Decentralizing Electronic Medical Records on the Blockchain Using Smart Contracts

B.V. Baiju[1], S. Saranya[2], D. Sriram[3], M. Rifath Ahmed[4], Adnan Mohammed[5]

[1]Department of Information Technology, Hindustan Institute of Technology and Science, Chennai, India. E-mail: bvbaiju@hindustanuniv.ac.in

[2]Department of Information Technology, Hindustan Institute of Technology and Science, Chennai, India. E-mail: saranyas@hindustanuniv.ac.in

[3]Department of Information Technology, Hindustan Institute of Technology and Science, Chennai, India. E-mail: sriramd5559@gmail.com

[4]Department of Information Technology, Hindustan Institute of Technology and Science, Chennai, India. E-mail: rifathahmed0107@gmail.com

[5]Department of Information Technology, Hindustan Institute of Technology and Science, Chennai, India. E-mail: 1911adnan@gmail.com

Abstract

The blockchain technology is considered as the most secure and decentralized way to manage your payments with cryptocurrencies. Furthermore, with the advent of NFT's which are a way to make owning digital art a possibility we can see how blockchain has multiple purposes. Blockchain gained traction because of its attributes such as security, immutability, expandability and decentralism. We can see blockchain being used more and more for non-financial applications. On the topic of electronic medical records which need to be secure and be accessed globally, it is still being stored locally or on the cloud which is confined to an organization or a group of organizations. We can observe that healthcare is a field that can benefit massively from blockchain technology. It can make electronic medical records be securely accessed in case of emergencies using smart contracts making the system effectively be used hand in hand with conventional database systems. Smart contracts can be used to manage the accessibility of electronic medical data by third party organizations globally without the data being tampered, manipulated or misused. The system can be used with the current database as it is interoperable. With the successful implementation of this system, it will give access to patients, health care organizations and other third parties the ability to view and manage the electronic medical data.

Keywords: Blockchain, Decentralized, Smart Contracts, Medical Records.

DOI: 10.47750/pnr.2022.13.S03.050

INTRODUCTION

Within the world of healthcare in recent times, there are two major terms that need to addressed are the data ownership and data security. Due to lack of secure structure currently, there is very high chances of the data becoming misused these lending the data breaches with severe consequences. The Division of Wellbeing and Human Administrations and Office for Respectful Rights (OCR) received notices of numerous information of breaches that come about within the presentation of 11 million add up to records of healthcare. In the recent study which was conducted by the ponemon institute in support of IBM security breach that is taken by in USA in terms of healthcare sector has the highest per capita cost, even more concern is that patients are currently unable to have a full ownership to their medical data and the concept that is in personalized medicine and wearables, with this now both issues are to be resolved.

On a daily basis, our dependence on the digital documents has steadily increase which has its shortcomings. Patients do not tend to carry their medical reports with them all the times, the EMR data which is being issued by a hospital can be easily stored on a secure blockchain database to which the issues get chance to access them and edit and make changes accordingly managing and maintaining is only going to authorized by the issuers and the patients who will be using them in whole scale the organization can easily access to the EMR to know if the patient had any previous complication even before the medicals could take over. Medical data have significant incentives for their data to be lost in their hands like the names, address, identity, numbers, address and permanent account number details.

In this work, the design of the blockchain is built on the Ethereum blockchain. The system that's built utilizing truffle. EMRs availability is overseen utilizing smart contracts with the assistance of the consensus calculation. The contracts are utilized within the system to oversee the exchanges and the computations included within the administration of client information. As blockchain has been used for cryptocurrencies and NFTs which are very different resources compared to medical information we have to be essentially adjust the approaches to make it attainable.

Blockchain

The blockchain is a system of saving the data in a way that makes it troublesome to alter, deceive or hack the network. It is basically an advanced model of record exchanges that's duplicated and distributed all over the network and the change is recorded to each participant's ledger which are maintained by miners and other hosts. The database that's decentralized and overseen by different peoples is known as DLT. The Blockchain is a kind of DLT (Distributed Ledger Technology) in which transactions are recorded and a cryptographic signature is hashed.

It means in case one square in a chain is changed. It would show up promptly that was handed to be altered and degenerate. Blockchains such as Ethereum and Bitcoin are ceaselessly developing modern blocks that are being included to the chain, which essentially includes more security to the record for a deeper understanding, The key blockchain features are as follows:

Decentralized-Blockchain network excludes the high risks of sensitive data being kept centrally at a single point of attack.

Distributed-In a synchronized database, it is accessible across various geographic locations and regions.

Immutable record-All blockchain networks follow a particular protocol for validating each and every new block. the data is registered at any block it cannot be changed without altering all the remaining blocks which requires the consent of the entire network.

Consensus Algorithm

A consensus calculation is the strategy through which all the peers and the hubs of the Blockchain network come to an understanding approximately the past and the present state of the values it speaks to on the disseminated record. In this way, the agreement calculation accomplishes a solid unwavering quality on the blockchain arrange which encourage builds up a solid believe between the known and unknown peers on the dispersed computing environment. Basically, the work of consensus protocol is to create sure that each novel square that's added or altered to the Blockchain network is the first form that's concurred upon by all the hubs on the tremendous network. The Blockchain consensus convention particularly comprises of goals such as coming to an understanding, collaboration, co-operation, giving break even with rights to all the hubs on the complete organize and making beyond any doubt that every hub has interest within the agreement prepare. Thus, as the name suggests consensus algorithm vies for consent with regards to set agreements and policies on the entire network. To accommodate this in real time, consensus algorithms assume that some of the systems processes will be unavailable or the communications between the systems will be lost. As a result, the algorithm must be completely fault-tolerant. The algorithm typically as an example assumes that only a portion of nodes will respond from the entire part of nodes which is set at 51 % At minimum.

Ethereum

Ethereum was made to control developers with the capacity to construct and distribute smart contracts and other dispersed applications (dApps) which can be utilized without the dangers of fraud, obstructions from third parties or downtime caused by server-side crashes. Ethereum is known as the "world's programmable blockchain". When compared to bitcoin, Ethereum allows its programmable blockchain framework to serve as a marketplace for financial services, applications, games and more recently art in the form of NFTs. Ethereum network also has its own cryptocurrency known as Ether which again is backed by all the principles of blockchain and more. Ether is considered as one of the most valuable cryptocurrencies second only to bitcoin. Ethereum's main competitors in crypto and blockchain networks are Bitcoin, Ripple, IBM, Block stream, NEO etc. Ethereum also has an estimated market cap of $500 billion according to analysts which is only trumped by bitcoin at an estimated $1 trillion dollars.

There are a number of projects which are already using the Ethereum network and multiple others which are experimenting with a variety of concepts. Mainstream companies such as Microsoft are currently partnering with ConsenSys to offer Ethereum Blockchain as a service or EBaaS on its Azure cloud. It is considered to offer Enterprise level clients and developers a blockchain developer environment on a single click. With strong fundamental principles Ethereum is a database that is designed to be immutable and un hackable which is ideal in providing data security and data integrity.

RELATED WORKS

Encrypting medical image is also one of the crucial things that has to be secured as Yi Ding, [1] has proposed a clever way to use DeepKeyGen a cipher generator based on deep learning to decrypt and encrypt images like CT scam, X-Ray etc.

Privacy and leakage during transmission are addressed by using analytics and Time series data to monitor the receiving and sending of data [2] – [4]

In the industrial IoT sector which plays an important role in managing supply chain and manufacturing. A innovative method of implementing credit-based consensus blockchain with changes in PoW mechanism of the consensus algorithm can be seen [5] This credit-based approach in PoW makes a fundamental change contract based dApps built on blockchain-based systems and frameworks.

The contract-based systems and architecture of the blockchain based system are innovated. Blockchain-based development platforms such as Ethereum and Hyperledger are taken into consideration for better security [9] and it also shows the benefit of contacts on a digital format where it holds its value very well.

CONCEPTUAL FRAMEWORK

The complex system of the blockchain network is explained with the diagram.

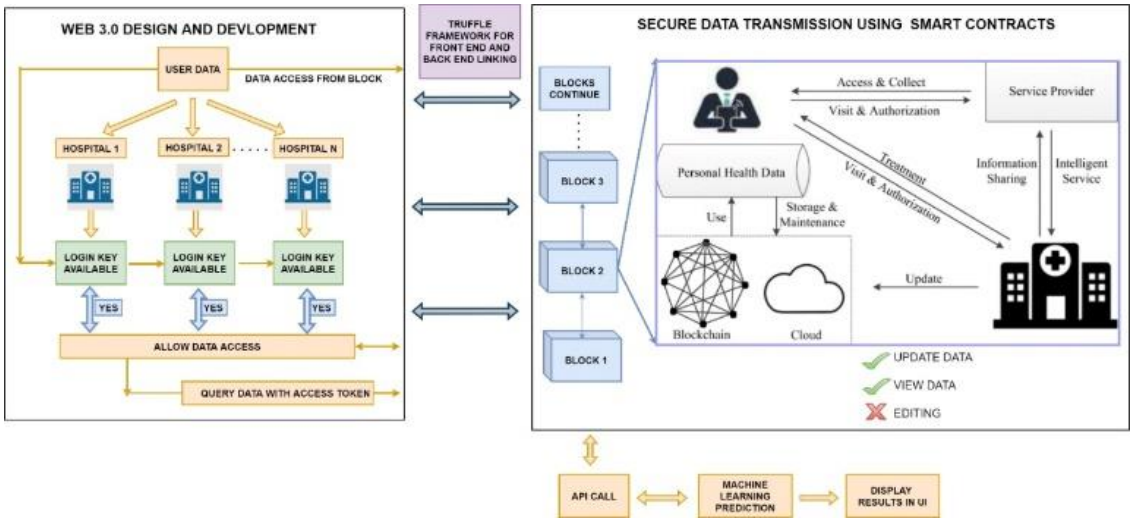

Figure 3.1.1: Conceptual Framework

METHODOLOGY

To store the medical data on the blockchain, smart contracts are created which specific needs and allows the user to enter the data and stores it in the blockchain. They store the data using the address of the dApp wallet and it is required to access them and edit the details of the patient. Secondly, after the data is entered it is tunneled via the API to an already up and running logistic regression model which analyzes the data sent via the API to determine the health condition of the patient and sends the data back after the model is computed. The data that is returned is shown on the portal. The ability to analyze multiple data at a same time is a feature that can be integrated in the future to help simultaneously analyze multiple data end point with the problem of bottleneck at any end of the application.

Smart Contracts

Smart contracts are set of code that administer the blockchain transactions and characterize the conditions of mutually concurred contracts. As of late numerous blockchain based ventures have actualized smart contracts such as the Hyperledger and Ethereum stage. They permit exchanges and trusted agreements to be rendered among unmistakable, mysterious substances with no require for central authority or external authorization component. The Ethereum stage permits the advancement of smart contracts that suit the necessities of the required framework. Within the see of receiving smart contracts in EMRs frameworks, they permit the creation of versatile and energetic conditions, rules and terms to safely share and trade restorative records.

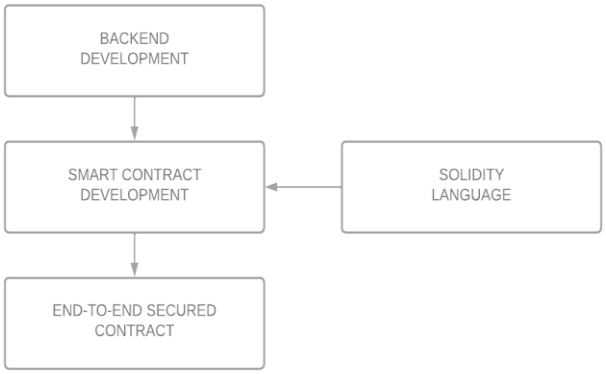

Figure 4.1.1: Smart Contract Development

Functionality Testing

Remix IDE is used to test functions of the project. Functionality testing is used by Quality Assurance engineers to check the compliance of all the functions. They are used to check all the predetermined requirements of the software. It uses the technique of black-box testing, in which the tester is not aware of the internal system logic and only tests the outward functionalities. It is important to check the functionalities of the created blockchain app.

Functionality testing in Blockchain also takes the size of the blocks in the blockchain. The changing of the size of blocks and its behaviour needs to be evaluated to make sure the maximum limit of the block is not exceeded even when many transactions are assigned to a single block. On the other hand, it is important to make sure whether the chain provides a permanent immutable record or not.

Adding a block: To make sure that the whole system works the chain of the blocks must be immutable and vastly expandable, therefore it is mandatory for testers to validate the

immutable behaviour of the blockchain application by adding multiple blocks and ensuring that the system responds and acts as intended.

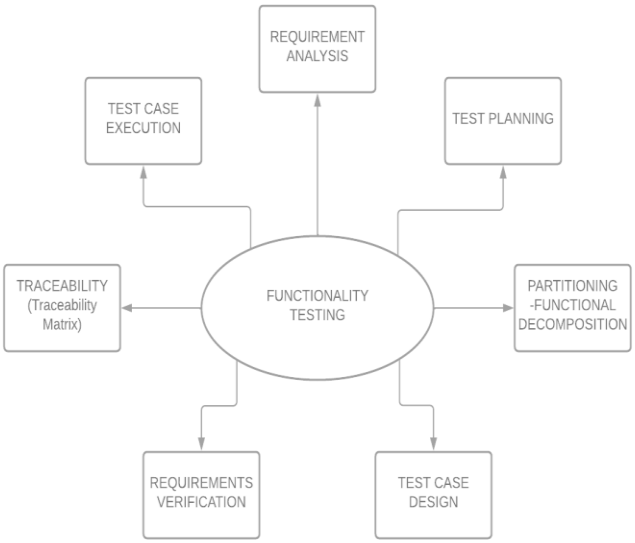

Figure 4.2.1: Functionality Testing

Truffle Framework Integration

It is an integrated development environment used for testing frameworks, asset pipelines and additional functionalities for blockchains that runs on the Ethereum Virtual Machine (EVM). The framework is aimed at making the life of a developer easier by avoiding the initial complexities. It is used widely by over 1.7 million Blockchain developers and is constantly upgraded and maintained. Coupled with Drizzle, a front-end development kit which is a suite of tools that provides an end-to-end dApp development platform. This can be used to deploy the smart contracts easily and communicate without the need of a heavy client-side programming.

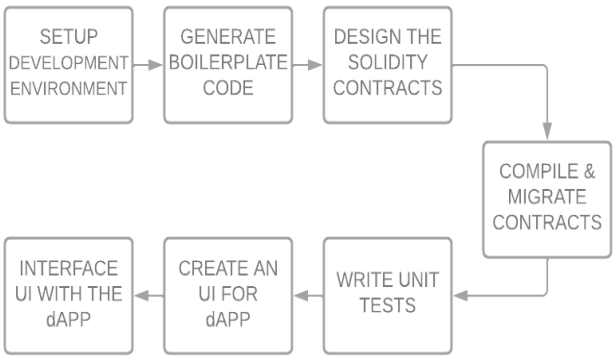

Figure 4.3.1: Truffle Framework Integration

Web 3.0 Frontend Development

Web 3.0 architecture and applications are very different when compared to web 2.0architecture. While web 2.0 applications are dependent on a medium to work, Web 3.0 works completely different by keeping no middle men and is Peer-to-Peer. There is no centralized location where the application state can be store like a database, and no single location where the application logic stays.

In Web 3.0, we can utilize the benefit of smart contracts which can be deployed on to a decentralized machine that can hold and define the backend logic of an application. Blockchain propels a new age of innovation that defines storage of information and databases to a new level. Furthermore, the distributed ledgers architecture of the blockchain network sets the stage global and encourages collaboration on any information to a level that has never been seen before. With Web 3.0 decentralized creation and Semantic web collaboration is massively accelerated due to its abilities like the ability to gather large amount of structured or unstructured data for the most part and process them easily with the use of techniques like natural language processing (NLP), language/text analytics and some sectors of data mining. And to collaborate on a global scale to use this distributed method of storing to perform machine to machine operations with the of AI and ML globally without any human intervention.

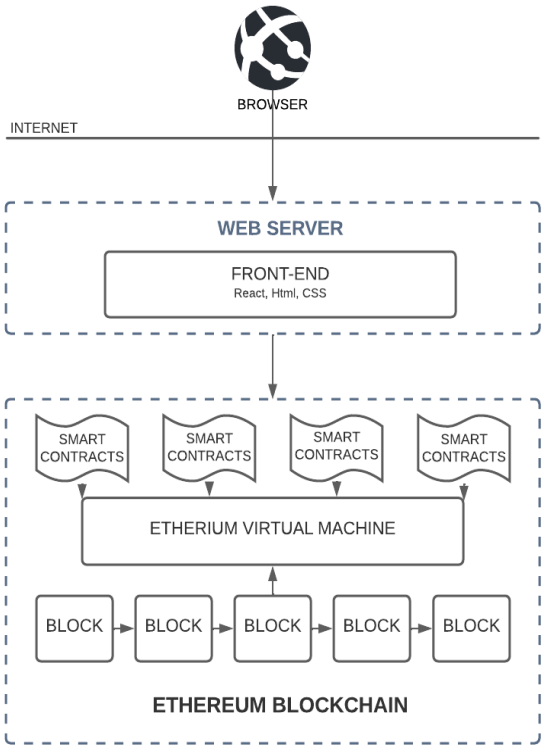

Figure 4.4.1: Web3.0 Front-End Development

Metamask Integration

MetaMask is a wallet for dApps which can activated as a browser extension which can be used by users on Ethereum-enabled web service or application. Metamask is a token wallet that securely manages the transactions and identities of both the sender and the receiver on an Ethereum-enabled blockchain environment. It manages the Ether's on the wallet

and maintains the hash codes safely.

Metamask allows its users to manage keys on their accounts in a diverse way such as including a personal hardware wallet, and isolates them from the site context. The aforementioned feature is great security improvement over conventionally storing the keys on a solo server or storage device which can be vulnerable and easily be wiped in mass account thefts. Developers can use the global API for Ethereum that identifies users that use web 3 based apps.

Test Network

The test network is a method provided by the Ethereum network to test non-production and non-revenue applications. In this project, it will be collecting output from the overall development. Then, it will be deployed in local platform and it will be integrated with the blockchain network. The network checks the feasibility of smart contract. No encryption or decryption key is required for accessing data which eliminates the fear of data being hacked or tampered by the hacker. Thus, this system successfully provides an end-to-end data security to the medical records of a hospital.

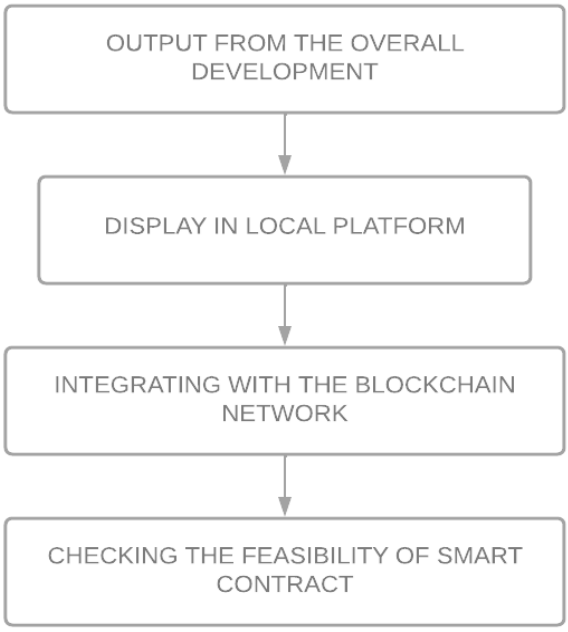

Figure 4.6.1: Test Network

Logistic Regression Algorithm

Logistic regression is one of the popular ML Algorithms and comes under supervised learning method, here in our project we use logistic regression to predict the health abnormality of a patient using the medical data entered as the dataset.

The data once entered to be stored in blockchain goes through an API to be processed by the ML model and output is displayed on the portal.

Step 1: Import the libraries

Step 2.: Import the dataset

Step 3: Initialize Logistic Regression Algorithm

Step 4: Train the model

Step 5: Check accuracy of the predicted model

Step 6: Send the predicted value to be displayed using the API pipeline.

Results & Analysis

Smart contract for accepting the data from the user and storing it in the blockchain. This contract allows acts as a protection for a user to allow only the contacts that are prioritized by the user to be able access the medical data.

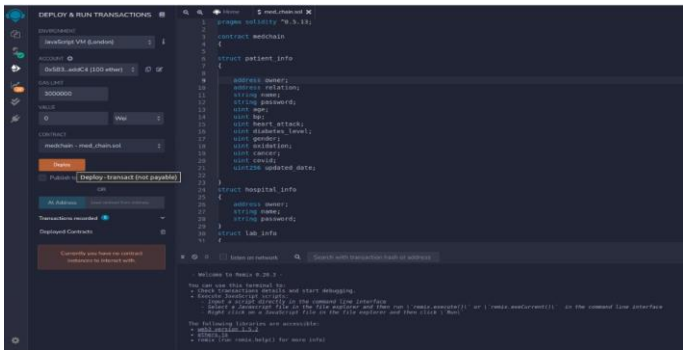

Figure 5.1.1: Smart contract

Authentication into the portal using Metamask. The account ID is verified and the data is validated. After verification is successful the user the taken into the portal where he can enter the data. The same applies for hospitals and laboratories who can access the data of a patient by using his ID.

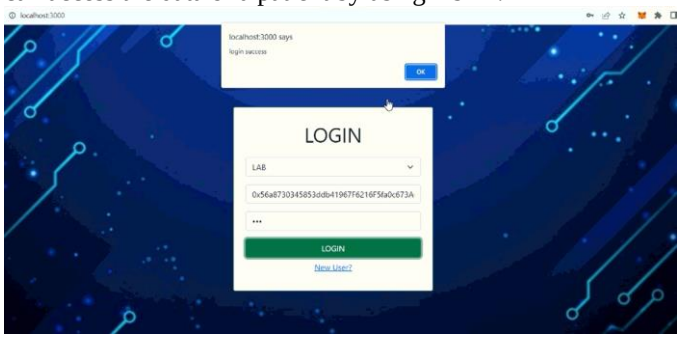

Figure 5.1.2: Authentication using Metamask

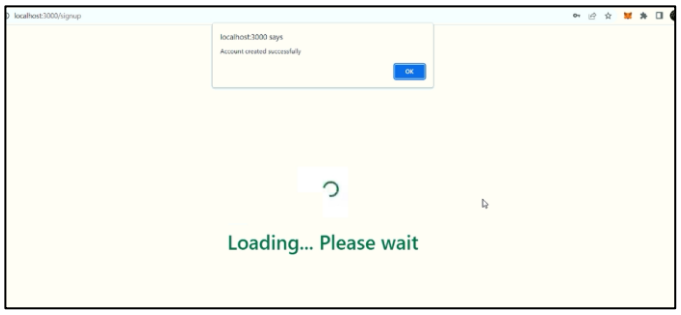

Figure 5.1.3: Successful account creation

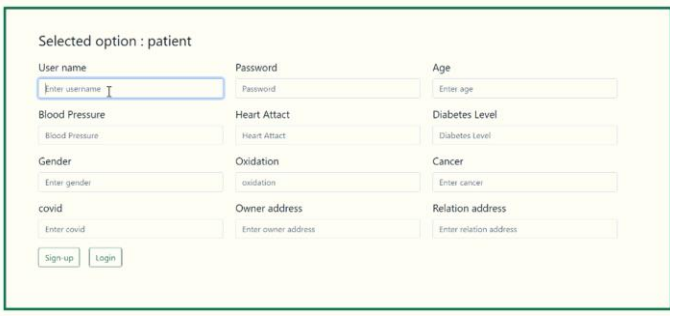

Figure 5.1.4: Entering the data to be stored in blocks

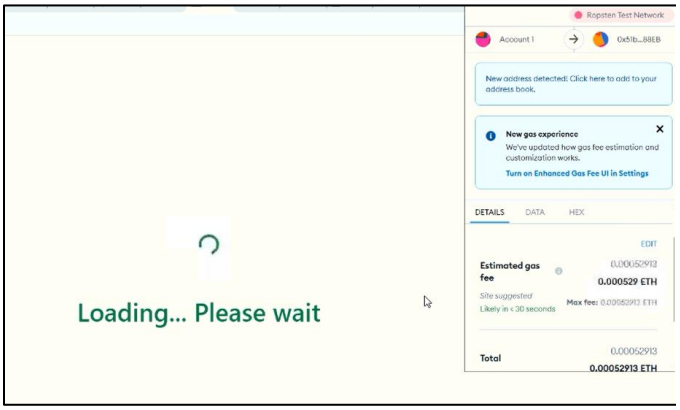

Figure 5.1.5: Metamask verification of the transaction

CONCLUSION

With more and more usage of blockchain in various government and private entities the architecture of the blockchain can be used to predict real-time medical from wearables and other IoT devices that are connected to the internet. Medical data can be stored easily and maintained easily without the fear of losing it or being hacked. The system can be further used to predict the abnormalities of a patient in real time which can be used by people to monitor the elderly wherever in the world.

REFERENCES

Yi Ding; Fuyuan Tan; Zhen Qin; Mingsheng Cao; Kim-Kwang Raymond Choo; Zhiguang Qin, "Deep Key Gen: A Deep Learning-Based Stream Cipher Generator for Medical Image Encryption and Decryption", IEEE Transactions on Neural Networks and Learning Systems.

Xiaoning Liu; Yifeng Zheng; Xun Yi; Surya Nepal, "Privacy-Preserving Collaborative Analytics on Medical Time Series Data", IEEE Transactions on Dependable and Secure Computing.

Yang Yang; Robert Deng; Ximeng Liu; Yongdong Wu; Jian Weng; Xianghan Zheng; Chunming Rong, "Privacy-preserving Medical Treatment System through Nondeterministic Finite Automata", IEEE Transactions on Cloud Computing.

Haiping Huang; Tianhe Gong; Ning Ye; Ruchuan Wang; Yi Dou, "Private and Secured Medical Data Transmission and Analysis for Wireless Sensing Healthcare System", IEEE Transactions on Industrial Informatics [Vol no: 13, 2017]

Junqin Huang; Linghe Kong; Guihai Chen; Min-You Wu; Xue Liu; Peng Zeng, "Towards Secure Industrial IoT: Blockchain System With Credit-Based Consensus Mechanism", IEEE Transactions on Industrial Informatics [Vol no: 15, 2019]

Kai Fan; Wei Jiang; Hui Li; Yintang Yang, "Lightweight RFID Protocol for Medical Privacy Protection in IoT", IEEE Transactions on Industrial Informatics [Vol no: 14, 2018]

Massoud Masoumi, "Novel Hybrid CMOS/Memristor Implementation of the AES Algorithm Robust Against Differential Power Analysis Attack", IEEE Transactions on Circuits and Systems II: Express Briefs [Vol no: 67, 2020]

Mauro Mangia; Alex Marchioni; Fabio Pareschi; Riccardo Rovatti; Gianluca Setti, "Chained Compressed Sensing: A Blockchain-Inspired Approach for Low-Cost Security in IoT Sensing", IEEE Internet of Things Journal [Vol no: 6, 2019]

Shuai Wang; Liwei Ouyang; Yong Yuan; Xiaochun Ni; Xuan Han; Fei-Yue Wang, "Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends", IEEE Transactions on Systems, Man, and Cybernetics: Systems [Vol no: 49, 2019]

Wenhui Yang; Xiaohai Dai; Jiang Xiao; Hai Jin, "LDV: A Lightweight DAG-Based Blockchain for Vehicular Social Networks", IEEE Transactions on Vehicular Technology [Vol no: 69, 2020]

Caixue Zhou, "Comments on "Light-Weight and Robust Security-Aware D2D-Assist Data Transmission Protocol for Mobile-Health Systems"", IEEE Transactions on Information Forensics and Security [Vol no: 13, 2018]

Dariush Abbasinejad-Mood; Morteza Nikooghadam, "Efficient Design of a Novel ECC-Based Public Key Scheme for Medical Data Protection by Utilization of Nano Pi Fire", IEEE Transactions on Reliability [Vol no: 67, 2018]

Yasmin Mustapha Kamil; Muhammad Hafiz Abu Bakar; Mohd Hanif Yaacob; Amir Syahir; Hong Ngee Lim, "Dengue E Protein Detection Using a Graphene Oxide Integrated Tapered Optical Fiber Sensor", IEEE Journal of Selected Topics in Quantum Electronics [Vol no: 25, 2019]

Caio Davi; André Pastor; Thiego Oliveira; Fernando B. de Lima Neto; Ulisses Braga- Neto; Abigail W. Bigham, "Severe Dengue Prognosis Using Human Genome Data and Machine Learning", IEEE Transactions on Biomedical Engineering [Vol no: 66, 2019]

Ibrahim, S., & Koksal, M. E. (2021). Realization of a fourth-order linear time-varying differential system with nonzero initial conditions by cascaded two second-order commutative pairs. Circuits, Systems, and Signal Processing, 40(6), 3107-3123.