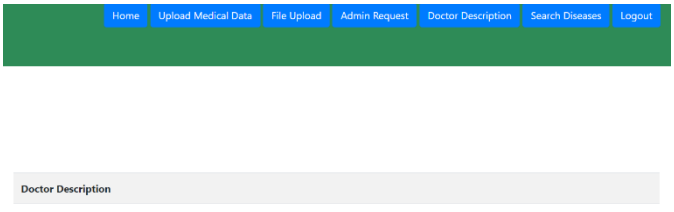

Fig.14 Doctor Prescription view from patient page

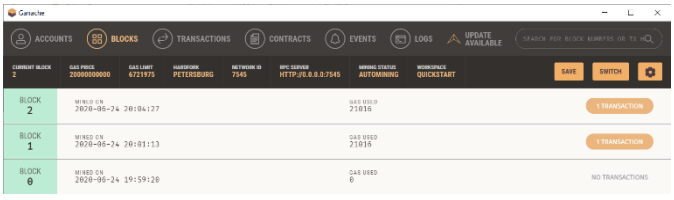

Fig.15 Ganache server

ISSN: 2233-7857 IJFGCN

V . CONCLUSION

Concluded that, the decentralized framework designed and developed for secure the patient health information. This decentralized framework based on block technology concluded the effectiveness in manipulation of patient's information and also the security in Electronic Health Records involved in the Medical industries using Block chain technology. . This paper proposed and concluded the efficiency in providing a high security and portability of the data manipulation about the patient health information. This paper concluded the security of patient's information from the intruder or the hackers in terms of hash value, cryptography with middleware based on block technology.

VI. FUTURE ENHANCEMENT

The future enhancement of this paper used to develop and deploy a block chain technology with data science. It can also remodified or redesigned using deep learning algorithm in order to provide an effective and efficient results.

REFERENCES

[1] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras and H. Janicke, "Blockchain Technologies for the Internet of Things: Research Issues and Challenges," in IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2188-2204, April 2019.

[2] B.L.Radhakrishnan, A. S. Joseph and S. Sudhakar, " Securing Blockchain based Electronic Health Record using Multilevel Authentication," 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), Coimbatore, India, 2019, pp. 699-703.

[3] Q. E. Abbas and J. Sung-Bong, "A Survey of Blockchain and Its Applications," 2019 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), Okinawa, Japan, 2019.

[4] Gordon W and Catalini, "Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability," Comput Struct Biotechnol J., pp. 224-230, 2018.

[5] F. M. Enescu, N. Bizon, A. Cirstea and C. Stirbu, "Blockchain Technology Applied in Health The Study of Blockchain Application in the Health System (I)," 2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Iasi, Romania, 2018, pp. 1-4.

[6] S. Vyas, M. Gupta and R. Yadav, "Converging Blockchain and Machine Learning for Healthcare," 2019 Amity International Conference on Artificial Intelligence (AICAI), Dubai, United Arab Emirates, 2019.

[7] Shan Jiang, Jiannong Cao, Hanqing Wu, Yanni Yang, Mingyu Ma, Jianfei He, "BlocHIE: A BLOCkchain-Based Platform for Healthcare Information Exchange," in Proc. IEEE on Smart Compu. (SMARTCOMP), 2018.

[8] S. M. Riazul Islam, Daehan Kwak, MD. Humaun Kabir, Mahmud Hossain, and Kyung-Sup Kwak, "The Internet of Things for Health Care: A Comprehensive Survey," IEEE Access, vol. 3, pp. 678-708, 2015.

[9] Kuo TT, Kim HE, and Ohno-Machado L, "Blockchain distributed ledger technologies for biomedical and health care applications," Ame. Medi. Infor.Assoc. J., vol. 6, pp. 1211-1220,2017.

[10] Lo.ai A. Tawalbeh, Rashid Mehmood, Elhadj Benkhlifa, and Houbing Song,"MobileCloudComputingModelandBigDataAnalysisforHealthcare Applications," IEEE Access, vol. 4, pp. 6171-6180, 2016.

[11] Bahga A, and Madisetti VK "A Cloud-based Approach for Interoperable Electronic Health Records (EHRs)," IEEE J Biomed Health Inform., pp. 894-906, 2013.

ISSN: 2233-7857 IJFGCN