IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁑ Impact Factor 8.102 ⁑ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.124123

Revolutionizing the Insurance Industry: A Blockchain based Claims Management System

Sanket Wakekar[1], Prof. Rupali Meshram[2], Swaranjali Jadhao[3], Vaishnavi Pachpol[4], Vaishnav Umbarkar[5]

Student, Dept. of Computer Science and Engineering, PRMIT&R, Amravati[1,3,4,5]

Assistant Professor, Dept. of Computer Science and Engineering, PRMIT&R, Amravati[2]

Abstract: Low efficiency and complex services are issues in the present medical insurance claims procedure. A patient must visit the hospital to request a diagnosis certificate and receipt before sending the necessary application materials to the insurance provider in order to submit a medical insurance claim. The patient won't get paid until the business has finished verifying everything with the hospital. However, blockchain technology has the potential to make the situation better. The new project is an integrated healthcare system in which all the hospitals and insurance companies will be able to do registration in the system. The patient's health record eg. medical bills, reports, admit cards, etc. will be maintained on blockchain servers in encrypted format and patient will be able to claim the insurance. The insurance company will be able to review all the bills and reports. As all data is maintained on blockchain servers there is no possibility of manipulation in bills and reports hence transparency will be maintained and security of the claims processing will be increased.

Keywords: Blockchain, Medical Insurance, Insurance claim, AES, SHA**.**

I. Introduction

Healthcare data is relevant to everyone. It records physical information about our bodies. It is important for the diagnosis and treatment of diseases [1]. With the rapid development of artificial intelligence, medical data has become a great asset. It can help us build artificial intelligence diagnostic models and assist doctors in diagnosis. Although the recording of medical information has evolved from the initial paper records to electronic medical records (EMR), which are more convenient for data access and storage, more attention needs to be paid to protecting the privacy of data [2]. Many hospitals and institutions have reduced data transfer and sharing in order to avoid data privacy leakage, which has led to the formation of data silos as medical data is scattered among various medical institutions [3]. Health care data privacy and security also lead to other problems. For example, for security, patients need to be re-examined every time they go to a new hospital. This behavior wastes energy and money.

In order to protect patient privacy, medical data cannot be shared with scientific institutions, which prevents medical development. These have prompted the search for secure data storage and transmission methods, and blockchain is widely used, because of its decentralized, tamper-proof nature, for sharing medical data [4]. Innoplexus combines artificial intelligence and blockchain to enable continuous scanning of global life science data [5]. The system provides data to research institutions and pharmaceutical companies. BlockRx is a platform that has been successfully used in real-world applications [6]. Rahman et al. analyze blockchain-based methods for sharing healthcare data, dividing the technologies into three cases in terms of application scenarios: blockchain-based healthcare data storage and access, blockchain and internet of medical things (IOMT) and blockchain-based federal learning [7].

In the system, the use of AES algorithm for blockchain data and documents encryption and SHA algorithm to maintain hash values in blockchain management are done. Two separate blockchain servers and one IPFS (Interplanetary File System) server for document storage and one application server are used.

II. LITERATURE SURVEY

With respect to application scenarios, there are now three types of blockchain use cases for the sharing of medical data. The first is the secure storage and access of data using a blockchain. The second is use of IOMT along with blockchain technology. The third is the use of blockchain to replace the central institution of federal learning.

1. Blockchain based Data Security Storage and Access:

The emergence of EMR has brought convenience as well as privacy issues. Subject to security issues, medical data cannot be shared freely. Some blockchain-based models have been proposed [7]. A blockchain-based 'medichain' model was proposed by Rahul et al. [8]. Medichain model uses the blockchain as a database to store the complete case information of the patient in the block. The transaction records are hashed to store the obtained hash values in the Merkle tree to ensure the security of the data and prevent tampering, thus reducing errors in clinical decision- making. To address the problem of a wide range of sources and diverse structures of medical data, the data of all fields are combined into a single hyperfield stored in the proposed framework. The method uses on-chain storage. However, the blockchain is less scalable. On-chain storage is also expensive. Wu introduces a patient-oriented privacy preserving access control model into the process of access control of private information in healthcare systems [9]. Then, blockchain technology is used to build a private information storage platform, and standard cryptographic algorithms are used to realize information transmission. Hence, the privacy information is also secured by a file authorization contract to further prevent the theft of medical privacy information. The model proposes a fine-grained privacy-preserving access control method that grants different privileges to users by judging their types. EMR information is stored in the cloud database and hosted by a third-party cloud service organization. When data are stored on the cloud, a hash of that data is generated. Then the hash is stored on the blockchain. When the data in the cloud is tampered with, it can be compared by the hash value on the chain. Here, the consensus algorithm is POW, which requires a lot of invalid computations by the nodes. Liu et al. propose a lightweight blockchain-based model for sharing and protecting medical data [10].

The authors of [11] propose a blockchain-smart healthcare-based FL framework. An adaptive differential privacy algorithm is proposed to add an additional security layer to FL. The algorithm adapts the noise according to the training process, balancing privacy and model accuracy. Finally, an efficient consensus protocol based on gradient verification is designed to encourage reliable IoT devices and edge nodes to contribute their data and computational power to federation learning. Blockchain replaces centralized institutions that may be risky. This avoids the situation where a central node is evil, and each transaction is recorded on the chain, which enables timely detection of malicious nodes and provides oversight. Blockchain also has unique economic properties that can motivate nodes to participate in model learning by posting tokens.

2. Traditional Methods Based on Cryptography:

Data encryption is the traditional method of data protection, and a way to protect data privacy using encryption algorithms. Finally, the traditional methods are compared with blockchain-based methods. A lightweight encryption algorithm with a shorter secret key computation time has been proposed by Hasen et al. [12]. The algorithm solves the problem that traditional encryption algorithms are not applicable to medical image data, and the algorithm obtains a lower signal-to-noise ratio. Yang et al. propose the use of a plaintext encryption method, which embeds private data into medical images [13]. The correlation with the original image is intuitively difficult to see in the plaintext encrypted image, which reduces the chance of being attacked. David et al. optimized the traditional homomorphic encryption model [14]. First, edge computing is used to speed up plaintext encryption. Then, avoiding the use of complex centralized encryption algorithms reduces the high computational and communication overhead. There are some problems with the traditional approach. For example, the risk of secret key leakage is greater when there are more organizations to share it with, and traditional cryptographic algorithms have no way to achieve finegrained access control. The blockchain-based approach enables fine-grained access control through smart contracts, and many image data have some distortion after encryption and decryption.

Today, there are many new opportunities for effective management of healthcare data, patient access to data, and provision of necessary medical information. A centralized IT system that stores digital copies of medical records makes sharing them challenging. It takes time to send, receive, and compile patient data, both costly, time-consuming.

In existing system, patient must send all the reports and proofs hard copies to insurance companies for verification but if we are using blockchain there is no need to verify all the reports as patient will not be able to change or delete any uploaded medical record maintained on blockchain server. Hence, we can increase security and maintain transparency in claims processing.

DOI: 10.17148/IJARCCE.2023.124123

A. APPLICATIONS

Table I Significant Applications of Blockchain in Healthcare

S/N	Applications	Description	References
1	Store information of an individual patient	Before and after the different clinical study phases, a significant amount of patient information and health data is generated. There are many people's blood tests, quality assessments, estimates, and wellness polls. It can provide results that show the existence of some document or record. Healthcare providers traverse the stored data and suspect its validity, and they will check this seamlessly by matching it to the original records stored on the Blockchain system. Blockchain is based on existing cryptographic techniques, which include the appropriate framework for cryptography for data sharing. The patient's name, date of birth and diagnosis, treatments, and ambulatory history are recorded in EHR format during patient details by the healthcare provider. This information is stored in cloud computing or the current databases.	[[15], [16]]
2	Analyse the effects of a particular procedure	Researchers can effectively analyse any particular procedure on a large part of the patient population through verified access to the patient data. This produces significant results that enhance the mode of management of these patient groups. With the Blockchain infrastructure in place, pharmaceutical firms will gather data in real-time to deliver a wide range of precisely adapted prescription drugs or services for patients. Blockchain makes the job of the pharmacies simpler since it has all the data on top of it. They will efficiently instruct patients on how to take the medication from these results. It will update the clinicians on the present stage of the patient with the wearable data gathered in real-time and alert them to any emergency.	[17]
3	Validation	Transactions are validated in a Blockchain until they are linked to the chain and are done by algorithms. The authenticity is sealed until the material is encrypted, digitally signed and saved. Healthcare companies, technological innovators, and the healthcare industry are trying to find opportunities to find out what it can do now and what it can do to make healthcare safer and cheaper in the future. Blockchain can make a breakthrough in the health ecosystem when healthcare management can adequately validate the results.	[18]
4	Safety and transparency	It provides excellent safety and transparency while enabling physicians to devote more time to treat patients. It would also allow supporting clinical trials and treatments for any rare disorder. Smooth data exchange among providers of medical solutions can contribute to diagnostic precision, efficient therapies and cost-effective ecosystems in a healthcare system. Blockchain enables various health ecosystem organisations to remain in touch and exchange information on a commonly distributed leader for better safety and transparency. The users can exchange and monitor their data and other actions in the system without searching for more solutions for integrity and confidentiality when using such a system.	[19]

5	Health record keeping	Blockchain can be a perfect technology for record-keeping in the medical world. Its applications include sharing healthcare data, keeping electronic healthcare records, managing insurance, and performing administrative tasks. Patients can send their health information via an app to a Blockchain network. The collaboration of sensors and intelligent devices is facilitated based on digital Blockchain contracts. In most cases, electronic health records are spread through various care institutions. Blockchain will unify all details and provide patients with historical access. The connection of all data in the same place will give us new perspectives on a patient’s health status. Therefore, the Blockchain paradigm would ensure the information is authentic and legitimate and preserve users’ privacy.	[20]

III. PROPOSED SYSTEM

Here, we proposed such a system where an Online Secure Healthcare Web Application is developed where we implement Blockchain Technology for EHR storage, and the document storage is done using encrypting the documents through AES and SHA algorithms. AES algorithm’s security is increased by using bytes reverse scheme. The User needs to register himself by giving the access to data. Hence, all the data will get stored in the form of blocks in blockchain. IPFS (InterPlanetary File System) is used for document storage.

An advanced system using blockchain technology to keep healthcare records transparently and securely on blockchain servers in encrypted format. Users of the applications are hospitals, medical stores and lab attendants, patients, insurance companies. When patient admitted in hospital, hospital users will upload his health records which will be maintained on blockchain server. If patient wants to claim for policy, he will send application with required docs to insurance company. Insurance company will be able to view all the shared docs and approve or decline the claims. Blockchain transactions will be maintained in encrypted format and patient or any other user will not be able to edit those transactions. As the use of blockchain technology is done to maintain all the medical transactions, patient will not be able to do any fraud in bills or other details. Hence the insurance company will get real medical data.

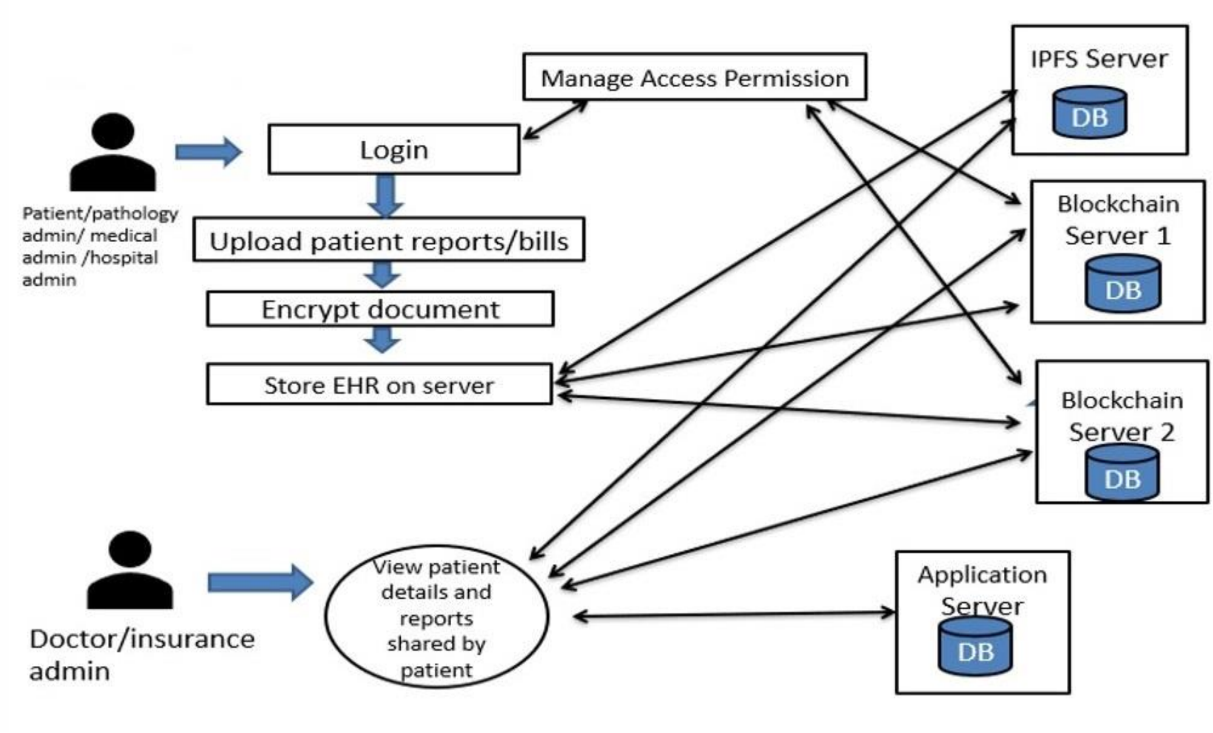

Figure 1. System Architecture

IV. METHODOLOGY

We select the AES technique to encrypt transactions because of its widespread use and excellent efficiency in preventing the leakage of sensitive information. AES method gains the best performance in many use situations, including time consumption, response time, the number of requests processed per second, and battery power consumption, despite the fact that the efficiency of the various algorithms is affected by the difference parameter. The AES technique is therefore appropriate for maintaining a high frequency of transactions and encrypting the certificates.

1. Advanced Encryption Standard

The AES algorithm is a symmetric-key block cipher that uses a fixed block size of 128 bits and key sizes of 128, 192, or 256 bits. It was developed to replace the aging Data Encryption Standard (DES) algorithm and is now widely used for secure communication, data storage, and other applications that require strong encryption.

Key Features:

The AES algorithm has several key features that make it a popular choice for encryption. These include:

Strong security: The AES algorithm uses a complex series of substitution and permutation operations that make it difficult to break the encryption without the correct key.

High efficiency: The AES algorithm is designed to be fast and efficient, making it suitable for use in a wide range of applications.

Scalability: The AES algorithm supports key sizes of 128, 192, or 256 bits, allowing for scalability depending on the needs of the application.

2. Secure Hash Algorithm

The SHA-256 algorithm is a member of the Secure Hash Algorithm family of cryptographic hash functions, and it is widely used to generate fixed-length digital fingerprints of data. It takes an input message of any length and produces a 256-bit hash value, which is unique to that specific input message.

3. Reverse Byte Scheme

For Encryption, Documents are uploaded, the document is read byte by byte then the bytes are reversed and the secret key is generated. At last, Reversed bytes are encrypted using AES algorithm. For Decryption, Documents are decrypted using AES algorithm then the decrypted bytes[] is reversed and then converted into document.

V. CONCLUSION AND FUTURE SCOPE

In this paper, An blockchain based secure EHR sharing and insurance processing system is suggested. The system achieves more transparency, reduces the possibility of frauds, becomes a reliable source to store medical transactions and makes the insurance claim process more transparent using blockchain technology. Our system as compared to previous system achieves same result in less amount of time and attains more security due to implementation of an enhanced version of Advanced Encryption Standard (AES) Algorithm. The usage of bytes reverse scheme in Advanced Encryption Standard Algorithm makes the system achieve an extra layer of security.

In future, the addition of hybrid cryptography and steganography concept for document encryption can be done to increase the security of the EHR documents.

REFERENCES

[1]. Stanfill, M.H.; Marc, D.T. Health Information Management: Implications of Artificial Intelligence on Healthcare Data and Information Management. Yearb. Med. Inform. 2019, 28, 056–064. [CrossRef] [PubMed]

[2]. Adamu, J.; Hamzah, R.; Rosli, M.M. Security issues and framework of electronic medical record: A review. Bull. Electr. Eng. Inform. 2020, 9, 565–572. [CrossRef]

[3]. Enaizan, O.; Zaidan, A.A.; Alwi, N.H.M.; Zaidan, B.B.; Alsalem, M.A.; Albahri, O.S.; Albahri, A.S. Electronic medical record systems: Decision support examination framework for individual, security and privacy concerns using multiperspective analysis. Health Technol. 2020 , 10, 795–822. [CrossRef]

[4]. Agbo, C.C.; Mahmoud, Q.H.; Eklund, J.M. Blockchain Technology in Healthcare: A Systematic Review. Healthcare 2019, 7, 56. [CrossRef]

DOI: 10.17148/IJARCCE.2023.124123

[5]. Paul, S.; Riffat, M.; Yasir, A.; Mahim, M.N.; Sharnali, B.Y.; Naheen, I.T.; Rahman, A.; Kulkarni, A. Industry 4.0 Applications for Medical/Healthcare Services. J. Sens. Actuator Netw. 2020, 10, 25. [CrossRef]

[6]. Hosseini Bamakan, S.M.; Ghasemzadeh Moghaddam, S.; Dehghan Manshadi, S. Blockchain-enabled pharmaceutical cold chain: Applications, key challenges, and future trends. J. Clean. Prod. 2020, 302, 120020. [CrossRef]

[7]. Rahman, M.A.; Hossain, M.S.; Islam, M.S.; Alrajeh, N.A.; Muhammad, G. Secure and Provenance Enhanced Internet of Health Things Framework: A Blockchain Managed Federated Learning Approach. IEEE Access 2020, 8, 205071–205087. [CrossRef]

[8]. Johari, R.; Kumar, V.; Gupta, K.; Vidyarthi, D.P. BLOSOM: Blockchain technology for Security Of Medical records. ICT Express 2022, 8, 56–60. [CrossRef]

[9]. Wu, H.; Dwivedi, A.D.; Srivastava, G. Security and Privacy of Patient Information in Medical Systems Based on Blockchain Technology. ACM Trans. Multimed. Comput. Commun. Appl. 2020, 17, 1–17. [CrossRef]

[10]. Liu, X.; Wang, Z.; Jin, C.; Li, F.; Li, G. A Blockchain-Based Medical Data Sharing and Protection Scheme. IEEE Access 2019, 7, 118925–118953. [CrossRef]

[11]. Chang, Y.; Fang, C.; Sun, W. A Blockchain-Based Federated Learning Method for Smart Healthcare. Comput. Intell. Neurosci. 2021, 2021, 12. [CrossRef]

[12]. Hasan, M.K.; Islam, S.; Sulaiman, R.; Khan, S.; Hashim, A.H.A.; Habib, S.; Islam, M.; Alyahya, S.; Ahmed, M.M.; Kamil, S.; et al. Lightweight Encryption Technique to Enhance Medical Image Security on Internet of Medical Things Applications. IEEE Access 2021, 9, 47731–47724. [CrossRef]

[13]. Yang, Y.; Xiao, X.; Cai, X.; Zhang, W. A Secure and Privacy-Preserving Technique Based on Contrast-Enhancement Reversible Data Hiding and Plaintext Encryption for Medical Images. IEEE Signal Process. Lett. 2020, 27, 256–260. [CrossRef]

[14]. Froelicher, D.; Troncoso-Pastoriza, J.R.; Raisaro, J.L.; Cuendet, M.A.; Sousa, J.S.; Cho, H.; Berger, B.; Fellay, J.; Hubaux, J.P. Truly privacy-preserving federated analytics for precision medicine with multiparty homomorphic encryption. Nat. Commun. 2021, 12, 1–10. [CrossRef] [PubMed]

[15]. M. Ejaz, T. Kumar, I. Kovacevic, M. Ylianttila, E. Harjula Health-BlockEdge: blockchain-edge framework for reliable low-latency digital healthcare applications Sensors, 21 (7) (2021 Jan), p. 2502

[16]. E.J. De Aguiar, B.S. Fai¸cal, B. Krishnamachari, J. Ueyama A survey of blockchain-based strategies for healthcare ACM Comput. Surv., 53 (2) (2020 Mar 13), pp. 1-27

[17]. A. Khatoon A blockchain-based innovative contract system for healthcare management Electronics, 9 (1) (2020 Jan), p. 94

[18]. R. Bhuvana, L.M. Madhushree, P.S. Aithal Blockchain as a disruptive technology in healthcare and financial services-A review based analysis on current implementations International Journal of Applied Engineering and Management Letters (IJAEML), 4 (1) (2020), pp. 142-155

[19]. S. Wang, J. Wang, X. Wang, T. Qiu, Y. Yuan, L. Ouyang, Y. Guo, F.Y. Wang Blockchain-powered parallel healthcare systems based on the ACP approach IEEE Transactions on Computational Social Systems, 5 (4) (2018 Aug 28), pp. 942-950

[20]. D. Berdik, S. Otoum, N. Schmidt, D. Porter, Y. Jararweh A survey on Blockchain for information systems management and security Inf. Process. Manag., 58 (1) (2021 Jan 1), p. 102397