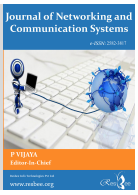
Vol.5 No.4 Oct 2022

Journal of Networking and Communication Systems

Received 19 July, Revised 27 September, Accepted 1 October



Access and Secure Storage Based Block Chain Scheme with IPFS Implemented in Electronic Medical Record in Lahore, Pakistan

Fahad Saddique
Institute of management Science, Lahore.

Nauman Mushtaq
Institute of management Science, Lahore.

Raza Hasan
Computing and IT, Global College of Engineering and Technology

Zia Ul Rehman
Institute of management Science, Lahore.

Muhammad Ali
Hon Superior University, Lahore.

Abstract: This work is now contributing to creating a system built on the effective sharing of secure IPFS (Interplanetary file system) for electronic medical records and, in addition, implementing a cipher text policy system in conjunction with the interplanetary file system (IPFS) and the most recent developments in blockchain technology. This strategy helps to govern the effectively while preventing retrieval access to electronic medical data. In addition, with the use of the technology known as the blockchain, which has traceable features along with being safe and allowing for the search of medically relevant data, it also contains a security-proof method related to assaults on the term that specify. The fact that the performance-based analysis system and the primary data set are being simulated demonstrates that it is both possible and efficient.

Keywords: *Attribute-Based Encryption, Access Control, Blockchain, Interplanetary File System, Electronic Medical Record*

1. Introduction

These days, the medical records of each patient are a significant asset for the healthcare provider. This data must be accurate across all their services, and privacy and security are important considerations. It is a significant challenge for every patient, but the most recent iteration of blockchain technology offers a solution. A decentralized ledger system for secure, transparent transactions, eradicating the requirement for intermediaries or involvement of third-party [14]. It is a decentralized system which permits for transactions to be recorded and verified by a network of users, before a central authority [15]. The main aspects of blockchain technology is that it presents a high level of transparency and accountability, as every transaction can be traced and verified by all users in the network. Additionally, it presents a high degree of security, as any effort to tamper with the data on the blockchain would need a consensus between the majorities of users in the network [16] [17]. Blockchain technology has several applications in industries, like finance, supply chain management, healthcare, etc [18]. This technique could help create a secure method for storing personal data, complete with hash chain characteristics such as transparency and data integrity [1]. Now, innovation delivers all the data as an electronic system primarily used in clinical treatment. It includes electronic and image clinical records, irresistible diseases, and indicative reports. Nevertheless, it is still having issues with security. They can make efficient use of this clinical information by examining it in this way.Fig.1 Secure Storage System for Medical Record.

https://doi.org/10.46253/jnacs.v5i4.a2

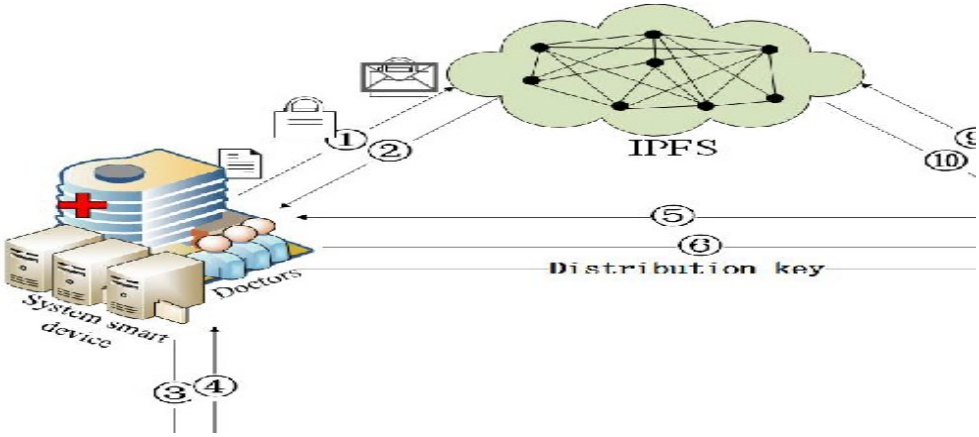


Fig. 1. *Diagrammatic representation of secure storage system for medical record*

Information about electronic clinical trials is readily available from the treatment provided to patients. In most cases, the techniques that have been used in the past to save data are not very successful, and the information may be mishandled. Counting clinical professionals, medical caretakers, and patients is necessary to get accurate information. This problem is one that blockchain technology is working to fix [2]. The user may be deciphering encrypted text in order to fulfill the requirements of the admission strategy. A blockchain-based record system with information recovery capabilities has been developed in response to this need. In the current investigation, the request was made to construct practicable access for controlling records for the investigation of cloud employees, which is semi-legitimate and led by initiatives. In addition, it has created a property basis encryption safe capacity storing system for healthcare records in the IPFS. It also covers the plan to influence IPFS as the capacity stage with the blockchain search system. Fig. 2. Block Chain-Based Storage with IPFS:

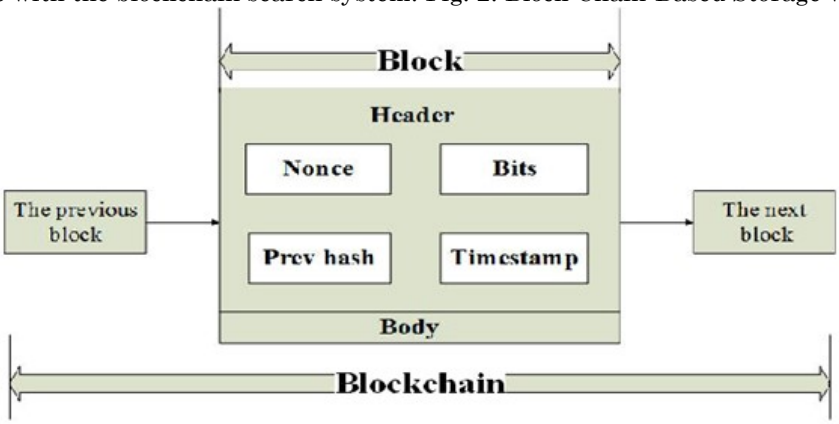


Fig. 2. *Block chain based storage with IPFS*

The following advantages are included in our plan of study:

1. Safe Storage: This refers to storing information using a distributed Inter-Planetary document framework (IPFS) system rather than a half-legitimate and inquisitive cloud worker, offering an additional layer of safety for clinical data. Additionally, 1PFS allots a unique hash value to each piece of information record that it stores. Consequently, records can only be stored away once while simultaneously freeing up some more space.

2. For this one perspective: users can quickly locate the relevant clinical records based on the preset keywords. In addition, users can validate the record's originality and monitor wellspring clinical documents.

3. Control Access: To keep irrelevant patient information from the clinical history, we will implement individual access contingent on the client's characteristics and encoded with ciphertext. The following topics are investigated in the study: The task is related to our strategy, and it segments the plan, provides a framework and security model, nuances the plan, and helps realize the plan. In conclusion, we will conclude the whole research.

2. Literature Review

The attribute and key policy basis were used with the cypher text in a biometric identification system. Because attribute encryption enables secure data access management at a granular level, it is becoming more popular for usage in various contexts [4]. The most common technique of securing medical data while saving money on local storage and ensuring data security is using attribute-based encryption and outsourcing data administration to cloud servers. This strategy also ensures that data was secure. It has been shown that attribute keyword searches with effective operator revocation was more scalable and permit search authorization. It enables many owners to partition their data and store it in separate locations on the cloud. The cloud server has successfully supplied all positive outcomes, and Guo has presented an access control architecture. They are used to encrypt medical data and assign it to various users, each of whom has a unique set of permissions to browse the records. However, the correctness of most search results cannot be verified, and the server waste resources by delivering a huge number of results that were irrelevant to the research. A cloud Su et al. [6] presented a system for attribute-based encryption as their contribution. It enables the server to reduce the amount of encryption while maintaining the integrity of the purity protection scheme that Miao et al. suggested. [7]. Using a tree access policy helps enable fine-grained control for data access while facilitating data sea. In any event, data storage was handled by an inquisitive and trustworthy cloud server in every one of the approaches described above. If even a single component of the cloud architecture fails, accessing any cloud servers will be impossible.

The idea was put out by Li et al. In file hierarchies, attributes encrypt various files at the same level. It would allow cloud storage users to have control while being flexible and safe. On the other hand, attribute encryption is used to resolve security concerns for essential authorities. The program was expanded to suit major multi-sector organizations and corporations, which has caused it to become inefficient. Because it provides vital information for the healthcare system, an accurate record-keeping system was necessary for the next appointment with the patient. Before uploading patient data to cloud servers for further processing, it was standard practice for medical facilities to encrypt such documents first. Wang and Lin [9] have developed mobile application access policies for PHRs within a semi-trusted system. They have optimized existing MA-ABE programs to introduce lazy and proxy technology to address the efficiency and security issues associated with mobile application access to personal health records. In addition to this, they are putting up PHR mobile application policies along with a framework. Using cypher text policy was the strategy that was offered by other research as a means of regulating medical data [10]. The cloud server was superior because it has a centralized management system; if just one server goes down, the whole network fails. whereas (IPFS) was used to disperse the system's storage space. It can store and share a wide variety of different types of data. It features a decentralized storage mechanism that helps to eliminate the need to store the same file continually. It eliminates the possibility of any errors occurring when storing many files for storage [12].

As a consequence of this, IPFS was a superior option to cloud servers for the storage of patient information. A single user was provided with this information via IPFS and blockchain [13]. Based on the prior study's findings, we suggest using IPFS with blockchain to store medical data. Every user was provided with the capacity to search for their privacy and the opportunity to verify information using this system.

3. Proposed Method

We propose a method with storage for this medical record and access to it. Its scope extends from patient registration up to the final diagnosis. The patient can get all their information from the database at any moment. In this case, protecting the patient's privacy must be a priority. Before uploading patients' medical records to IPFS for preservation, the doctor must get the patients' signatures on such records.

In contrast to the blockchain, the address is sent directly to the doctor when the data is transmitted. The data may be accessed using the transaction identifier taken from the blockchain. The medical professional can view the patient's record using smart gadgets anytime. A patient has access to his previous records via a smart device. It checks their record and then delivers a search token following validation. A smart device allows the patient to access his old record.

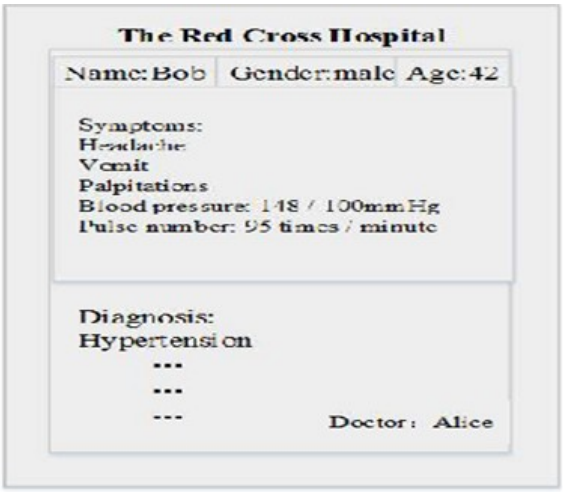


Fig. 3. *Medical record of Bob*

After this, the Diagnosis Hypertension system will access the block ID contained in the search token hash value and compare it to the block ID present on the blockchain to determine whether or not the address is token tramped. Then DU is used to confirm the address, after which it will download IPFS ciphertext. Aside from that, the medical records are encrypted and acquired via DU by using its safe secret Key in the process. When DU is complete, it does a check to see whether or not the hash value agrees with the one that is stored on the blockchain. Alice works as a doctor at the Red Cross facility, and Bob is a patient interested in visiting the hospital. A pair of public and private keys for him is produced based on his characteristics, including his name, age, gender, and identification as a patient. Bob's identification is verified at the Medical Centre using this public-private key pair. After Bob's diagnosis, Dr Alice produced his medical record, which is shown in Fig. 3, as follows: Alice has to begin by encrypting the medical record R before she can receive the cypher text CT. Second, Alice will create sig R by signing the cypher text CT. Alice's value was saved in the IPFS (Sig R, CT) as a last and concluding point. The IPFS then directs record requests to the address (h). The tuple representation of the encrypted hash address: Alice broadcasts a transaction on the blockchain by putting the hash values of (Hr and h) together, which allows her to retrieve the block ID. Alice pulls the information on Bob, a 42-year-old male with hypertension, from record R and then generates index lwj ji, mi for the keyword w.

The key = Bob's entry describes Bob as a hypertensive male. The first thing that Bob does whenever he comes back is to pull up R's previous medical file, and then he sends a request to the hospital, which includes the word "Bob, male" as an important part of the record. After the smart system gadget has established that Bob is who he claims to be, it will return for 10 STw = (ID, h, y). Now that Bob has established that the address h included in the token STw is accurate, they access the IPFS to get the encrypted medical record CT and use the address as a reference point. It was when he deciphered the medical record with his unique Key that he could finally access it. Registered users of the medical system can upload and search medical records (e.g., physicians, nurses, patients, researchers, etc.). Inpatient stays at a medical facility, and follow-up appointments with a primary care physician are covered under our plan.

We utilized data in the Paring Based Cryptography (PBC) laboratory to assess the solution's performance. The testing was done on server 15.4, which had a CPU that was an Intel Core i5. During our tests, we set Zp to 160 bits and GI to G2-to-GT-to, a total of 1024 bits in each case. As a consequence of the attributes of our plan, the ABKS-UR V and KSE schemes are impacted. Because the number of attributes substantially influences the performance of our KeyGen, Index, and Search algorithms, it enables [0,50] and [5], respectively. Compared to the VKSE and ABKS-UR schemes, our method involves a greater degree of administrative burden because we must generate the search and the secret private keys on an individual basis. The effectiveness of our system will improve if we choose not to include the feature in the algorithms, we use for indexing and searching.

Figures such as this one demonstrates that the technique has fewer overheads in terms of storage and computation compared to the YKSE and ABKSUR methods. As a consequence of this, our method is comprehensively safe and effective in every respect. Consequently, the outcomes of the theoretical analysis and the fundamental data analysis are consistent. Our approach offers lower expenses associated with storage and computation compared to both VKSE and ABKS-LTR. A further benefit is that it provides a mechanism for verifying the results without additional storage or processing resources, which is a significant benefit.

As a consequence of this, the findings of our simulations indicate that our system is both reliable and efficient. We use blockchain technology for this encryption system, combined with the InterPlanetary File System, to ensure the exchange of medical records in a safe, secure, and efficient (IPFS). Access to this system is only granted to those who can demonstrate their valid link to the patients.

Symbol	Description
R	electronic medical record
Sig_R	signature of electronic medical
I_{wj}	index of electronic medical rec
H	hash address returned by IPFS
h_R	hash of electronic medical recc
h_I	hash of index for electronic me
(T_1, T_2)	access request
W	access policy
S	attribute set of data user

4. Conclusion and Future Studies

IPFS storage was developed as an alternative to the dubious but fascinating cloud server to ensure safe data storage. This technology records search processes and storage, assuring data originality and traceability, resolving security issues as a central authority, and ensuring safe data storage. Despite these disadvantages, this system nevertheless provides users with several benefits, such as the capability to provide access to people whose credentials have just become invalid and the capacity to store data in the blockchain. In the following study, we will investigate the possibility of using attribute revocation to solve the problem of lapsed user access rights. In addition, we will include smart contracts in our strategy to make the data stored on our blockchain more reliable and applicable.

Compliance with Ethical Standards

Conflicts of interest: Authors declared that they have no conflict of interest.

Human participants: The conducted research follows the ethical standards and the authors ensured that they have not conducted any studies with human participants or animals.

Reference

[1] Van Doren J, Arns M, Heinrich H, Vollebregt MA, Strehl U, K Loo S. Sustained effects of neurofeedback in ADHD: a systematic review and meta-analysis. doi: 10.1007/s00787.

[2] Sun, J., Yao, X., Wang, S., & Wu, Y. Blockchain-Based Secure Storage and Access Scheme for Electronic Medical Records in IPFS. IEEE Access, Vol.8, pp.59389-59401, 2022.

[3] Chen Y, Ding S, Xu Z, Zheng H, Yang S. Blockchain-Based Medical Records Secure Storage and Medical Service Framework. J Med Syst., Vol43, no.1,pp.5, 2018. doi: 10.1007/s10916-018-1121-4. PMID: 30467604.

[4] Sahai, A., Waters, B. Fuzzy Identity-Based Encryption. In: Cramer, R. (eds) Advances in Cryptology EUROCRYPT 2005. EUROCRYPT 2005. Lecture Notes in Computer Science, vol 3494, 2005, Springer, Berlin, Heidelberg. https://doi.org/10.1007/11426639_27

[5] Canard, S., & Trinh, V. C., Constant-size ciphertext attribute-based encryption from multi-channel broadcast encryption. In International Conference on Information Systems Security (pp. 193-211). Springer, Cham, 2021.

[6] Sun, W., Yu, S., Lou, W., Hou, Y. T., & Li, H., Protecting your right: Attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud. In IEEE INFOCOM 2014-IEEE conference on computer communications,IEEE, pp. 226-234, 2014.

[7] Guo, C., Zhuang, R., Jie, Y., Ren, Y., Wu, T., & Choo, K. K. R., Fine-grained database field search using attribute-based encryption for e-healthcare clouds. Journal of medical systems, Vol. 40, no.11, pp.1-8, 2021.

[8] Su, H., Zhu, Z., Sun, L., & Pan, N., Practical searchable CP-ABE in cloud storage. In 2016 2nd IEEE International Conference on Computer and Communications (ICCC) IEEE, pp. 180-185, 2016.

[9] McKeeman, W. M., Representation error for real numbers in binary computer arithmetic. IEEE Transactions on Electronic Computers, Vol. 5, pp. 682-683, 1967.

[10] Li, J., Chen, N., & Zhang, Y. (2021). Extended file hierarchy access control scheme with attribute-based encryption in cloud computing. IEEE Transactions on Emerging Topics in Computing, 9(2), 983-993.

[11] Alshehri, S., Radziszowski, S. P., & Raj, R. K., Secure access for healthcare data in the cloud using ciphertext-policy attribute-based encryption. In 2012 IEEE 28th international conference on data engineering workshops IEEE, pp. 143-146, 2021.

[12] Xu, L., Xu, C., Liu, J. K., Zuo, C., & Zhang, P., Building a dynamic searchable encrypted medical database for multi-client. Information Sciences, Vol. 527, pp. 394-405, 2020.

[13] Malinen, I., Sustainable supply chain management in SMEs: A multiple case study of the food industry, 2022.

[14] Cheng, Xu, Fulong Chen, Dong Xie, Hui Sun, and Cheng Huang, "Design of a secure medical data sharing scheme based on blockchain", Journal of medical systems, vol. 44, no. 2, pp. 52, 2020.
[15] Fang, Weidong, Wei Chen, Wuxiong Zhang, Jun Pei, Weiwei Gao, and Guohui Wang, "Digital signature scheme for information non-repudiation in blockchain: a state of the art review", EURASIP Journal on Wireless Communications and Networking, no. 1, pp: 1-15, 2020.
[16] Wazid, Mohammad, Ashok Kumar Das, Sachin Shetty, and Minho Jo. "A tutorial and future research for building a blockchain-based secure communication scheme for internet of intelligent things." IEEE Access, vol. 8, pp: 88700-88716, 2020.
[17] Chen, Yongle, Hui Li, Kejiao Li, and Jiyang Zhang "An improved P2P file system scheme based on IPFS and Blockchain." In 2017 IEEE International Conference on Big Data (Big Data), pp. 2652-2657. IEEE, 2017.
[18] Cui, Zhihua, X. U. E. Fei, Shiqiang Zhang, Xingjuan Cai, Yang Cao, Wensheng Zhang, and Jinjun Chen. "A hybrid blockchain-based identity authentication scheme for multi-WSN." IEEE Transactions on Services Computing, vol. 13, no. 2, pp: 241-251, 2020.