International Journal of Enhanced Research in Management & Computer Applications
ISSN: 2319-7471, Vol. 13, Issue 4, April-2024, Impact Factor: 8.285
Presented at "ICRETETM-2024", Organized by GSMCOE, Pune, on 22nd - 23rd April 2024

Health Care Privacy Approach Using Blockchain Technology

Bhagyashree Jadhav[1], Sakshi Gawali[2], Sanjana Godse[3], Nikita Dhanage[4], Aakanksha Kate[5], Prof. Sangeeta Alagi[6]

Department Computer, Genba Sopanrao Moze College of Engineering, Pune, India.

ABSTRACT

A vast volume of data, produced by many applications in a computer network, is rapidly increasing due to continuous operating states. These apps are producing a large amount of information that is causing problems for processing and analyzing data in a predictable way. The cloud is well-equipped to manage this before the rapid expansion of Big Data. Blockchain technology reduces the need for a central authority to verify the accuracy and ownership of information, as well as facilitate transactions and the transfer of digital assets. It also allows for secure and partially anonymous transactions and agreements between partiesinvolved. This paper elucidates the mechanics of blockchain technology, along with its possible uses and impact on current SCM Registry systems and the role of legal specialists. This study introduces a novel approach using customized blockchain- based smart contracts to empower patients with ownership over their data. The proposed solution ensures decentralization, immutability, transparency, traceability, trustworthiness, and security. The suggested solution utilizes decentralized storage using interplanetary file systems (IPFS) and trusted reputationbased encryption oracles to securely retrieve, store, and exchange medical data of patients. We provide comprehensive algorithms together with their complete implementation information. We assess the suggested smart contracts by considering two crucial performance metrics: cost and accuracy. In addition, we providesecurity analysis and explore the generalization features of our method. A decentralized, traceable, dependable, and secure method that utilizes blockchain technology to empower patients with authority over their medical information.

Keywords: :Blockchain, Smart contracts, PHR (Personal Health Records), healthcare, access control.

INTRODUCTION

Cloud computing, often referred to as fog networking or fogging, is a paradigm that involves moving computer programs, data, and services from a centralized cloud to the network edge. A blockchain system is an exceptionally secure cryptographic database that may be used to store important medical information. The system is maintained by a network of computers that may be accessed by anybody using the program. Blockchain functions as a pseudo-anonymous system that nonetheless has privacy concerns since all transactions are visible to the public, yet being resistant to tampering in terms of data integrity. The design of the access control for diverse healthcare data of patients across numerous health facilities and equipment required meticulous consideration. Blockchain is not specifically intended to function as a storage system on a big scale. In the healthcare sector, using a decentralized storage system would effectively address the limitations of blockchain technology. Examines the practicality of using Blockchain technology in the healthcare industry. A technique for inferring network topology has been presented, and a proof of concept has been shown on an actual network. Blockchain has the potential to replace traditional systems of managing important data, such as contracts, intellectual property rights, and corporate bookkeeping. A blockchain system is an extremely secure cryptographic database that may be used to store important medical information. The decentralized nature of the blockchain network enhances its resilience by eliminating the vulnerability to single-point attacks or failures, which is a characteristic not seen in centralized systems. Personal health records (PHRs) havebeen crucial in facilitating safer, more streamlined, and patient-centered healthcare systems. Personal health records (PHRs)are very beneficial to people since they allow for the integration and management of personal medical data. A Personal Health Record (PHR) is a digital platform that allows people to effectively oversee and control their healthrelated data.

LITERATURE SURVEY

Patients have authority over their medical records thanks to blockchain [1]. Smart contracts based on the Ethereum blockchain allow patients control over their data in a decentralised, immutable, transparent, traceable, trustworthy, and safe way. To securely collect, store, and exchange patients' medical data, the proposed solution uses decentralised storage of interplanetary file systems (IPFS) and trusted reputation-based re-encryption oracles. Algorithms are presented together with complete implementation information. We assess the suggested smart contracts based on two key performance indicators: cost and accuracy. We also explore the generalisation elements of our technique and give security analysis. The suggested approach's drawbacks are outlined. On Github, we make the smart contract source code openly accessible. IPFS [2] provides a blockchain-based secure storage and access solution for electronic medical data. We built an attribute-based encryption scheme for safe storage and efficient exchange of electronic medical records in IPFS storage environment based on the ciphertext policy attribute-based encryption system and IPFS storage environment, paired with blockchain technology. Our method is based on ciphertext policy attribute encryption, which effectively regulates access to electronic medical data while maintaining retrieval efficiency. Meanwhile, we store encrypted electronic medical data in the decentralized Interplanetary File System (IPFS), which not only provides storage platform security but also eliminates the single point of failure concern. Furthermore, we use blockchain technology's non- tamperable and traceable characteristics to enable safe storage and search for medical data. Our approach delivers selective security for pick keyword assaults, according to the security proof. Our approach is efficient and viable, according to performance analysis and actual data set simulation studies. Blockchain technology is being used to handle health records [3]. a patient- centered, entirely decentralized strategy that can detect data theft, prevent data modification, and gives patients control over access. Blockchain technology is the most effective way to solve all issues and meet all demands. As a decentralized and distributed ledger, blockchain has the potential to affect billing, record sharing, medical research, identity theft, and financial data crimes in the future. Smart contracts in health care may help to simplify things even further. On the Blockchain, invocation, record generation, and validation will all take place. on a patient-driven model of record maintenance based on Blockchain technology, with smart contracts to be added in the future, allowing for more data sharing possibilities. Finding its vast reach, I hope that additional study will be conducted and actual applications will be realised. A medical data exchange and protection method based on blockchain[4]. To enhance the hospital's electronic health system, a medical data exchange and protection strategy based on the hospital's private blockchain was developed. For starters, the system may meet a variety of security requirements, including decentralisation, openness, and tamper resistance. Doctors will be able to retain medical data or retrieve patient history data via a secure approach that respects their privacy. A symptom-matching technique is also provided between patients. It enables patients who have the same symptoms to complete mutual authentication and generate a session key for future disease communication. PBC and OpenSSL libraries are used to implement the suggested approach. HealthyBlock is a blockchain-based IT architecture for electronic medical records that is resistant to network outages. [5]. a patient, posing a direct danger to the person and resulting in large public health expenses for governments. The creation of electronic medical record (EMR) systems using blockchain networks is one of the proposed solutions to this problem; however, most of them fail to account for the occurrence of connectivity failures, such as those found in various developing countries, which can lead to data integrity failures. To address these issues, Healthy Block is described in this paper as a blockchainbased architecture that proposes a unified electronic medical record system that takes into account multiple clinical providers, has data integrity resilience during connectivity failure, and has usability, security, and privacy characteristics. A prototype for patient care in a network of hospitals was developed based on the Healthy Block architecture. The evaluation's findings revealed a high level of efficiency in maintaining patients' EMRs unified, updated, and secure, regardless of which network healthcare provider they contact

METHODOLOGY

Methodology The system contains following modules: Hospital: An entity that communicates with the patient to generate a symmetric data to each medical record. An entity that requests medical record locally. Patient: Patients are responsible for registering themselves into the system, deploying their uploading and submitting the medical records, and responding to data queries from doctors (requests to share medical records). Insurance Company: Upload Policy details and show patient history. Distributed Block chain: The Blockchain is the distributed ledger used to represent the current state of delegated access rights in the system. Permissions to interact with the Blockchain are handled by the Root Authority and the Attribute Authorities Algorithms 1: SHA-256 Values Generation Input: The original block, previous-hash, and data d, Output: The hash H was generated based on the provided data's. Step-1: The record is inputted as d. Step-2: Utilize SHA-256 from the hash values range. Step-3: C_Hash= SHA-256(d) Step-4: RetrunC_Hash Algorithms 2: Peer-to-peer (P2P) verification protocols Input: The user receives an IP address and a User Transaction TID. Output:Activate the IP address or current query to determine the validity of any connection. Step 1:The user generates a mysql query using DDL, DML, or DCL. Step 2: Retrieve the present IPaddress. For each (read IP into IP address) If(Assuming that the connection (IP) is true) Flag-true

Else Flag-false End for-each Step 4 : if (Flag.equals(valid)) Peer-to-peer (P2P) verification valid Else Peer-to-peer (P2P) verification Invalid End ifEnd for Algorithms 3: Mining Algorithm for valid hash creation Input: Hash Validation Policy P[], Current Hash Values hash_Val Output: Valid hash Step 1: System generate the hash_Val for ith transaction using Algorithm 1 Step 2: if (hash_Val.valid withP[]) Valid hash Flag =1 Else Flag=0 Mine again randomly Step 3: Return valid hash when flag=1

Table 1: Overview of Existing System

Title	Methodology	Algorithm	Gap Analysis
Blockchain-enabled decentralized identity management: The case of self-sovereign identity in public transportation[6]	A decentralized identity management system based on blockchain technology can leverage the SSI architecture to offer robust securityand transparency for all stakeholderswithin public transportation systems.	Hyperledger Indy blockchain as a proof-of-concept and identity credentials via the SSI framework.	Recognizing the differences between the intended and actual states, such as the need for improved system interoperability, privacy concerns, and a lack of user control.
A peer-to-peer file storage and sharing system based on consortium blockchain [7]	A consortium blockchain- based peer-to- peer storage system with identity access facilitates data validation, cross- organizational data retrieval, trusted authorization, and sharing.	a consortium blockchain-compatible authentication mechanism and Role Based Control	Centralized control, no data integrity assurances, and the requirement for incentive mechanisms between the current systems and the idealstate.
Digital Identity Using Blockchain Technology [8]	A blockchain- based digital identification paradigm that utilizes encryption to guarantee the confidentiality, authenticity, and reliability of personal user data.	Ethereum blockchain and Smart Contract	It is very difficult to verify the level of security offeredby this system
A multi- layer trust framework for Self Sovereign Identity on blockchain [9]	This study a novel multi- layer structure that leverages faith relationships established through the entities involved in the SSI standards, namely the verifiers and issuers of verifiable identifications.	Solidity smart contracts and both private and public blockchain networks	Vulnerable to security and privacy
Fog-enabled private blockchain-based identity authentication scheme for smart home[10]	The authentication process is carried out collaboratively by smart contracts on the local private blockchain and off-chain operations.	fog nodes in smart homes and block chain, smart contracts	These concepts include Proof of Work, Proof of Stake, and Byzantine Fault Tolerance.

PROPOSED SYSTEM

System must validate the previous block before commit block. User can access the data over the internet 24*7. If any block has changed by third party attacker or unauthorized user, it must show during transaction current blockchain is invalid. It

can recover the invalid blockchain using other data nodes, with the help of majority of trustiness. The node or user who wants to initiate a transaction would record and broadcasts the data to the network. The node or user who receives the data verifies the authenticity of the data received in the network. Then the verified data is stored to a block. All nodes or users in the network validate the transaction by executing either the proof of work algorithm or the proof of stake algorithm to the block that needs validation. Consensus algorithm used by the network will store the data to the block that is added to blockchain. And all nodes in the network admit the respective block and extend the chain base on the block.

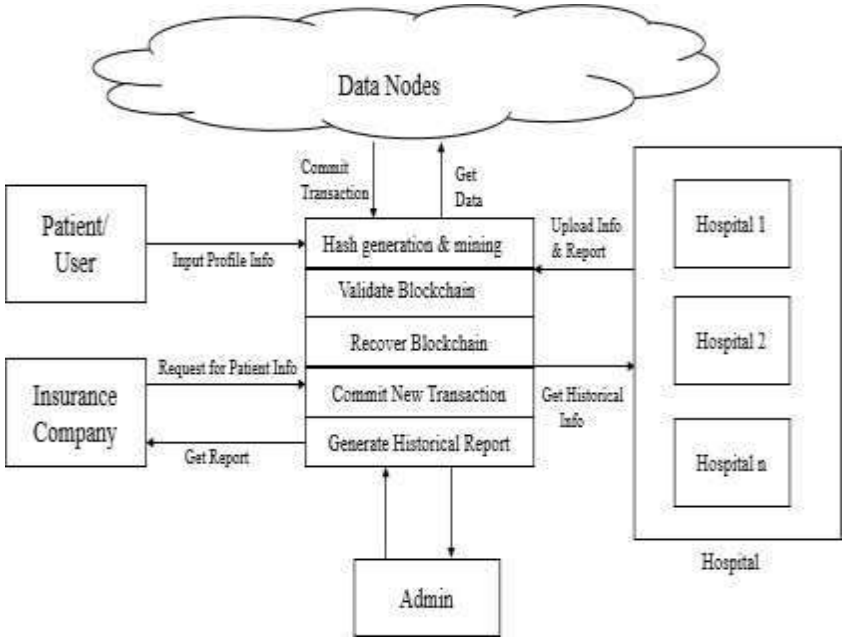

Fig.1: Proposed System Design

RESULT

The time required for the consensus algorithm to validate the blockchain in four nodes is shown in Figure 2. The X axis depicts the size of the blockchain, while the Y axis depicts the time needed in milliseconds for each of the four nodes.

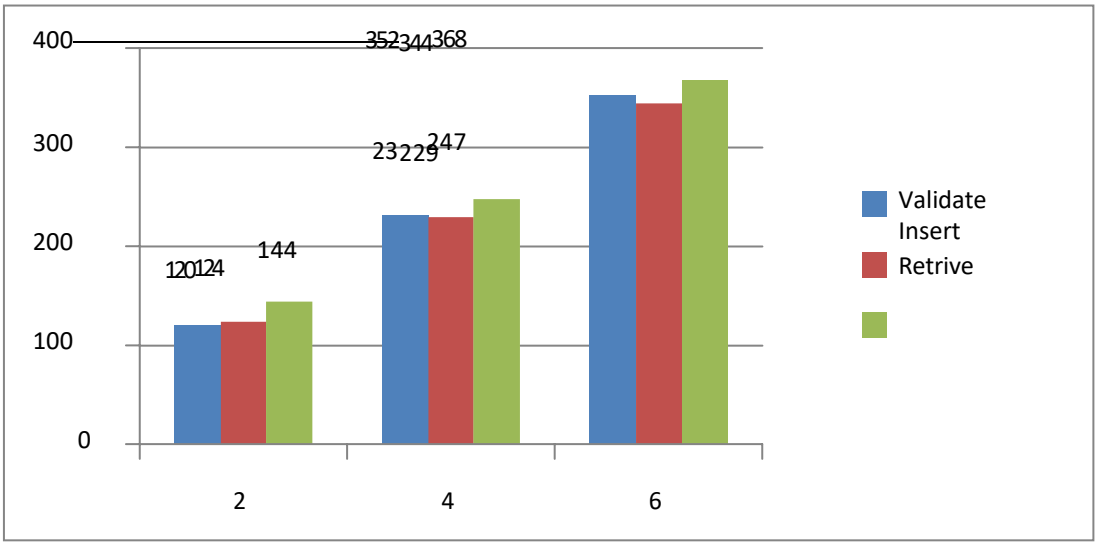

Fig. 2. Time required (in milliseconds) for complete transaction with different records blockchain using 4 datanodes in P2P Network

In the second experiment, we evaluate the proposed system with smart contract validation by consensus algorithm in a different number of peer to peer nodes.

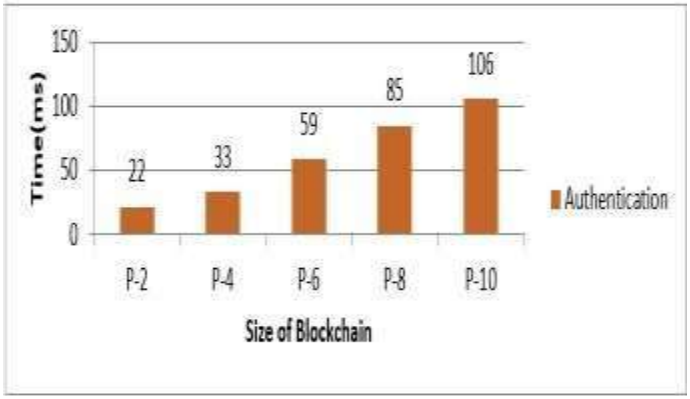

Fig.3: Time required for smart contract validation with different no. of P2P network in the blockchain.

CONCLUSION

There are many research directions in applying Blockchain technology to the healthcare industry due to the complexity of this domain and the need for more robust and effective information technology systems. An interoperable architecture would undoubtedly play a significant role throughout many healthcare use cases that face similar data sharing and communication challenges. From the more technical aspect, much research is needed to pinpoint the most practical design process in creating an interoperable ecosystem using the Blockchain technology while balancing critical security and confidentiality concerns in healthcare. Whether to create a decentralized application leveraging an existing Blockchain, additional research on secure and efficient software practice for applying the Blockchain technology in healthcare is also needed to educate software engineers and domain experts on the potential and also limitations of this new technology. Likewise, validation and testing approaches to gaugethe efficacy of Blockchain-based health care architectures compared to existing systems are also important (e.g., via performance metrics related to time and cost of computations or assessment metrics related to its feasibility). In some cases, a new Blockchain network may be more suitable than the existing Blockchains; therefore, another direction may be investigating extensions of anexisting Blockchain or creating a healthcare Blockchain that exclusively provides health- related services.

REFERENCES

[1]. Madine, Mohammad Moussa, et al. "Blockchain for giving patients control over their medical records." IEEE Access 8(2020): 193102-193115.
[2]. Sun, Jin, et al. "Blockchain-based secure storage and access scheme for electronic medical records in IPFS." IEEE Access8 (2020): 59389-59401.
[3]. Harshini, V. M., et al. "Health record management through blockchain technology." 2019 3rd International Conferenceon Trends in Electronics and Informatics (ICOEI). IEEE, 2019.
[4]. Liu, Xiaoguang, et al. "A blockchain-based medical data sharing and protection scheme." IEEE Access 7 (2019):118943-118953.
[5]. Gutiérrez, Omar, et al. "HealthyBlock: Blockchain- Based IT Architecture for Electronic Medical Records Resilient to Connectivity Failures." International Journal of Environmental Research and Public Health 17.19 (2020): 7132.
[6]. Stockburger, Lukas, et al. "Blockchain-enabled decentralized identity management: The case of self- sovereign identity in public transportation." Blockchain: Research and Applications 2.2 (2021): 100014.
[7]. Peng, Shaoliang, et al. "A peer-to-peer file storage and sharing system based on consortium blockchain." FutureGeneration Computer Systems 141 (2023): 197-204.

[8]. Careja, Alexandru-Cristian, and Nicolae Tapus. "Digital Identity Using Blockchain Technology." Procedia Computer Science 221 (2023): 1074-1082.
[9]. De Salve, Andrea, et al. "A multi-layer trust framework for Self Sovereign Identity on blockchain." Online SocialNetworks and Media 37 (2023): 100265.
[10]. Xu, Xianbin, Yajun Guo, and Yimin Guo. "Fog- enabled private blockchain-based identity authentication scheme for smarthome." Computer Communications 205 (2023):