EasyChair Preprint

№ 5987

Implementation of a Secure and privacy-aware E-Health record and IoT data Sharing using Blockchain

Sarath Sabu, H M Ramalingam, M Vishaka, H R Swapna and Swaraj Hegde

July 3, 2021

KeAi
CHINESE ROOTS
GLOBAL IMPACT

ScienceDirect

Procedia Manufacturing 00 (2019) 000–000

Global Transitions Proceedings

http://www.keaipublishing.com/en/journals/global-transitions-proceedings/

Global Transitions 2019, 14 October, 2019 - 16 October, 2019, Tsinghua University, Beijing, China

Implementation of a Secure and privacy-aware E-Health record and IoT data Sharing using Blockchain

Sarath Sabu[1*] , Ramalingam H M[2] , Vishaka M[3*] , Swapna H R[4*] , Swaraj Hegde[5*]

Department of ECE, *MITE*, *Moodabidiri*, 574225,*India*,Affiliated to VTU, Belagavi *
Senior Asst Professor,*Department of* ECE, *MITE*, *Moodabidiri*, 574225,*India*,Affiliated to VTU, Belagavi[2]

* Corresponding author. Tel.: +91-949-619-2307; E-mail address: sharatsaboo@gmail.com;

Abstract

Medical applications are fast growing in popularity, both for professional use and for patient-centered apps. The current Health record and IoT data sharing systems however have a fair amount of problems associated with privacy and security. The secure and privacy aware E-Health record to propose a mechanism using blockchain and IPFS (InterPlanetary File System) which offers a solution to all these problems. It also includes limitations and safeguards on what can be done and cannot be done with your personal information in some cases. The IPFS data will be dispersed among the nodes. Use of IPFS (Interplanetary File System) to store health records, which has the benefit of being distributed which in turn makes record tamper-free. In addition, the proposed model keeps track of disease statistics without invading any patient's privacy. This is conceivable not only for web pages, but for any type of file that a computer might save, whether it's a document, an email, or even a database record, thanks to IPFS.

Keywords: Blockchain, E-Health Record, IPFS, IoT Data Sharing.

1. Introduction

A Medical Health Record (MHR) is a digitized version of a patient's medical data. In the advanced environment of Information and Technology, Electronic Health Records are playing a vital role in the medical field. But have the problems of security and privacy of patient medical health reports [1]. We see many are working to overcome these issues by applying the concept of cloud-based systems and Ethereum blockchains, which allows the patient and doctors across, the world to be connected. It gives full control for the patient to access their data and can grant permission for others to view their data [2]. Today we are using our devices like mobile to carry our photos, video, emails, and event banking services but we are still unable to hold on to our medical records since in healthcare ecosystem is increasingly complex with stakeholders involved in difficult and important data interactions This can result in issues with privacy, information security, and operational efficiency. As a result, the issue of data-related health interoperability remains unresolved [3].

Blockchain technology was introduced in the year 2008 by Nakamoto, who published an article on Bitcoin. It is a peer-to-peer network of nodes that talks to one another [4]. The important features of blockchain are a decentralized network, distributed database, improved security, and having a peer-to-peer transaction verifiable, so in the healthcare system, blockchain technology has the potential in protecting patient information. Blockchain is a sophisticated data structure in which growing records are stored in blocks, information, current block hash, previous block hash, and timestamp are the 4 elements of these blocks [5]. So, when we add new data blocks to the blockchain, each new block is linked to the previous one. using a hash value which makes it immutable, and all the workflow is recorded are time-stamped which places an identity to it and the replicas are distributed to each network node that is a participant, this guarantees that the data integrity is kept between the endpoints without any human involvement [6].

IPFS (InterPlanetary File System) is a distributed storage method which is a peer-to-peer (P2P) bit torrent like method that aims to link all digital devices to the same file system of files, enabling the storage of huge quantities of medical records. Instead of storing the patient's health records in the blockchain network, only the hash address of the data needs to be stored [7]. IPFS is used to store digitized content with high integrity and globally available to everyone [8]. Since IPFS is distributed, it has no single point of failure [9]. IPFS also

includes a content-addressed block storage model for maximum bandwidth [10].

In the previous few years, The Internet of Things (IoT) has become increasingly widespread in recent years, especially in the healthcare sector [11]. As technology starts evolving the growth of IoT and wearable devices in the medical field starts to increase this has improved the quality of health care. Wearable devices gather patient health data and assign it to hospitals or doctors [12]. This medical data generated from wearable IoT devices are critical and sensitive. This data needs to be protected carefully because it's directly related to a patient's life. Blockchain is a good solution to safeguard medical data generated by these IoT devices [13].

2. Related Works

The blockchain techniques were launched in Bitcoin, in which each block is linked to former blocks using a hash value. It means the transactions once created are immutable [4]. Blockchains are gaining a lot of attention from researchers and scientists in the modern world for a variety of reasons, which include access control, data protection, privacy, and decentralization of wireless networks, and the health care environment is fast evolving as the technology evolves, with the advancement of electronic data related to health, patient data protection regulation and new chances are opening up for the health data management, also the convenience for patients to access their health records.[14].

Blockchain is a new, emerging, and disruptive technology that can provide a solution to the authenticity of digitized records. However, blockchain is a costly data storage platform, particularly for big amounts of data and digital material. We recommend using an IPFS file system for storing large amounts of data and content [11]. When comparing traditional storage methods like HTTP to IPFS, we can see that HTTP has a lot of shortcomings, including incompetence, lack of historical versioning, and centralization. As a result, IPFS overcomes HTTP's downsides [6]. Many health record systems are not developed to serve the needs and prerequisites of patients, resulting in challenges such as inefficiency and poor system adaptation. They also suggest the use of EHRs has introduced negative significances to information processing. Because of these issues, it is reasonable to seek out a platform that can assist in the transformation of the healthcare sector to one that is focused on patients, i.e., blockchain. A platform that is transparent, secure and also delivers data integrity to the health records of the patients. [15].

In the previous EHR models, the data is maintained in a cloud which have third-party dependency. A scheme for key management is employed to secure medical data. The data gets switched amongst peers by using a secret key. However, the typical use only one key for the exchange of data . Hence, if the key is known to the opponent, then data can be compromised or tampered with [7]. Blockchain always sets a time stamp on all the workflow and also gives an identity to it and the copies are distributed among all the nodes in the network. Although there are many advantages of blockchain it also has few drawbacks that create some domain-specific challenges. The 4 main challenges blockchain technologies face are scalability, storage, privacy, modification, and regulations. A few solutions for the above problems are:- Do not store personal data on the blockchain instead we can use IPFS to store data and the hash from IPFS we will store in blockchain. Record personal data pseudo-anonymously. The stored information in the referenced local database [10]. Traditional databases can be applied to the storage of data but it is a central authority to take control of a big quantity of data, one cannot trust the confidentiality, integrity, and authenticity of the data. Blockchain is made up of an increasing number of technology blocks that are linked by cryptographic algorithms. It is a distributed ledger in which there are no centralized data stores. The distributed Smart contracts can be written using ledger technology, which eliminates the need for a mediator by automatically defining and enforcing rules and duties set out by the parties in the ledger. IPFS it's possible to use as a peer-to-peer, storage system that is spread hypermedia in large quantities. It uses a block storage approach with address linkages to the contents that make up a Merkle Directed Acyclic Graph (DAG). Since IPFS is distributed, it has no chance of failure [9].

Many EHR technologies came into the picture to store medical records, but the present electronic health record system has its problems associated to privacy and security. Some of the systems also used blockchain to overcome problems related to security concerns but they included complex medical procedures for accessing and managing a big quantity of medical data [1].

Variety of sensors, devices, and vehicles have been connected to the Internet in recent years. One of these technologies is remote patient monitoring Nowadays, it is usual to treat and care for patients in this manner. However, these technologies also have Digital data transmission and logging of data communications raises privacy and security concerns. The solution for data privacy, security of the health data could and is blockchain technology, each block has a Block Header and a Transaction. Counter, as well as transaction [12].

The majority of the papers that have been evaluated point to ECG monitoring in particular as which are in charge of the first remote vital sign monitoring and the second of a telemedical ECG system of a patient. All of these systems, while excellent, have specific issues with the treatment of certain diseases that affect people in the global economic and social arena. It is a very important way to develop a comprehensive solution because medical data generated from wearable IoT devices includes critical information of a patient. Many systems are already existing which fail to transfer these medical IoT device data securely. [16]

3. Proposed Model

The major requirements of the proposed models are:

1. The model must be a patient-centric platform in which the patient has complete control over their data.
2. The patient should have the ability to grant and revoke access to the records as and when they wish to do so.
3. Live data of a patient is sharable to doctor using wearable IoT devices in a protected environment.
4. Patient's data must be stored in IPFS which ensures the benefit of being dispersed and immutability of records and hash of the record only must be stored in Blockchain.
5. A doctor can seek permission from the patient to gain to his/her medical record.

Implementation of a Secure and privacy-aware E Healthrecord and IoT data Sharing using Blockchain is designed with the regulation of general data protection and regulation (GDPR). Concern management is a process that receives the problem or concerns that providers methods of tracking through the problem-solving stages. It is a legal framework that establishes rules for the privacy of individual data of people who reside in the European Union (EU). In our platform, the patient will be having complete access to his/her medical record and the patient can share his/her medical record with any of the doctors (for example: - if a patient wants to consult the doctor, the patient can share his/her access to the doctor to view his/her medical history) If the doctor wants to take consult from any of his/her colleagues, our platform allows the doctor to share the patient's medical record with his/her colleagues but only with the fullest control of the patient. Here we are ensuring or implementing the same with the help of concern management with the backbone of blockchain.

Blockchain is a record-keeping technology that uses a decentralised distributed database to keep data secure and safe. The list of records is kept in a block, and the blocks are linked together to form a chain, which is referred to as a Blockchain. Hacking a blockchain is tough because if one block is hacked, the attacker must hack every block because each block's hash pointer is linked to the next. Blockchain technology offers a wide range of applications in a variety of industries. Identity management, smart contracts, supply chain analysis, and other applications of blockchain are already in use. The true promise of blockchain technology is probably to be tapped anytime in the near future.

We created intermediate platform for doctor and patient, Medical Health Record Chain (MHR Chain). In this Model initially patient will register to platform by providing all necessary details. After registration patient can add medical record details along with pdf or image record file, which will be stored in distributed environment. Here we are using IPFS where medical image file or pdf will be splitted and stored in several nodes of server only hash will be retrieved from the server. This hash in turn will be stored in blockchain which allows secure storing of medical records which increases the retrieval efficiency.

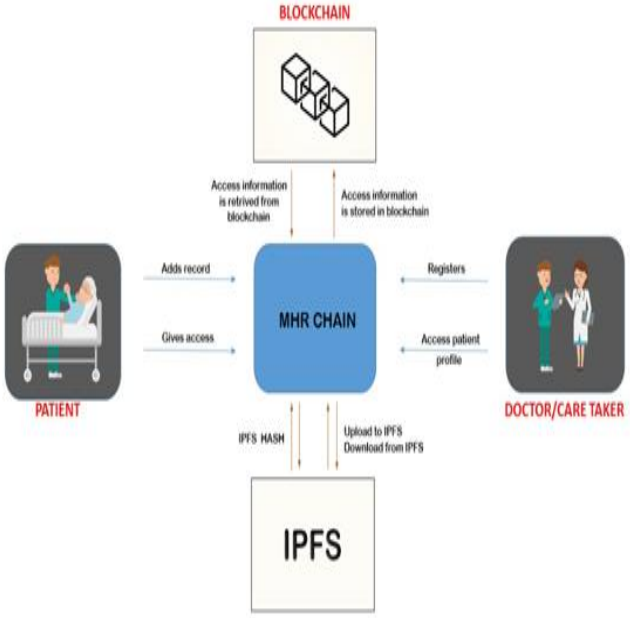

Figure 1: System Architecture

"System architecture mentioned in figure 1" platform is mainly concentrated to serve between patient and doctor, the patient can provide his/her digitalized medical record to the doctor during consultation safely and securely by ensuring privacy. All the transaction between the doctor and the patient is recorded in the blockchain with the time stamp. To store the data in blockchain we need to go for private or public blockchain, since private blockchain is a bit complex and the maintenance of its infrastructure is difficult so here we are using it to create a public blockchain to store data. We are all aware that blockchain is not suitable for storing a large data, storing huge data will slow down the blockchain furthermore and blockchain, however, is a pricey data storage media, especially for big amounts of data and digital material.

We propose utilizing to store vast amounts of data and content efficiently. Using an IPFS is an open-source file system. The system, which is a distributed, file system that isn't centralized and a platform to store data and files with high integrity and resiliency. Here when a patient uploads a medical record it will be first uploaded in the IPFS This has the benefit of being widely disseminated and ensures the immutability of records then there's the hash returned from the IPFS is only blockchain-based storage which again improves the security of

data since blockchain is a distributed network, this ensures the secure storage of records. The use of IPFS not only increase the security of data but also improves the retrieval efficiency of data.

4. Result and Discussion

The methodology that we adopted here can be employed for supply chain management, multimedia transfer to maintain the privacy of data, then we could use it in social media to maintain our privacy especially in the case of matrimonial sites where We are in charge of the situation where people can see our profiles and IoT

This system can be used by the patient to share live data with the doctor using blockchain and IoT devices as we can see in the figure. Once the patient Login to this platform the patient can share the live data, the doctor will be requested for access. After receiving access from the patient the doctor can view the LIVE data of the patient wearing a wearable IoT device. The audit is maintained using blockchain for the future reference of the patient with a time stamp.

Now let's compare MHR Chain model with other existing systems/models.

Name	Distrib -uted Ledger	IPFS used to Store Data	IoT Data Sharing	Patient Centric Platfor- m
MedRec [17]	✓	X	X	X
MeDShare [18]	✓	X	X	X
Secure and Trustable Electronic Medical Records Sharing using Blockchain [19]	✓	X	X	✓
Proposed Model MHR Chain	✓	✓	✓	✓

Table 1: Comparison with Related Works

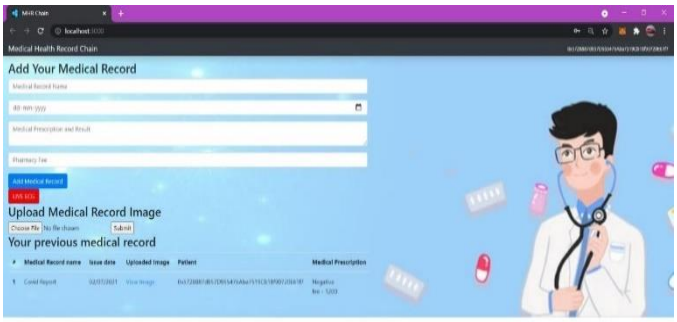

Figure 2: Patient Page

Here, Figure 2 shows the patient's page where the patient can add his\her medical record, the patient can see their previously added medical report, and also can share Live ECG by wearing wearable IoT devices.

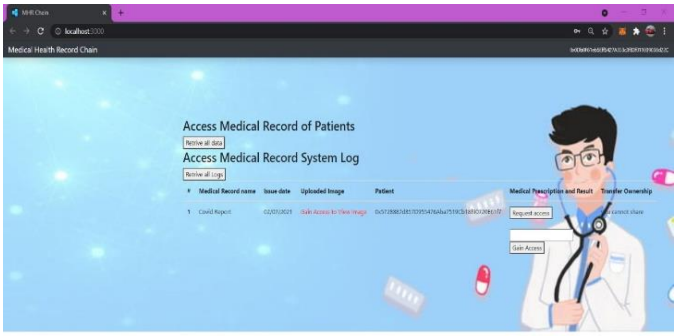

Figure 3: Doctor Page Before Access

Figure 3 shows the doctor's page before accessing the medical report of the patient. Since we are concerned with the patient-centric platform, patient authentication through OTP is needed for the doctor to gain access to the medical report of the patient.

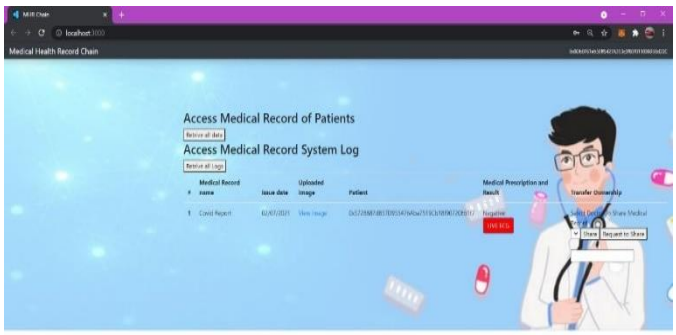

Figure 4: Doctor Page After Access

Figure 4 shows the doctor's page after gaining access to the patient medical record. The doctor will get complete access to the medical report along with the time stamp added by the patient including a Live ECG of the patient.

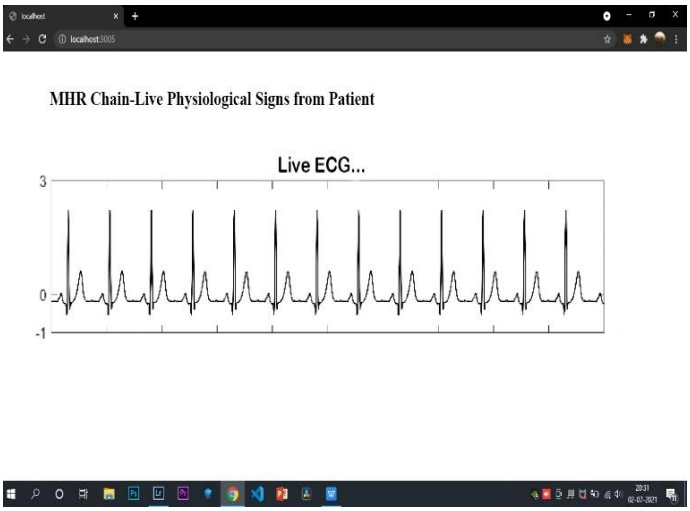

Figure 5: LIVE ECG

Figure 5 shows the live ECG of the patient wearing a wearable IoT device which can be used in a heart monitoring system to find the malfunction of the heart.

5. Conclusion

We combined blockchain and IPFS (InterPlanetary File System) in this model to overcome the majority of the challenges we face in the healthcare sector. This system aids in the secure and efficient storage and sharing of data. This system includes smart contracts to keep data on the blockchain, which is more timeless and functional. Sometimes the distance between the doctor and patients will be a major problem to get a health-care service quality and also trouble in regular health monitoring. So IoT based medical healthcare system helps the patient to get proper medical attention at a place where they are comfortable. The ECG device is implemented and successfully acquires the result of the patient. Hence, the reduced computational complexity and also the flexible use of the device help the patient to get smooth regular medical monitoring from the doctor. Interoperability is a challenge for EHR systems. The limitations of medical health record system is because doctors or hospitals have access to a patient's records, the healthcare sector is affected. If a patient wishes to view his medical records, he must go through a lengthy and inconvenient process. With greater privacy and security protections in place, as well as cutting edge technologies, EHRs may soon serve as the backbone for a revolution in digital health record monitoring, and data security methods and approaches can be used to digital monitoring in banks, finance, supply chain management, social media, the internet of things, and other industries.

Acknowledgments

We would like to thank Mr. H M Ramalingam, Senior Assistant Professor, Dept of ECE, Mangalore Institute of Technology & Engineering for the efforts in providing valuable insights and comments and helping us in many ways.

References

[1] Reen, G. S., Mohandas, M., & Venkatesan, S. (2019). Decentralized patient centric e-Health record management system using blockchain and IPFS. 2019 IEEE Conference on Information and Communication Technology, CICT 2019. https://doi.org/10.1109/CICT48419.2019.9066212

[2] Shahnaz, A., Qamar, U., & Khalid, A. (2019). Using Blockchain for Electronic Health Records. IEEE Access, 7, 147782–147795. https://doi.org/10.1109/ACCESS.2019.2946373

[3] Mayer, A. H., da Costa, C. A., & Righi, R. da R. (2020). Electronic health records in a Blockchain: A systematic review. Health Informatics Journal, 26(2), 1273–1288. https://doi.org/10.1177/1460458219866350

[4] Alam Khan, F., Asif, M., Ahmad, A., Alharbi, M., & Aljuaid, H. (2020). Blockchain technology, improvement suggestions, security. challenges on smart grid- and its application in healthcare for sustainable development. Sustainable Cities and Society, 55(November 2019), 102018. https://doi.org/10.1016/j.scs.2020.102018

[5] Abu-elezz, I., Hassan, A., Nazeemudeen, A., Househ, M., & Abd-alrazaq, A. (2020). The benefits and threats of blockchain technology in healthcare: A scoping review. International Journal of Medical Informatics, 142(February), 104246. https://doi.org/10.1016/j.ijmedinf.2020.104246

[6] Onik, M. M. H., Aich, S., Yang, J., Kim, C.-S., & Kim, H.-C. (2019). Blockchain in Healthcare: Challenges and Solutions. In Big Data Analytics for Intelligent Healthcare Management. Elsevier Inc. https://doi.org/10.1016/b978-0-12-818146-1.00008-8

[7] 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 and NETworkS, COMSNETS 2020, 1–5. https://doi.org/10.1109/COMSNETS48256.2020.9027313

[8] Nizamuddin, N., Hasan, H. R., & Salah, K. (2018). IPFS-blockchain-based authenticity of online publications. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 10974 LNCS, 199–212. https://doi.org/10.1007/978-3-319-94478-4_14

[9] Rajalakshmi, A., Lakshmy, K. V, Sindhu, M., & Amritha, P. P. (2018). A Blockchain and IPFS based framework for secure Research record keeping. International Journal of Pure and Applied Mathematics, 119(15), 1437–1442.

[10] Benet, J. (2014). IPFS - Content Addressed, Versioned, P2P File System. Draft 3. http://arxiv.org/abs/1407.3561

[11] Alblooshi, M., Salah, K., & Alhammadi, Y. (2019). Blockchain-based Ownership Management for Medical IoT (MIoT) Devices. Proceedings of the 2018 13th International Conference on Innovations in Information Technology, IIT 2018, 151–156. https://doi.org/10.1109/INNOVATIONS.2018.8606032

[12] Dwivedi, A. D., Srivastava, G., Dhar, S., & Singh, R. (2019). A decentralized privacy-preserving healthcare blockchain for IoT. Sensors (Switzerland), 19(2), 1–17. https://doi.org/10.3390/s19020326

[13] Chendeb, N., Khaled, N., & Agoulmine, N. (2020). Integrating Blockchain with IoT for a Secure Health-care Digital System. 1–8. https://hal.archives-ouvertes.fr/hal-02495262

[14] Khatoon, A. (2020). A blockchain-based smart contract system for healthcare management. Electronics (Switzerland), 9(1). https://doi.org/10.3390/electronics9010094

[15] Shahnaz, A., Qamar, U., & Khalid, A. (2019). Using Blockchain for Electronic Health Records. IEEE Access, 7, 147782–147795. https://doi.org/10.1109/ACCESS.2019.2946373

[16] Patil, P., Waichal, R., Kumbhar, U., & Gadkari, V. (2020). Patient Health Monitoring System Using Iot & Gsm. Journal of Critical Reviews, 7(05), 638–641. https://doi.org/10.31838/jcr.07.05.340

[17] A. Azaria et al., ”MedRec: Using Blockchain for Medical Data Access and Permission Management,” Open and Big Data (OBD) International Conference on, pp. 25-30, 2016

[18] Qi Xia, Emmanuel Boateng Sifah, Kwame Omono Asamoah, Jianbin Gao, Xiaojiang Du AND Mohsen Guizani, ”MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain”, IEEE Access, Vol.5, pp.14757-14767, 2017

[19] Alevtina Dubovitskaya, Zhigang Xu, Samuel Ryu, Michael Schumacher and Fusheng Wang, ”Secure and Trustable Electronic Medica Records Sharing using Blockchain”, ArXiv170906528 Cs, 2017.