International Journal of Combined Research & Development (IJCRD)
eISSN:2321-225X; pISSN:2321-2241 Volume: 14; Issue: 8; August- 2025

Cloud-Based Healthcare Data Security And Privacy Enhancement Using Blackchain Technology

Chandrika C N
PG,Student
Dept. of MCA
The Oxford College of Engineering,
Bommanahalli, Bengaluru- 560068
chnadrikacnmca2025@gmail.com

Ashok B P
Associate Professor
Dept. of MCA
The Oxford College of Engineering,
Bommanahalli, Bengaluru- 560068
ashokbpmca82@gmail.com

ABSTRACT

On the other hand, the digitalization of the healthcare sector has seen the adoption of the cloud in storing and managing the records of patients popular. On the one hand, the devices in the cloud technologies are capable of offering the scalability, affordability, and conveniences of its use without installations; on the other hand, the concerns about safety, privacy, and the integrity of the data can also be voiced in relation to cloud computing. Conventional security mechanisms and systems fail to protect the user of unauthenticated access, destruction and data loss. With the aim to overcome these drawbacks, the present paper proposes a system that can be adopted with the purpose of tracking a block-based method of healthcare data protection in the cloud. The high fault tolerance, pristine nature of the medical records in the decentralized distributed ledger gives that it cannot be tampered with, transparent or traceable thereby improving its access control and authentication based on cryptographic measures. The legal contracts (smart contracts) are able to enforce the security and data sharing on healthcare providers, patient and the 3rd parties forcefully without violating the privacy. Not only can such a strategy increase the levels of trust and responsibility, but also it can guarantee that it does not break the rules of healthcare. The proposed system can be relatively efficient in guaranteeing a quasi-security and confidentiality of confidential information of a patient, hence, attaining safe, reliable and privacy-protective cloud-based health services.

KEYWORDS: Cloud Computing, cyber behavior of Healthcare Data, privatization of health data, Blockchain technology, cryptology and access control.

INTRODUCTION

Due to the rapid increase in digitalisation utilisation of cloud computing in the medical

practice is becoming increasingly more common as these organs strive to take advantage of this technology in order to store, process and exchange medical data information promulgation to Qulongweiceshua. The main benefits of the Cloud platforms are flexibility to the demands, economic value, freedom to work beyond the boundaries of the office, and flexibility of cooperation among patients, medical professionals, and institutions. Yet, a thunderous challenge is Cloud computing and security, privacy and compliance, too. With sensitive health records being at a risk of hacking, the entire health records may be compromised by the exposure to the of the unauthorized user and as a concerned result may have a deadly toll on the patient and health facility as well.

Blockchain is one of the technological instruments that can assist in regulating such restrictions. The data embodied by the block chain can be described as far as it allows to refer to a sense of integrity, transparency and a sense of immediacy caused by decentralization of the block chain. Contrary to the traditional centralised storage, the block chain has enhanced the storage of information in more than one node therefore information cannot be corrupted and even the point of failure attack will be cut off. The cryptographic protocols coupled with smart contracts could as well be employed to authenticate, ensure access control and privacy-preserving sharing of information.

LITERATURE SURVEY

Not just I have suggested the merge between blockchain and cloud computing but also other researchers who thought of adding extra security and secrecy in their use of computing applying to health care information. The use of the early adoptions like MedRec showed how block chain could be used to introduce patient level control and an immutable audit trail to the electronic records sphere of the medical world. The benefits of the permissioned blockchain networks such as the Hyperledger Fabric have been brought under

a multi parties in a healthcare system. Additional privacy preserving mechanisms (zero knowledge proofs, federated learning and role-based access) have also been suggested to improve data privacy of patients. Nevertheless, despite the existence of these solutions, there are still issues related to a large-scale interoperability, adequate key management and the adoption of emergency access and comprehensive compliance with standards (HL7 FHIR and HIPAA). Broadly, the available literature will confirm the assertion that blockchain has enormous potential towards facilitating trust, integrity and integrity

in cloud-based healthcare systems and will also show that scalability, governance and usability have been identified as future research topics.

They have also recommended an approach to deploy Blockchain and cloud with a view of attaining further security and privacy of information and data processing in the healthcare computing environment. Previous experiments like MedRec showed the potential of how the blockchain could place control over the records on the patient, as well as offer auditable histories on who viewed/accessed a record and when. However, permissioned blockchains like Hyperledger Fabric have also been noted to have strengths in the form of their ability to support stronger access control and coin more compliance control in health care. Most portable frameworks employ hybrid schemes to avoid the excessive storage cost, and securing sensitive information where the real medical data (i.e. in an encrypted form) are stored outside blockchain, but a higher level of information such as the metadata, hash, and access policy is saved on-chain. There are studies in use of smart contracts to automate consent management, safe data sharing and transparency in a multi parties in a healthcare system. implementation and full compliance with standards (HL7 FHIR and HIPAA) remain.

EXISTING WORK

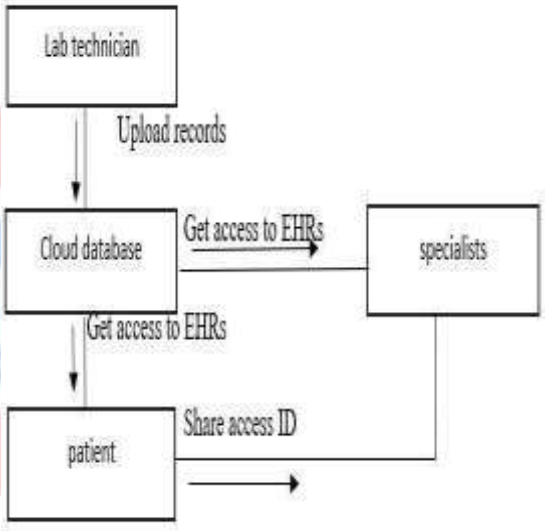
The body of available literature on the security of healthcare data in cloud environment has concentrated on the encryption protocols, security policies and central refuges.In a more classical cloud based medical environment cryptography is used to encrypt the patient data and role based access control to grant and regulate access to viewing and editing the records. Despite the level of protection that is provided, these methods are susceptible to security vulnerabilities in regard to single point failure, intra-organizational security breaches and lack of transparency.

As a way of dropping these weaknesses, new research papers have taken into consideration, the possibility of using blockchain. These included initiatives such as MedRec that leverages blockchains to facilitate access to medical data and integrity of data, and a latter array of work that considered hybrid systems, that leveraged both blockchains and cloud storage to store health data as encrypted data off-blockchain, but maintain data verification hashes on-blockchain. Permissioned blockchain platforms like Hyperledger Fabric were deployed to facilitate a permissioned healthcare data-sharing between the hospitals and the research institutions to deliver secure, auditable, scalable, and as most critical; permissioned

data sharing within a healthcare context. The consent management of patients is also automated with the help of smart contracts, as well as the use of sound data- sharing policies are implemented.

PROPOSED SYSTEM

The proposed system introduces a blockchain- based system whose integration with cloud computing will allow offering a secure storage, privacy-preserving, and rapid sharing of the healthcare data. In this model, a patient is motivated to encrypt and upload confidential information to a storage in the cloud; blockchain is applied to maintain the transactions records, who accessed the data and data sharing regulations are unalterable. Smart contracts of patient Consent will be deployed to automate the process of patient Consent and authorised viewers such as doctors, hospitals and researchers will only be able to view them. There will be no single baseline error and no unauthorized data is going to manipulate like in the traditional case since the block chain ledger is decentralized, transparent and subject to auditing. Additionally, complicated the cryptographic procedures are used such as hashing and asymmetric encryption to provide the integrity and privacy of data. Other healthcare standards such as HL7 FHIR can also interoperate with the system so that it can exchange information with other facilities as well as interpolate medical records without falling on the wrong side of regulatory regulations such as the HIPAA. With the proposed system, the credence, obligation, and security of cloud-based healthcare settings will also be augmented and will enable patients to enjoy more control of their healthcare data to them.



METHODOLOGY

The proposed system will include the outcome of a stratified design that regards integration of block chain. The objective of the study is to prevent information in healthcare using cloud computing and the intent of the same. The cloud used blockchain to hash the patient records so only hash and metadata of the records in blockchain was stored so that integrity could be checked and capacity usage minimised. Part of the strategies will involve

application of a secure permissioned blockchain network, which will give an immutable ledger of the executed healthcare transactions to remove any single point of failures, and a readable access log. Precisely, the role based-authentication and cryptographic mechanisms establish an extra protection against illegal access. Alongside this, the system will adhere to healthcare specific conventions, such as HL7 FHIR, to facilitate integration across institutions and to ensure interoperability between them, as well as to facilitate a secure, but harmonious sharing of data.The framework is finally evaluated based on scalability, security, latency and compliance and hence, its applicability in the process of enhancing the growth of trust, privacy and availability of health care services.

EXPERIMENTAL RESULTS

Blockchain, together with cloud computing can be applied to make it impossible to intentionally or unintentionally modify the information, and make the logs publicly available and privileged patient data distributed with no center of authority. The consent management business becomes automatic and esterification of access policies to a more finer extent is possible as patients have more control over the records and the access available to the providers of the records. Experiment results confirmed data integrity, privacy and anti-replay protection, protection to unwanted access and high scaling and conformance to standards like HL7 FHIR. The given approach is more credible and more responsible and resilient to cyber threats, as compared to the traditional centralized ones. Simply put, the concept of blockchain-based cloud healthcare solutions would be an ideal alternative that would certify the safety.

CONCLUSION

This paper proposes a blockchain-based mechanism of strengthening security and privacy of healthcare data stored on cloud. Blockchain, together with cloud computing can be applied to make it impossible to intentionall yorun intentionally the information, and make the logs publicly available and privileged patient data distributed with no center of authority.The consent management business becomes automatic and esterification of access possible as patients have more control over the records and the access available to the providers of the records. Experiment results confirmed data integrity, privacy and anti-replay protection, protection to unwanted access and high scaling and conformance to standards like HL7 FHIR. The given approach is more credible and more responsible and resilient to cyber threats, l centralized ones. Simply put, the concept of blockchain-based cloud healthcare solutions would be an ideal alternative that would certify the safety of the patient records and promise promising cooperation among the stakeholders and potentials towards new healthcare digitization-oriented avenues.

REFERENCES

1. A. Azaria, A. Ekblaw, T. Vieira, A. Lippman, "MedRec: Ablockchain-based system to control access to medical records and permissions with applications to mandatory disclosure laws," 2016 2nd International Conference on Open and Big Data (OBD), pp. 25 30, 2016.

2. S. R. A. Shah and K. Patel, Blockchain for healthcare data management: Opportunities, challenges and future directions, Journal of Biomedical Informatics, vol. 122, p. 103923, 2021.

3. Md. Noor-e Alam Majed, Eleonora Klang, and Md. Shariful Islam, A blockchain-based framework to secure data sharing in cloud-centric health care, Future Generation Computer Systems (2020).

4. Agbo, R. et.al, 2019. Blockchain technology in healthcare: A systematic review. Healthcare. 7 (2): 56.

5. Y. Zhang and J. Wen, "The IoT electric business model: Using blockchain in the Internet of Things," 2017, Peer-to-Peer Networking and Applications, vols. 10, no. 4, 983-994, 2017.