An Efficient Personal Health Record Storage using Block Chain Technology

Dr. E. Kodhai¹, Manga Haneesha Gowri², Susmitha. S³, Muthamizh. R⁴
Department of Computer Science and Engineering
Sri Manakula Vinayagar Engineering College, Puducherry, India

Abstract:
Block chain is a technology in which data are stored in blocks and linked using cryptographic principles (i.e. chain) in chronological order. In fast moving world health issues and managing health records have become a tedious process. In order to secure our personal health records from being accessed by unauthorized people for easy access globally. The existing system uses access control scheme for PHRs which can be provided by multiple patients. The scheme combines the encryption of data from different patients where the data are under the same access policy. In this paper, proposes a novel based encryption scheme for efficient PHR storage in Ethereum Block chain Technology. PBE based MD5 with Triple DES Algorithm is used for the file data security. The MD5, message digest-5 algorithm is enhanced with password-based encryption and triple DES for further data security in each level of PHRs transactions.

Keywords: Personal Health Records, Block chain, Security, Ethereum block chain, PBE, MD5.

I. INTRODUCTION

In the recent years, with the development of new technologies and software are applied on all the fields of the services and the products. Healthcare services are also playing a major role in using the services provided by the information technology. Health department are using software and technologies for their storage of database. In hospitals, they store the patient details, address, disease and the reports of the medical test. By using cryptographic techniques, the health records of the patients are protected [1]. Personal Health Records (PHRs) as such is an electronic version of patient’s health information. In an electronic medical system, patients can share their PHRs with medical staff for monitoring and diagnosis with the help of security keys. The requirements for storage and continuous availability of PHRs necessitate the use of the Block chain services. Block chain in healthcare global is a trade organization whose aim is to reduce deeply entrenched governance and regulatory barriers that are stifling block chain innovations [2]. Medical chain uses block chain technology to securely manage health records for a collaborative, smart approach to healthcare. Block chain is an effective technology that can help prevent data breaches in the healthcare industry. It is a secure and reliable method of recording, storing, and sharing sensitive data. Block chain is a shared record of transactions [20]. It enables participants in a group to securely share data with each other without a middleman and keep track of what was exchanged and when. “The challenges that block chain addresses in healthcare are very disruptive” [18]. It could solve the problem of interoperability by allowing doctors to gather information about the patient from personal health records. By this model third party cannot involve in the reports of the patients and there will be a safety for the patient. Here we are implementing the cipher-text policy ID-based encryption by using Ethereum Block chain technology. By this patient reports are secured and there will be no chance of third party access [3]. In this Ethereum block chain technology to a cipher text-policy id-based encryption algorithm and use Ethereum smart contract technology to store the publicly available information into the block chain network, at the same time to achieve the role of supervision and track the behaviour of the data access as shown in the fig 1. All access records are recorded in the block chain network [4]. In our framework, decentralization of access control scheme is achieved without any trusted centre authority by using block chain technology. PHRs permit patients to keep up data on their ailments, medications, and practices identified with self-care and self-observing of their wellbeing. In any case, get to constrained by the patients speaks to an ever-present concern since it requires a free however safe harmony between framework customizations, protection, and security controls [4]. Some variation names for PHR showed up in the writing, for example, e- PHR (electronic PHR) or UHR (widespread wellbeing record). The primary idea alludes to the utilization of PHR in an electronic configuration, while the second proposes PHR-imparting information to medicinal services suppliers. Another term is insightful PHR (iPHR), which utilizes medicinal information to envision the wellbeing needs of patients and elevate instruments to direct scans for sicknesses and proposals for nursing exercises or restorative items [5]. In spite of the fact that these various classifications are utilized, we utilize the term PHR all through this work. The PHR fills in as a stage for patients’ and human services suppliers’ utilization, empowering the trading of data with social insurance frameworks. PHR has likewise developed as a component for patients to make meetings with their social insurance suppliers [6]. The point is to address patients’ advancing needs by utilizing explicit techniques to improve their mind and predict medical problems. The advances used to process wellbeing related information incorporate AI, design acknowledgment, applied science, measurements, master frameworks, information sharing, and man-made brainpower calculations. Additionally, propels in data and correspondence innovation (ICT) have permitted both the capacity and simple access of a lot of information, permitting the arrival of physical space, encouraging examination and the relationship of information inside clinics. In any case, the expanding number of patients who need care, particularly with the expanded future of individuals in a few nations, has been a

IJESC, May 2020  26065  http://ijesc.org/
deterrent to overseeing gigantic databases of medicinal records [7]. Security threat is one of the major issues in today’s technological world. When data are stored in cloud there is an intermediate third-party who gives keys and access privileges [16]. When the intermediate third-party is not trust worthy our data privacy is under threat. Thus, block chain helps us to avoid such circumstances. Personal Health Records of people are more delicate data that are needed to be very much secured from unauthorized access. Hence by using Ethereum block chain technology and ID-based encryption algorithm the data is made secure [11].

II. RELATED WORK

Wei Li et al [1] used a novel quality-based encryption plot for fine-grained and flexible access control to PHRs information in distributed computing. The plan creates shared data by the basic access sub strategy which depends on various patients’ entrance strategies. At that point the plan consolidates the encryption of PHRs from various patients. In this way, both time utilization of encryption and decryption can be diminished. Through execution and recreation, they exhibit that the proposed plan is efficient as far as time.

Distributed computing is developing as another processing worldview in the social insurance division other than different business areas [19]. Huge quantities of wellbeing associations have begun moving the electronic wellbeing data to the cloud condition. Presenting the cloud benefits in the wellbeing part not just encourages the trading of electronic clinical records among the emergency clinics and facilities, yet in addition empowers the cloud to go about as a clinical record stockpiling focus. In addition, moving to the cloud condition calms the medicinal services associations of the repetitive undertakings of foundation the board and furthermore limits improvement and support costs. In any case, putting away the patient wellbeing information in the outsider servers likewise involves genuine dangers to information protection [18]. In light of plausible divulgence of clinical records put away and traded in the cloud, the patients’ protection concerns ought to basically be viewed as when structuring the security and protection components. Different methodologies have been utilized to protect the security of the wellbeing data in the cloud condition. This study plans to envelop the cutting-edge utilized to protect the security of the wellbeing data in the protection components. Different methodologies have been basically be viewed as when structuring the security and traded in the cloud, the patients’ protection concerns ought to light of plausible divulgence of clinical records put away and involves genuine dangers to information protection [18].

Shangping Wang et al [3] distributed storage structure is decentralized, that is, there is no confided in outsider in the framework. Our plan has three primary highlights. Initially, as the Ethereum block chain innovation is utilized, information proprietor can store cipher text of information through brilliant agreements in a block chain arrange. Besides, information proprietor can set legitimate access periods for information client so that the cipher text must be unscrambled during substantial access periods. At long last, as the creation and summon of each savvy agreement can be put away in the block chain.

Baodong Qin and Dong Zheng [11] has used a model that uses ABE scheme that can achieve decryption outsourcing. To produce the actual result, it needs two types of keys to decrypt the entire information needed for this purpose. On updating of the user’s key pair, the adaptive security model also holds a generic construction. Setup Phase 1 of working process which involves encrypting the data, working on the challenges, Phase 2 of working process which involves decryption of cipher text.

Hongyang Yan et al [10] use cloud system managing PHR records. It contains 5 participants who involve in this process starting from health care provider to the PHR user [9]. They use Advanced Encryption Standard key to encrypt the message and thus leading to high end security policy. It uses KP-ABE scheme for access control policy [9]. This system ensures privacy protection for patients.

III. PROPOSED SYSTEM

In the proposed model we shift the data stored in cloud to “Block chain”. Block chain technology allows us for verification without any intervention of the third party. The Personal Health Records of the patients are divided into blocks and is stored [10].

Patient details are to be collected and uploaded in the server by using block chain technology and documents are stored. In fig 2 Attribute Authority provides the keys to the doctor whenever doctor needs the data or information of the patient. After getting the key the doctor can see the document or can download it for his patient treatment purpose PBE based MD5 with Triple DES Algorithm is utilized for the document information security. The MD5, message digest-5 calculation is improved with secret word-based encryption and triple DES for additional information security in each degree of PHRs transactions followed by the fig 2 architecture.
The documents of the patients are 1st loaded and then encrypted using certain encryption algorithms in blockchain. Since the records of the patients are really very sensitive data they are to be properly encrypted and handled with high security. These data in the encrypted form are then stored in the cloud. Using the correct keys (i.e.) the match pair of the key used for encryption is used to decrypt the file. The attribute authority is the person who encrypts the data through blockchain and stores it in the cloud. The file uploaded by the attribute authority is encrypted in the form of blocks and the encrypted form is stored in the cloud so that it is more secured and cannot be easily accessed by unauthorized members. The records of the patients are collected and are given to the attribute Authority and they are encrypted and stored in the cloud. There are certain people who have the key that is used for decrypting the data that is stored in the cloud. Only the doctors have the accessibility to view the records of the patient. Thus it is kept securely in the encrypted form in the authority module. The encrypted form of data is then stored in the cloud server for easy accessibility.

The proposed system is divided into 4 major modules so that the work can be easily done. They are:

1. Patient Module
2. Authority Module
3. Cloud Module
4. Doctor Module

3.1. Patient Module

The first and foremost module in the proposal system is the patient module system. Here the documents of the patients are collected (i.e.) the medicines they use, the history of their treatment, and the type of disease they are affected by. These details are collected and maintained as Personal Health Records. These PHR’s are encrypted using blockchain and is then stored in the cloud for security purpose. The patient module registers and login into the system. While registering it accesses more details because the data is to be stored and hidden in the database server. After encrypts data which are stored. Later they will encrypt the data and upload into the using blockchain technology. Doctor Management System allows registering the doctors, working in a hospital as well as their clinic details. It helps in the duty management of doctors and updates them to complete appointment details with a patient health history. Hospital management system is developed by the solution dots system which provides the complete assistance in Patient Management. In the patient module management system, there are facilities to register patients and view their reports and history. Patient management system allows getting detail information of Patient’s health condition. Firstly, patient creates the account by giving the details of the patient which and all needed to create an account. By sign into the account of the patient, they encrypt the data. After that they upload encrypted data into the using blockchain technology. Compulsory fields for urgent patient data according to JCI Standards. It Produces Smart Card with Unique Health Identification Number (UHID). Progressed multi-criteria scan for enlisted patients. Arrangement for recording backer, insurance and clinical the travel industry subtleties.

3.2. Authority Module

Being the second module the Authority module enables us to encrypt and decrypt the file. The Personal health records of the patients are collected in the Patient Module. These records are then processed and stored in the cloud in encrypted form using blockchain. The Authority module will provide the key when the system verifies the patient account properly. It uses symmetric keys to secure the records. And it encrypts the data in the form of documents in a database server application. Authentication provides keys whenever medical staff or doctor needs the document from the database. Authority’s module is able to manage their available resources, analyze staff work, reduce the equipment downtime, optimize the supply chain, etc. Another fact to mention is that hospital staff deal with the digital data instead of endless paperwork.

1. After registering system verifies and provides authentication.
2. Authority holds the keys; data can be handled safely by using keys.
3. Keys establish the major role of hiding the data from the intruders.
4. Authority handles the symmetric keys, which encrypts and decrypts the data.
5. Details are to be stored in the form of documents on a server application.
6. If the doctor or medical staffs needs the keys then authority distributes the keys.
7. It can used to decrypt the data by the doctor or medical staff.

3.3. Cloud Module

Cloud Module it is also known as the storage module since it is used to store the data. The encrypted form of the Personal Health Records of the patients which are encrypted using blockchain technology are stored in cloud storage. Storing the data in the cloud enables the user to access the data from anywhere and everywhere. The cloud storage server will store the documents into the cloud, where it can be accessed from anyplace and from anywhere. It can store documents or records in server without any modification and also it can update the list whenever patient updates the files or records of the treatment done by the doctor. Data should be stored in the
FUTURE SCOPE

Prepared access to a great deal of comprehensive, refreshed patient data, snappy, dependable and make sure about data. Streamlining of clinical information and useful assets that fare thee well, supporting multi-disciplinary group activities. Faster access to advisor specialist conclusions and ID. Diminished patient data the board, paper-work, duplication and different structures – less time spent finding unidentified notes, x-beams, confirmation or release data.

IV. CONCLUSION

The proposed system would be built with all the above-mentioned functionalities produces confidentiality to patient medical records victimization “Block chain Technology". Patient information secrecy or confidentiality is one amongst the foremost necessary pillars of drugs. Protecting the personal details of a patient isn't simply a matter of ethical respect, it's essential to bond trust between the doctor and also the patient.

V. REFERENCES

[1]. Wei Li, Bonnie M. Liu, Dongxi Liu, Ren Ping Liu, Senior Member, IEEE, Peishun Wang, Shoushan Luo, and Wei Ni, May 2019


[3].https://blockchain.intellectsoft.net/blog/how-the-consortium-blockchain-works/

[4].https://builtin.com/blockchain/blockchain-healthcare-applications-companies

[5]. Shangping Wang, Xu Wang, And Yaling Zhang, 2019, Doi 10.1109/Access.2019.2929205

[6].B. Narendra Kumar Rao, B. Bhaskar Kumar Rao, Vellingiri J, 8 June 2019

[7].https://www.healthit.gov/faq/are-there-different-types-personal-health-records-phrs


[9].Jo’ao Pedro Dias, Lu’ís Reis Hugo Sereno Angelo Martins, 31 May 2018

[10]. Hongyang Yan, Xuan Xian and Jiali Duż


