JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

PRIVACY PRESERVATION IN HEALTH APPLICATIONS

[1]Saniya Fathima, [2] Vijayakumar Adaickalam
[1] PG Student, School of Computer Science & Information Technology
[2] Professor, School of Computer Science & Information Technology
Jain Deemed to be University, Bangalore, India
Email: [1] saniyafathimaofficiall@gmail.com [2] vijay.pattukkottai@gmail.com

ABSTRACT: THE HEALTHCARE INDUSTRY ELECTRONICALLY MAINTAINS MEDICAL DATA WHICH HAS PATIENT'S INFORMATION LIKE PATIENT'S PERSONAL INFORMATION, DIAGNOSTIC REPORTS, AND DOCTOR PRESCRIPTIONS. CURRENTLY, SENSITIVE INFORMATION IS STORED IN THE CENTRALIZED STORAGE MODEL. ONE MAIN DISADVANTAGE OF THE CENTRALIZED MODEL IS THAT THE PROBLEM IN PRESERVING USER PRIVACY. THREATS PERTAINING TO THE USER (PATIENT) PRIVACY INCLUDE UNAUTHORIZED ACCESS OF CRITICAL INFORMATION LIKE IDENTITY DETAILS AND DISEASES FROM WHICH A PATIENT IS SUFFERING AND MISUSE OF PATIENTS' DATA AND THEIR MEDICAL REPORTS. TO HANDLE THIS ISSUE, WE PROPOSE A DISTRIBUTED OFF-CHAIN STORAGE OF MEDICAL DATA USING IPFS (INTERPLANETARY FILE SYSTEM) AND BLOCKCHAIN TECHNOLOGY. THE PROPOSED FRAMEWORK WHILE PRESERVING PATIENT PRIVACY FACILITATES EASY ACCESSIBILITY OF MEDICAL DATA BY AUTHORIZED ENTITIES LIKE HEALTHCARE PROVIDERS (E.G., DOCTORS AND LABORATORY PERSON). MOREOVER, IT ACHIEVES CONSISTENCY, INTEGRITY, AND AVAILABILITY.

KEY WORDS — BLOCKCHAIN, HEALTHCARE, IPFS, PRIVACY, CENTRALIZED

I. INTRODUCTION

The healthcare industry generates large volumes of medical data that need to be stored, disseminated, and accessed daily. For instance, medical data gets created when a patient undergoes medical tests such as computerized tomography, CT-SCAN, and X-Ray. Another source of these data is when a doctor issues a prescription. A patient's medical information must be stored in such a way that it is accessible by the physicians in other hospitals within the network when the need arises. However, this information must be kept private. Moreover, it should be immutable. The requirement of transparent process for storing medical records demands a structure where data can be easily maintained and accessed. The blockchain technology provides a decentralized storage scheme, wherein a patient's medical record (viz., diagnostic report, patient personal information, doctor's prescription and so on) can be shared easily among the peers (hospitals or doctors) in a healthcare system. This technology ensures various features such as privacy, immutability, integrity, and consistency which are important requirements in a modern healthcare system. A blockchain consists of a list of blocks of transactions which are linked with the help of cryptographic hash thereby ensuring the immutability of the transactions (medical records). The details of medical records of a patient including past and present ailments can be efficiently stored in the blockchain network and can be disseminated among the peers. The structure of the blockchain network makes every record transferable, permanent and easily accessible. However, in order to maintain these large volumes of medical records, there is a need of a distributed storage (off-chain) system with a peer-to-peer structure. Moreover, the system must provide persistent storage of records

2. LITERATURE REVIEW

Rajesh Gupta et.al., (1) proposed about A Blockchain-based Outdoor Delivery Scheme using UAV for Healthcare 4.0 Services and how Patient and caregiver are both included in this layer, along with bystanders. This layer allows patients, caregivers, or bystanders to request healthcare aids. This layer also gives the location where the required supplies get delivered by Unmanned aerial vehicle UAVs and must be in the proximity of EW. In this paper, a blockchain-based secure outdoor healthcare supply delivery scheme using UAVs called VAHAK is proposed. They have suggested deep insights into the traditional BC-based UAV system and highlight the latency, network bandwidth, and storage cost issues in detail. They presented how ESC with IPFS and 5G-TI ensures security, privacy, ultra-low latency, ultra-high reliability, and cost-effective data storage by eliminating third-party organizations. They deployed the SCs over Remix IDE to view the block information. Finally, the performance of VAHAK is compared by considering the latency, scalability, and network bandwidth with the traditional BC-based systems over the LTE-Advanced communication network. By eliminating the partial convoy effect with AI techniques, we will be able to improve priority queue performance in the future.

Sabyasachi Chakraborty et.al. (2) presented about how the crust of the framework is the amalgamation of Internet of Things (IoT), Blockchain and Machine Learning for detecting anomalies in the health data of the patient. The methodology demonstrated is basically a system that uses the Internet of Things module to intercept and retrieve data generated by the wearable devices worn by the patient. Ideally, the Blockchain-based system depicted would be used for the storage and maintenance of patient data in the form of multiple transactions, as well as providing access control to stakeholders. Furthermore, the Blockchain architecture is also used for supporting medical research by maintaining patient pseudo-anonymity, and authenticating and trusting data for a more accurate research process. The Machine Learning Using the models is mainly for the detection of anomalies and the forecasting of certain scenarios that may arise with time based on the parameters provided by the doctors for basic identification of the conditions faced by the patients. The IoT module deals with the process of fetching and sensing the data from the wearable devices and the biosensors that are either worn by the patients or that are present in the environment in which patients are monitored. The processing and storage of the vast amounts of information generated by the patient need to be managed and secured, in accordance with some security protocol. Further, when there are multiple stakeholders associated with the generated data, an access management system must be implemented, which is addressed by the Blockchain Network. In order to maintain accuracy, security, and authenticity of the data generated from the patients, the data must always be governed appropriately. Consequently, for the purpose of managing access and storing data to manage transactions, we recommend that the concept of blockchain be adopted, which is a consortium of multiple stakeholders, such as hospitals, doctors, pharmacists, pathologists, imaging centers, medical research institutes, and insurance companies. Therefore, such systems can be considered as a significant whole in uplifting the society with accurate and efficient healthcare.

Ilhaam A. et.al. (8) proposed a blockchain-based GPO contract solution that connects manufacturers, distributors, GPOs, and healthcare providers within the same decentralized Ethereum network. Our solution adopts blockchain technology to promote transparency, data provenance, and data immutability in the contracting process. These stakeholders interact with one another using the smart contracts. Our proposed solution uses five smart contracts: Registration smart contract, Price Negotiation smart contract, Purchase Order smart contract, Rebates Settlement smart contract, and Loyalty Rebates smart contract. Each one of those contracts is specialized in carrying out particular tasks. They discussed how the presence of GPOs in HCSCs helps various stakeholders in the HCSC, in particular the providers by achieving cost savings from quantity discounts and operational savings due to efficient procurement practices. GPOs also help provide managerial support and help in the vendor qualification process. On the other hand, they benefit manufacturers by reducing market costs and volume sales while monitoring hospital contract compliance. Nonetheless, the current GPO contract process is complex, time-consuming, and inefficient. Hence, their proposed solution integrates blockchain and decentralized storage technologies to promote collaboration, transparency, data integrity, and data provenance among stakeholders in the HCSC. More-over, help avoid pricing discrepancies between stakeholders and streamline communication. The system architecture, algorithms, sequence diagrams, and testing can be customized for several product types in HCSC. The proposed solution guarantees that only registered stakeholders are allowed to register and interact with the smart contract ensuring trust and transparency among stakeholders.

Mahmood A. Bezel et.al. (10) addressed in-depth discussions on the convergence of blockchain with systems of healthcare. They presented how blockchain can help healthcare companies manage big data in a decentralized, open, available, traceable, auditable, trustworthy, and stable way and ensures immutability and tamper-proof health data storage. They went through the features and benefits of the technology of blockchain to demonstrate how it can use to handle healthcare big data to its full potential. They spoke about the main opportunities of this technology in the applications of healthcare industry. They introduced several potential areas to demonstrate how this technology has aided and complemented different healthcare systems. The critical open research obstacles impeding the spread blockchain technology adoption in the healthcare industries were also described and addressed. The integrating of blockchain with systems of healthcare raises a number of technological issues that need to more attentions.

William Bodies, George P. Corser (9) presented on the implementation and integration of blockchain in healthcare is examined in this paper. The papers retrieved from the ACM Digital Library were categorized into three categories: adoption, implementation, and integration. Based on this brief literature review, they conclude blockchain adoption has been covered thoroughly. Their primary contribution is an up-to-date classification of current research papers in the field of blockchain technology in Healthcare. They also identify understudied research areas, potential areas for future research work. Additional research is needed in the areas of blockchain implementation and integration for healthcare systems. Based on our observations, we conclude that there must be a great deal more research into the area of blockchain before the healthcare industry achieves advanced levels of acceptance, implementation and integration.

Randhart Kumar et.al. (5) proposed scheme has not considered the case when the size of the data is too large to be supported by the blockchain ledger. In this work, they have sought to address these issues. They propose a distributed storage model, in which they store only the content-addressed hash of medical records instead of storing them in the blockchain network, thereby reducing the size of the network. i.e., medical records are stored using the IPFS distributed file storage system. They implement proof-of-work consensus for validation of transactions (records) and block creation in the blockchain network using local mining to ensure scalability. i.e., privacy of patient diagnostic reports is preserved using hash representation on blockchain storage. They present a blockchain-based distributed off-chain storage for patient diagnostic reports using IPFS. The underlying storage model is immutable and content addressable. The primary objective of this framework is to provide privacy of the patient reports. To achieve the privacy, they divided our framework in three different modules: data upload, mining process, and data storage. The healthcare provider uploads the details of each patient using a Web-UI (Web User Interface). Then, the mining process is performed to validate the transactions and to provide consistency in the network. Finally, hash-based data storage is used to provide privacy of patient diagnostic report.

Patrick Ndayizigamiye and Shopee Dube (6) presented about how each transaction is recorded and time stamped, the proposed system provides an irrefutable proof of who conducted the transactions and when the transactions was conducted. This enables traceability of all transactions related to a patient's healthcare. This will assist in forensic audit to hold stakeholders in patient healthcare accountable as the integrity and validity of transactions within the patient's healthcare continuum can be verified. Should any data within the patient's records be tampered with, the hash algorithm will change and will be flagged. In addition, should a patient case need to be escalated from a district to specialised care in a specialized hospital, all is needed is to add another bock to the existing blockchain network instead of creating a new blockchain network and hence increasing traceability of patient's treatment history. This will therefore ease the patient's referral process.

In addition, if permissioned blockchain is used the patient is in control and he/she can decide who to share this information or not Blockchain technology promises to enhance healthcare systems by providing a platform whereby transactions are immutable and traceable within a decentralized ledger. This paper argued that blockchain can contribute to strengthening the South African public healthcare sector by fostering accountability and transparency in patient-centered services. However, since blockchain is a fairly new technology, there is a need for developing standards that define how data is imported from outside blockchain distributed ledger. In addition, there is a need for a regulatory framework that govern when and how data can be accessed by a third party within the public healthcare continuum.

Mansukh deep Kaur et al. (4) proposed their concepts bout how implementing private blockchain in healthcare industries is a best option to secure the information and also very beneficial to maintain the privacy of sensitive data of patients. Private blockchain allows limited access over information and not every participant can have access to data. Private blockchain use strict data access management. Moreover, in this private healthcare technique, only authorized people or patients can access and manage own data and medical records stored in private centralized blockchain which will be accessible to only authorized people. It can be an effective solution to maintain the privacy of data. Secure data management and storage is complicated in healthcare systems due to various security attacks such as data breaches, data theft or leakage, data modification etc. Traditionally, healthcare application was more prone to attacks and were using traditional security methods for protection which was not much efficient. In recent years, blockchain has introduces new security methods and mechanisms for healthcare applications which are providing strong securities and privacy to the information as well as various applications in healthcare such as clinical, biomedical, HER medical as we discussed in this research paper. Blockchain has brought various changed to the data security and application security in healthcare industries.

Shuai Wang and Jing Wang, Xiao Wang (7) presented the framework of blockchain powered PHS based on the ACP approach. The PHSs use an artificial system modelling to simulate and represent the actual healthcare scenarios; then, the training and evaluation of various disease diagnosis and treatment schemes are performed through computational experiments; through parallel execution between the actual and AHSs, the accurate forecasting and guidance of the disease diagnoses and treatments are realized. Next, they reviewed the application of the emerging blockchain technology in the healthcare field and present a preliminary prototype system of the proposed parallel healthcare framework called PGDTS which has been successfully deployed in China. They also propose to build a consortium blockchain that contains patients, hospitals, health bureau, and so on with the purpose of enabling the PHS more integrity, scalability, and security. In the future, they will further improve the blockchain powered PHS and make it available for more disease treatments scenarios.

Thomas K. Dasaklis, and Fran Casino (3) motivated the necessity for a general framework that may gather blockchain technology and context-aware smart health approaches for improving healthcare services. to the current end, three streams of possible synergies between blockchain technology and smart health are identified and further analyzed: (i) consent management, (ii) data sharing during a smart environment, and (iii) research commons approaches. Several challenges for actually implementing blockchain-based applications within the healthcare industry are further discussed. Additionally, various opportunities for future research directions like overcoming certain problems with interoperability, privacy/access control, and data sharing are examined.

3. Technical Preliminaries

3.1 Blockchain Technology

A blockchain could be a variety of shared database that differs from a conventional database within the manner during which it stores information; blockchains store data in blocks that are linked by cryptography. New data is added to new blocks. Once the block is stuffed with data, it's chained onto the previous block in chronological order. There are differing kinds of data which will be stored on a blockchain, but its most typical use has been as a ledger for transactions. Blockchain is employed in Bitcoin in a very decentralized way, in order that no single entity or group has control—rather, all users have control collectively. Decentralized blockchains are immutable, which implies the information entered cannot be reversed. this suggests that Bitcoin transactions are permanently recorded and viewable by anyone.

3.2 Blockchain and privacy protection

A key aspect of privacy in blockchains is that the use of personal and public keys. Blockchain systems use asymmetric cryptography to secure transactions between users. In these systems, each user contains a public and personal key These keys are random strings of numbers and are cryptographically related.

3.3 Working of Blockchain Technology

The goal of blockchain is to permit digital information to be recorded and distributed, but not edited. during this way, a blockchain is that the foundation for immutable ledgers, or records of transactions that can't be altered, deleted, or destroyed. this is often why blockchains are referred to as a distributed ledger technology (DLT).

First proposed as a probe project in 1991, the blockchain concept predated its first widespread application in use: Bitcoin, in 2009.

The amalgamation of the net of Things (IoT), Blockchain and Machine Learning for the anomaly detection within the behavior of the health data of the patient is that the crust of the whole framework. The methodology demonstrated is essentially a system that demands the employment of the net of Things module to intercept and fetch the info that's been generated by the wearable devices worn by the patient. The Blockchain system depicted is preferably utilized for storing and maintaining the information of the patients within the kind of multiple transactions and also support access control to the various stakeholders respectively. Moreover, the Blockchain architecture is additionally used for supporting the medical research by maintaining the pseudo-anonymity of the patient's identification and to supply authenticated and trusted data for more accurate research. The Machine Learning model is employed basically for the detection of anomalies and to forecast certain scenarios that will arise within the due course of your time by analyzing the info supported the parameters that are passed on by the Doctors for basic identification of the conditions that are faced by the patients.

3.4 Transaction and Access Management using Blockchain

The storage of the huge amount of data that is being generated by the patient is required to be managed and processed by maintaining some secured protocol. Moreover, when there are multiple stakeholders associated with the data being generated then a key module that is an access management system is to be implemented which is further addressed by the Blockchain Network. In the proposed architecture we have defined the usage of two vital blockchain networks namely the Personal Health Care (PHC) Blockchain and the External Record Management (ERM) Blockchain. The Personal Healthcare Blockchain is typically maintained by the Patient as it senses and captures the data from the personal wearable devices. The access to the data can be further communicated to the doctor which will be utilized for proper medication and understanding of the ailment that the patient is going through. The data generated by the wearable devices are further stored in an external cloud database which is regulated by the blockchain network.

The External Record Management Blockchain is utilized for the purpose of managing the data that is being generated when a patient goes to the doctor. The ERM Blockchain usually stores the data generated by the healthcare centers, pharmacy bills, medical test reports, prescriptions and image data. The data is being appended to the chain based upon the consensus of all the stakeholders of the blockchain on the “Proof of Stake” algorithm. In the case of ERM Blockchain, the majority stake lies with the Healthcare Center and the Doctor as all other stakeholders are a cumulative holding of them. The Blockchain network also welcomes the access of insurance companies for validating the data of the patient in case of a claim is being raised by the patient.

3.5 Dissemination of Patient Diagnostic Reports using Blockchain Technology

The following steps are involved in the proposed framework:

1) The healthcare provider must have to register in consortium network in order to get the Proof-of-Identity (Poi) i.e., Registration-Id.
2) The healthcare provider uploads patient diagnostic reports using a web user interface.
3) The uploaded report (transaction) gets validated by the local miners using proof-of-work (Pow) approach. This mining process is applied to maintain the consistency in blockchain network.
4) The miner disseminates the transactions among the peers of the blockchain network to verify the transactions with their local copy in order to create the block.
5) The verified transactions get stored into the IPFS distributed storage system. Additionally, the content addressed hash generated by the IPFS gets stored in the blockchain network.

4. CONCLUSION

The medical industry can benefit from blockchain technology in a variety of ways. With this technology, the healthcare services may move to next level in the future, by lowering the costs of tracking, configuration, as well as handling the healthcare big data, similar to how the internet revolutionized healthcare and implemented tele-health. Because of the distributed ledger's availability, as soon as a patient enrolls in the system, the entire set of data will be available at once, greatly reducing processing time. Furthermore, since physicians can access the original, accurate, and quality source-documented data in real time, they won't have to worry about the patient giving them an honest medical history, minimizing the risk of medical history errors. Patients won't have to think about getting another opinion from another physician because the data is transparent. Due to the patients’ records stored on a blockchain network, stakeholders can interact with several others worldwide with similar medical conditions, which will not only benefit their wellbeing but also make them feel welcomed, encouraged, and give them more willpower to fight the disease. Also, the patients can have full control of their data and will be able to choose who they share it with.

REFERENCES

1. Gupta, R., Shukla, A., Mehta, P., Bhattacharya, P., Tanwar, S., Tyagi, S., & Kumar, N. (2020). Vahak: A Blockchain-based outdoor delivery scheme using UAV for Healthcare 4.0 services. *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. doi:10.1109/infocomwkshps50562.2020.9162738

2. Chakraborty, S., Aich, S., & Kim, H. (2019). A secure healthcare system design framework using Blockchain technology. *2019 21st International Conference on Advanced Communication Technology (ICACT)*. doi:10.23919/icact.2019.8701983

3. Dasaklis, T. K., Casino, F., & Patsakis, C. (2018). Blockchain meets Smart Health: Towards Next Generation Healthcare Services. *2018 9th International Conference on Information, Intelligence, Systems and Applications (IISA)*. doi:10.1109/iisa.2018.8633601

4. Kaur, M., Murtaza, M., & Habbal, M. (2020). Post study of Blockchain in smart health environment. *2020 5th International Conference on Innovative Technologies in Intelligent Systems and Industrial Applications (CITISIA)*. doi:10.1109/citisia50690.2020.9371819

5. Kumar, R., Marchang, N., & Tripathi, R. (2020). Distributed off-chain storage of patient diagnostic reports in healthcare system using ipfs and Blockchain. *2020 International Conference on COMmunication Systems & NETworkS (COMSNETS)*. doi:10.1109/comsnets48256.2020.9027313

6. Ndayizigamiye, P., & Dube, S. (2019). Potential adoption of blockchain technology to enhance transparency and accountability in the public healthcare system in South Africa. *2019 International Multidisciplinary Information Technology and Engineering Conference (IMITEC)*. doi:10.1109/imitec45504.2019.9015920

7. Wang, S., Wang, J., Wang, X., Qiu, T., Yuan, Y., Ouyang, L., . . . Wang, F. (2018). Blockchain-powered parallel healthcare systems based on the ACP approach. *IEEE Transactions on Computational Social Systems, 5*(4), 942-950. doi:10.1109/tcss.2018.2865526

8. Omar, I. A., Jayaraman, R., Debe, M. S., Salah, K., Yaqoob, I., & Omar, M. (2021). Automating procurement contracts in the healthcare supply chain using blockchain smart contracts. *IEEE Access, 9,* 37397-37409. doi:10.1109/access.2021.3062471

9. Bodeis, W., & Corser, G. P. (2021). Blockchain adoption, implementation and integration in Healthcare Application Systems. *SoutheastCon 2021*. doi:10.1109/southeastcon45413.2021.9401885

10. Bazel, M. A., Mohammed, F., & Ahmed, M. (2021). Blockchain technology in healthcare big data management: Benefits, applications and challenges. *2021 1st International Conference on Emerging Smart Technologies and Applications (eSmarTA)*. doi:10.1109/esmarta52612.2021.9515747

11. Zhao, H., Bai, P., Peng, Y., & Xu, R. (2018). Efficient key management scheme for Health Blockchain. *CAAI Transactions on Intelligence Technology, 3*(2), 114-118. doi:10.1049/trit.2018.0014

12. Bhuiyan, M. Z., Zaman, A., Wang, T., Wang, G., Tao, H., & Hassan, M. M. (2018). Blockchain and Big Data to transform the healthcare. *Proceedings of the International Conference on Data Processing and Applications - ICDPA 2018*. doi:10.1145/3224207.3224220