Investigating how Blockchain can Facilitate Secure Data Sharing Between Different Entities in a Cloud Environment in Healthcare Sector

Jyothsna Sista
Student
Amrita Vishwa Vidyapeetham
Bengaluru, Karnataka, India.

Maria Sabastin Sagayam
Assistant Professor
Amrita Vishwa Vidyapeetham
Bengaluru, Karnataka, India.

Abstract

Introduction: In the healthcare sector, the ability to share data securely and seamlessly among various entities is essential for maintaining continuity of care while complying with strict privacy regulations. Traditional cloud environments, although scalable, encounter issues related to data security, integrity, and interoperability. Blockchain technology, known for its decentralized, immutable, and transparent qualities offers a potential solution to these challenges.

Objective: This research explores how blockchain can enable secure data sharing within a cloud environment specifically for the healthcare sector, with an emphasis on improving data privacy, access control, and accountability among stakeholders such as healthcare providers, patients, and insurance companies. The aim of this study is to evaluate the potential of blockchain in addressing significant security issues while facilitating efficient data sharing within cloud infrastructures.

Methodology: A descriptive method approach is utilized, incorporating a thorough literature review alongside case studies from current healthcare blockchain applications. Furthermore, a conceptual framework is introduced that merges blockchain with cloud-based healthcare systems, ensuring data security, auditability, and adherence to regulations like GDPR and HIPAA.

Conclusion: The study concludes that integrating blockchain with cloud platforms enhances data security, reduces the risks of unauthorized access, and builds trust among entities offering a secure, scalable, and compliant solution for healthcare data sharing.

Keywords

Blockchain, Cloud environment, Healthcare data sharing, Data Security, and Privacy compliance.

1. Introduction

The traditional healthcare paradigm is primarily predicated on the delivery of medical treatment via hospital and outpatient clinic systems. The availability of contemporary equipment, hospital infrastructure, and medical staff training constitute just a few of the many factors that influence the quality of healthcare. The model may vary based on the country. However, the core notions remain the same. It is concerned with the "patient-oriented" strategy and supporting mechanisms that provide the most effective possible access to healthcare services. Due to the population's demand for high-quality medical treatment and the rapid advancement of technology, such a conventional platform has faced considerable challenges in recent decades. Furthermore, emerging digital technologies have the ability to rapidly expand the capabilities of various diagnostic treatment tools and systems.

In reality, medical digital technologies can make healthcare more accessible and flexible for the general public. The internet provides free access to health, treatment, complications, and scientific research information. On the other hand, diagnostics and clinical consulting services are becoming more widely available, particularly in low-income countries. Telemedicine and online pharmacy platforms provide high-quality consultation and guidance to folks in rural and remote places, while also allowing them to obtain necessary prescriptions without traveling.

Another fascinating and rapidly expanding field is applying the artificial intelligence (AI) in biomedicine, healthcare, and medical education. The application of AI in biomedicine, healthcare, and medical education is a rapidly growing topic. AI has the potential to significantly improve diagnostic tools' functionality and performance. Optimizing treatment processes may also be advantageous, leading to improved therapeutic efficacy, happier patients, and reduced expenses.

Clinical trials and biological research may benefit from AI as well. AI will also be essential in sectors that require a lot of manual labor and automation. But even with recent developments, AI cannot fully replace people in biological research and healthcare. (Senbekov et al., 2020)

As healthcare equipment provides appropriate monitoring and patient health records are transferred and collected utilizing cloud computing services, cloud computing, and health monitoring are being used together more and more. These days, the usage of IT resources and services is increasing constantly in all sectors, including stock, education, the military, gaming, agriculture, and healthcare. The IT sector provides services in a more functional and authentic manner than the conventional one. It increases demand for IT-related services (Ali et al., 2018). From a variety of angles, the composition discusses the topic of communicated processing in healthcare administrations.

However, there are a number of security and confidentiality threats that might affect the cloud. Confidentiality and security issues seem to be the biggest obstacles to the development and widespread adoption of something similar to the Cloud. The main issues with cloud-based solutions seem to be privacy and information security. Cloud encryption standards enable openness when using or storing data in the cloud. Because all information in the public cloud is secured, you can use pooled cloud-based services with ease and security. Cloud technology encryption methods protect crucial documents while limiting communication. Compliance is one of the most commonly used techniques to safeguard information systems. Authentication is a policy that enables, denies, or restricts access to resources in a computer system. Furthermore, it detects and reports any attempts to obtain access to a machine. It is a really helpful tool for managing cybersecurity. Finding the best and safest way to transfer user data is therefore another difficult task in the cloud-based environment (Rai et al., 2022).

In this case, Blockchain can be used to transfer or store data in the most secure manner. Blockchain is renowned for connecting and sealing the storage unit "block" using robust encryption to create a structure for data that resembles a chain. An attacker faces a difficult and unprofitable scenario as the chain lengthens because it becomes more difficult to interfere with the data that is happening. In addition, many copies of the data chains, or ledger, are stored locally at various network participants. One modified copy can lead to criticism from others.

The aim of this research is to investigate how blockchain technology enables secure and transparent data sharing among various entities in a cloud-based healthcare environment. The study focuses on how the cryptographic and decentralized characteristics of blockchain can address significant security challenges, including data privacy, integrity, and access control while building trust among healthcare providers, patients, and other stakeholders. Additionally, this research aims to investigate blockchain in integration with existing cloud services to help mitigate risks related to data breaches and unauthorized access in the healthcare industry.

2. Review of the Literature

Blockchain technology, often connected to cryptocurrencies like Bitcoin, is a distributed and decentralized ledger that keeps a record of transactions across a network of computers. It functions without a central authority, which makes it tamper-resistant and ensures that no individual can change the transaction history. Unlike traditional centralized databases, blockchain is supported by the entire network, and verified transactions form an unalterable chain. The core components of blockchain architecture are listed as follows:

- Nodes - Individual devices that maintain a separate copy of the blockchain ledger
- Transaction - A record of data exchange between participants
- Block - A collection of transactions bundled together
- Hash - A unique cryptographic code that represents content in a block
- Consensus mechanism - The protocol by which nodes agree on the validity of transactions
- Wallet - A tool that allows users to perform transactions. It contains a private key and a public key (Monrat, Schelen and Andersson, 2019)

Users initiate transactions through their wallets during the exchange of data or assets. These transactions are collected into a block, which is given a unique hash, that acts like a fingerprint for its contents. The block is then sent out to all nodes in the network. Nodes utilize a consensus mechanism to verify the block and its transactions. Once confirmed, the block is added to the existing chain, linking it to the hash of the previous block. All nodes update their ledger copies with the new block (Komalavalli, Saxena, and Laroiya, 2020). The blockchain's design and cryptographic hashing make it resistant to tampering. This process repeats for every new batch of transactions, allowing the blockchain to grow continuously.

There are three types of blockchain: Public, Private, and Consortium. These systems can be compared using different perspectives such as Consensus determination, Read permission, Immutability, Efficiency, and Centralized platform. Though blockchain can be differentiated based on these factors, all three systems contain similar characteristics such as decentralization, immutability, transparency, security, anonymity, privacy, resilience, programmability, and interoperability. (Vokerla et al., 2019)

Blockchain's transparent and decentralized platform is increasingly appealing to a variety of industries for different business applications. Banks and payment systems are utilizing blockchain to create smoother and more secure operations, enabling efficient fund transfers. In healthcare, blockchain aids in rebuilding trust between patients and providers by simplifying authorization processes and reducing instances of fraud and record loss. The legal sector is utilizing blockchain to securely verify documents, potentially decreasing the likelihood of court disputes (Ali et al., 2021). Additionally, blockchain can improve electoral integrity through transparent voter registration and validation. Sectors such as insurance, education, transportation, and retail are implementing blockchain to lower costs, enhance transparency, and establish trust, with rapid growth expected in banking, government, and pharmaceuticals.

Cloud computing has become an inseparable part of healthcare, offering numerous advantages. Cloud computing in healthcare is largely concerned with deploying remote server access through the Internet to store, manage, and process medical data. This approach provides a customizable alternative for healthcare industry participants to remotely access servers where the data is stored (Narkhede et al., 2020). The remote accessibility of healthcare data breaks down the location barriers to accessing medical services. Cloud computing for healthcare has numerous benefits for both patients and healthcare practitioners, allowing them to use a vast amount of data safely from anywhere, anytime, improve patient care, streamline operations, and automate various processes.

Cloud computing for healthcare has altered the sector by providing high-data accessibility, on-demand availability, and internet-based services. This is why medical professionals who are proficient in technology, are quickly adopting cloud technology in the healthcare industry. The key benefits of cloud computing in healthcare include the real-time availability of resources that can be paid for based on consumption. It allows medical personnel to access a wide range of patient data, exchange the data with key stakeholders, and provide timely protocols (Morais et al., 2022). This boosts collaboration between healthcare stakeholders, providers, and patients.

There are two ways that cloud computing operates in the healthcare sector. By considering the deployment model, there are four types of cloud computing Private (where only one healthcare firm/chain can use the facility), Community (where a group of healthcare bodies can access the cloud), Public (in which the cloud is open for all the stakeholders to access) and Hybrid (which combines multiple clouds with various access options). By considering the distribution model, it can be classified into Saas (Software as a Service - the provider offers IT infrastructure, and the client deploys operating systems and applications), IaaS (Infrastructure as a Service - The provider gives an IT infrastructure and operating system, and the client deploys applications) and PaaS (Platform as a Service - The provider gives an IT infrastructure, an operating system, applications, and every other component in a ready-to-use module). (Qian et al., 2009)

The adoption of healthcare cloud computing requires the storage of medical information in the cloud. However, this increases the likelihood of a data leak. It happens because the isolation methods intended to keep healthcare businesses apart may not work when the data of an organization shares a server with multiple healthcare organizations in a typical cloud architecture. It causes a situation where organizations fail to secure their cloud infrastructure from the growing incidents of cyber attacks. Blockchain acts as a solution to mitigate these kinds of risks caused by cloud computing in the healthcare sector. Since blockchain technology is decentralized, no single entity can be considered an authoritative source of global health data, allowing all parties to have limited access to identical health records. Since data put on the blockchain cannot be altered, recovered, or corrupted, its immutability greatly increases the security of health data stored on it. Every piece of health data on the blockchain is timestamped, encrypted, and added chronologically. Additionally, encrypted keys are used to keep health data on the blockchain, protecting patient privacy and identification (Chauhan and Kumar, 2013). This assures patients that their personal medical information will not be misappropriated by other stakeholders and that there will be a mechanism in place to detect such exploitation. Blockchain's transparent and open nature fosters a sense of confidence surrounding distributed healthcare apps. This improves the acknowledgment of such applications by healthcare stakeholders. The reliability and validity of blockchain records may be confirmed without access to their plaintext. This function is extremely beneficial in healthcare settings that involve record verification, such as pharmaceutical supply chain management and insurance claim processing.

MedRec is a blockchain system designed to manage Electronic Health Records (EHR) and medical research data. Its core objective is to provide access to a patient's medical history and record in a secure, decentralized, and interoperable way across healthcare providers. Traditional EHR systems are often fragmented across various healthcare providers, which hampers patients' ability to access a comprehensive medical history. Additionally, limited interoperability between these systems leads to disjointed medical records. MedRec uses blockchain technology to devise an immutable, transparent log of medical data. It allows the patient to access, share, and control his medical records while maintaining the integrity and security of the data. It uses Ethereum's smart contracts to control access levels regarding who can view a patient's medical record. It only contains pointers to records off-chain in local provider databases for safety and security. Smart contracts automate relationships between patients and providers, logging permissions pertaining to access to any data. MedRec has a decentralized approach with no single point of failure that reduces the possibility of cyberattacks (Ekblaw, 2017). It restores patient agency over health data and provides a robust system for permission-based sharing. It also enhances medical research by providing large datasets with secure access. The system fits the national healthcare priorities, which are also aligned with patient empowerment, interoperability, and precision medicine.

3. Research Methodology

This study adopts a descriptive research methodology that relies exclusively on examining existing literature, academic papers, case studies, and technical reports related to blockchain technology, cloud computing, and the management of healthcare data. The focus is on exploring how blockchain can enable secure data sharing between various entities in a cloud environment within the healthcare sector. It provides an overall and systematic thinking on how blockchain technology might be used to alleviate serious security threats in cloud-based healthcare systems. It is the outcome of reviewing literature and synthesizing it in collecting available literature for the purpose of understanding the overall potential for integration of blockchain within healthcare cloud environments and their limits. The study uses secondary data that accrues from peer-reviewed journal articles, research-based studies on blockchain, cloud computing, and applications in healthcare studied with a view of extracting key findings, technological developments, and use case, relevant conference papers related to blockchain in healthcare or cloud security are reviewed for new developments and emerging trends, case studies or existing implementations of blockchain in healthcare such as MedRec and other cases are reviewed to understand how the practicality of blockchain has been applied in real life to share secure data. This study also used technical white papers on industry reports and information from leading organizations, cryptographic mechanisms, and how they integrate with cloud systems, and official reports on healthcare data security, privacy laws such as HIPAA, and data governance frameworks to understand the compliance and regulatory context of blockchain in healthcare. The actual process of data collection involves systematically searching and retrieving literature from databases such as Google Scholar, IEEE Xplore, PubMed, SpringerLink, and ScienceDirect. The gathering of relevant studies is based on the following keywords and search terms: "blockchain in healthcare, secure data sharing, blockchain cloud integration, healthcare cloud security, and blockchain privacy." Selection criteria involve studies that fall under the categories of both blockchain and cloud computing and healthcare and research studies that are security, privacy, and trust-related issues specific to cloud-based healthcare systems. The data is analyzed by thematic content analysis that involves key themes explored within blockchain security mechanisms, cloud integration, data privacy, and access control, challenges and limitations related to scalability, implementation, interoperability, and complexity in healthcare, and analysis of documented case studies such as Medrec and Modelchain. A conceptual framework, based on the literature review, has thus been developed to show the interaction between blockchain and cloud environments in the healthcare data-sharing context. Although the research is based on secondary data, issues of ethics would actually reflect that sources cited should be authentic and valid. Also, all the literature referred to is quoted appropriately, and due attention is taken to avoid misinterpretation of the findings reported so far. Therefore, this methodology is designed to provide an effective understanding of how blockchain technology can enhance secure data sharing in healthcare cloud environments by analyzing existing research. A systematic literature review and thematic content analysis would serve the study in its aim of unveiling the essential benefits, challenges, and future directions for blockchain adoption in healthcare.

4. Analysis and Findings

Cloud computing services should be always available for health practitioners to support effective functioning and access to patient information. A cloud computing failure might be caused by software, hardware, network failure, cyberattack, or a catastrophe. It does not always provide greater availability as compared with the traditional IT system. Cloud computing services have to ensure data is error-free and reliable since critical health decisions rely on these data. The distributed nature of cloud services is therefore prone to errors, and any software or network failures have to be addressed as soon as possible in order to maintain the reliability of the system. Millions of patient records are stored in e-Health clouds and should be replicated efficiently across several sites with high availability and reliability. That amount of data calls for scalable and fault-tolerant storage systems for securely backing medical applications. Sometimes, cloud computing systems may not accommodate the diverse needs of various healthcare providers. The cloud infrastructure may not be flexible and expandable to quickly meet changing healthcare demands and new services. Data privacy is a major concern in e-Health cloud systems. Patient data must be safeguarded from unauthorized access during data exchange between healthcare providers and cloud services. Ensuring privacy is crucial before fully transitioning to cloud-based healthcare systems. The cloud computing system does pose threats to the confidentiality, trust, and legal liability of data breaches, which could damage reputation and patient trust. Due to its centralized architecture, cloud computing deteriorates greatly in terms of trust and transparency. Currently, cloud providers and customers must rely on trusted third parties to resolve disputes resulting from service-level agreement violations. Cloud computing's essential requirements include accessibility, elasticity, manageability, data security, federated systems, on-demand integration, multi-tenancy, and resource management. Blockchain could help cloud computing developers create novel apps that provide trust, transparency, and more control to cloud customers, as important blockchain capabilities include decentralized governance, immutability, transparency, persistence, auditability, security, and smart contracts.

The interoperability issues in blockchain, which occur when different blockchain networks are unable to communicate and share data with each other as each blockchain is built with different standards and code bases which makes them incompatible, can be attributed to the fact that universal application development standards do not exist. Applications created by different vendors or built on varied platforms are incompatible and hence cannot share medical records seamlessly across systems. This severely affects the end promise of blockchain for healthcare seamless data exchange. In security terms, the threat is susceptible to attacks where any unscrupulous source gets to dictate control over the network by outnumbering honest nodes. Private keys used in accessing blockchain data can also be stolen or lost. Future technologies such as quantum computing will break any encryption method current in the future. What concerns arise regarding healthcare blockchain systems is the transparency-based nature of blockchain technology. While hashing the values may anonymize public addresses, it is likely to identify patients when linking the related data. Malicious attacks from criminal organizations or government entities can also breach the privacy of the patients. Data integrity and patient privacy both are very much needed to be assured for the success of blockchain in managing EMRs. One of the challenges for scalability is due to the large amount of healthcare data and also processing delays inherent in existing blockchain platforms. Blockchain's complexity is sometimes a challenge for its stakeholders. Patients and healthcare providers will not be able to manage healthcare data unless they are sufficiently educated and trained to make use of blockchain; thus, it contradicts the entire concept of empowering patients with control over their data.

The interoperability issue can be solved by developing protocols that make sure the interoperability between blockchain networks exists, and also work on open standards for data storage and transfer. To solve the security challenges, permissioned blockchains like ModelChain can be implemented to present a safer alternative than the public blockchain such as Bitcoin in which only approved nodes are participating. In addition, embedding private pointers to data in the blockchain while actual data will be kept off-chains boosts privacy. Adopting permissioned blockchains along with adherence to secure design principles can be helpful in reducing such privacy risks. One possible solution for scalability issues is the use of blockchain as an index for healthcare data, with the actual data stored off-chain, but this would blow away some of the key strengths of blockchain technology, which are redundancy and availability. To overcome the complexity of data caused by blockchain, simplification of blockchain applications can be done, thereby making them user-friendly, which also encourages a higher adoption rate.

5. Discussions and Conclusion

The incorporation of blockchain and cloud computing presents a valuable opportunity for secured sharing of data in the healthcare industry. The decentralized, immutable, and transparent characteristics of blockchain improve the security and integrity of medical data, tackling the weaknesses found in traditional cloud systems. Research indicates that the cryptographic features of blockchain can effectively protect patient privacy, ensuring that sensitive health information remains safe from unauthorized access and breaches. Furthermore, blockchain promotes trust and transparency among healthcare providers, patients, and stakeholders, leading to a more efficient and secure data-sharing environment.

Nonetheless, the study also points out challenges such as the complexity of blockchain, issues with scalability, and interoperability hurdles between various blockchain networks. To achieve widespread adoption in healthcare, these challenges must be addressed through the creation of open standards, interoperability protocols, and user-friendly blockchain applications. Despite these obstacles, the potential for blockchain to transform cloud-based healthcare services is substantial, providing improved security, transparency, and trust in managing sensitive medical data. Thus, blockchain plays a vital role in reshaping healthcare data sharing, ultimately enhancing patient outcomes and healthcare delivery systems.

6. References

1. Ali, O., Jaradat, A., Kulakli, A., & Abuhalimeh, A. (2021). A Comparative Study: Blockchain Technology Utilization Benefits, Challenges, and Functionalities. *IEEE Access*, *9*(1), 12730–12749.
2. Ali, O., Shrestha, A., Soar, J., & Wamba, S. F. (2018). Cloud Computing-enabled Healthcare Opportunities, Issues, and Applications: A Systematic Review. *International Journal of Information Management*, *43*, 146–158.
3. Chauhan, R., & Kumar, A. (2013). Cloud Computing for Improved Healthcare: Techniques, Potential, and Challenges. *2013 E-Health and Bioengineering Conference (EHB)*.
4. Ekblaw, A. C. (Ariel C. (2017). *MedRec: Blockchain for Medical Data Access, Permission Management, and Trend Analysis*. Dspace.mit.edu.
5. Komalavalli, C., Saxena, D., & Laroiya, C. (2020, January 1). *Chapter 14 - Overview of Blockchain Technology Concepts* (S. Krishnan, V. E. Balas, E. G. Julie, Y. H. Robinson, S. Balaji, & R. Kumar, Eds.). Science Direct; Academic Press.
6. Monrat, A. A., Schelen, O., & Andersson, K. (2019). A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities. *IEEE Access*, *7*(7), 117134–117151.
7. Morais, D., Pinto, F. G., Pires, I. M., Garcia, N. M., & Gouveia, A. J. (2022). The Influence of Cloud Computing on the Healthcare Industry: A Review of Applications, Opportunities, and Challenges for the CIO. *Procedia Computer Science*, *203*, 714–720.
8. Narkhede, B. E., Raut, R. D., Narwane, V. S., & Gardas, B. B. (2020). Cloud Computing in Healthcare - A Vision, Challenges, and Future Directions. *International Journal of Business Information Systems*, *34*(1), 1.
9. Onik, Md. M. H., Aich, S., Yang, J., Kim, C.-S., & Kim, H.-C. (2019, January 1). *Chapter 8 - Blockchain in Healthcare: Challenges and Solutions* (N. Dey, H. Das, B. Naik, & H. S. Behera, Eds.). Science Direct; Academic Press.
10. Qian, L., Luo, Z., Du, Y., & Guo, L. (2009). Cloud Computing: An Overview. *Lecture Notes in Computer Science*, *5931*, 626–631.

11. Rai, V., Bagoria, K., Mehta, K., Vandana Mohindru Sood, Gupta, K., Sharma, L., & Chauhan, M. (2022). Cloud Computing in Healthcare Industries: Opportunities and Challenges. *Springer EBooks*, 695–707.
12. Senbekov, M., Saliev, T., Bukeyeva, Z., Almabayeva, A., Zhanaliyeva, M., Aitenova, N., Toishibekov, Y., & Fakhradiyev, I. (2020). The Recent Progress and Applications of Digital Technologies in Healthcare: A Review. *International Journal of Telemedicine and Applications*, *2020*(1), 1–18.
13. Vokerla, R. R., Shanmugam, B., Azam, S., Karim, A., Boer, F. D., Jonkman, M., & Faisal, F. (2019). An Overview of Blockchain Applications and Attacks. *2019 International Conference on Vision towards Emerging Trends in Communication and Networking (ViTECoN)*.