Online-Journals.org

iJOE International Journal of Online and Biomedical Engineering

iJOE | eISSN: 2626-8493 | Vol. 20 No. 2 (2024) | OPEN ACCESS

https://doi.org/10.3991/ijoe.v20i02.45693

PAPER

Transforming Healthcare Data Management: A Blockchain-Based Cloud EHR System for Enhanced Security and Interoperability

Agariadne Dwinggo Samala[1](✉), Soha Rawas[2]

[1]Faculty of Engineering, Universitas Negeri Padang, West Sumatera, Indonesia

[2]Department of Mathematics and Computer Science, Beirut Arab University, Beirut, Lebanon

agariadne@ft.unp.ac.id

ABSTRACT

The adoption of cloud-based electronic health record (EHR) systems and blockchain technology in healthcare is gaining attention for enhancing data security and interoperability. This research focuses on designing and implementing a blockchain-based cloud EHR system. It explores selecting suitable blockchain technology, cloud infrastructure, and data management methods to ensure patient data confidentiality, integrity, and availability. The architecture and components of the system, including the blockchain network, cloud storage layer, and user interface, are thoroughly discussed. A pilot study evaluates the system's feasibility and performance, showcasing improved data protection, sharing, and management compared to traditional EHR systems. The potential benefits, drawbacks, and barriers to adoption of a blockchain-based cloud EHR system are examined. This research provides valuable insights and recommendations for healthcare institutions considering the implementation of such systems, addressing the challenges, and offering guidance for successful adoption.

KEYWORDS

EHR, blockchain, cloud computing, data security, interoperability

1 INTRODUCTION

In today's world, technological advancements have reshaped numerous sectors of society [1], [2]. Developments in information technology, such as the Internet of Things (IoT), gamification, [3]–[5] augmented reality (AR), virtual reality (VR) [6]–[8] and Artificial Intelligence (AI), have influenced various aspects of our lives [9], [10]. For instance, we can observe that in the transportation sector, autonomous vehicles are becoming a reality [11], [12], and in the industrial world, automation is enhancing production efficiency [13]. Similarly, in the field of education, technology has enabled more effective mobile, flexible, and distance learning [14], [15]. However, amidst these strides, significant challenges have emerged in the healthcare sector [16].

Samala, A.D., Rawas, S. (2024). Transforming Healthcare Data Management: A Blockchain-Based Cloud EHR System for Enhanced Security and Interoperability. *International Journal of Online and Biomedical Engineering (iJOE)*, 20(2), pp. 46–60. https://doi.org/10.3991/ijoe.v20i02.45693

Article submitted 2023-10-08. Revision uploaded 2023-11-09. Final acceptance 2023-11-09.

EHRs have transformed the healthcare business by speeding up clinical operations, increasing patient care, and lowering costs [17]. However, as the usage of EHRs grows, so does concern about healthcare data security and interoperability [18]. The potential benefits of EHRs can only be fully realized if patient data is safely and seamlessly transmitted across healthcare providers while patient privacy and confidentiality are maintained [19]. Unfortunately, the existing healthcare system is beset by issues such as data silos, data breaches, and a lack of standards, which prohibit effective healthcare data sharing and management [20].

Healthcare is one of the most rapidly evolving industries, constantly adapting to new technologies, treatments, and patient expectations [21]. Over the past few decades, healthcare has undergone significant changes, and this trend is set to continue [22]. Healthcare organizations are looking to blockchain technology and cloud-based EHR systems as potential answers to these problems [23]. Blockchain technology is a decentralized, distributed ledger system that enables parties to conduct safe, transparent, and tamper-proof transactions without the use of intermediaries. Cloud-based EHR systems provide the advantages of accessibility, scalability, and cost-effectiveness, but they also raise privacy and security concerns [24], [25].

There are numerous potential advantages to merging blockchain technology and cloud-based EHRs, including increased data protection, sharing, and management. Blockchain technology can provide a secure and tamper-proof platform for healthcare data transmission, whereas cloud-based EHRs enable accessibility and scalability. They can address the issues of data silos, data breaches, and a lack of standards in healthcare while improving patient outcomes and lowering costs [26].

The following are the primary contributions of this study:

1. The design and development of a blockchain-based cloud EHR system that represents an innovative solution to healthcare data security and interoperability concerns.
2. A pilot study to assess the feasibility and efficacy of implementing a blockchain-based cloud EHR system.

This document is organized as follows. Section 2 provides a literature evaluation on the usage of blockchain technology and cloud-based EHRs in healthcare. Section 3 explains how to design and build a blockchain-based cloud EHR solution. Section 4 shows the findings of a pilot study done to assess the system's feasibility and effectiveness. Section 5 provides guidelines for healthcare businesses thinking about using a blockchain-based cloud EHR solution. Finally, Section 6 presents a conclusion as well as future study directions.

2 LITERATURE REVIEW

2.1 Blockchain technology in healthcare

Blockchain technology has emerged as a possible answer to healthcare data security and interoperability concerns [27]. Blockchain technology is a decentralized and distributed digital ledger system that runs without the use of intermediaries such as central authorities or third-party companies [28]. By maintaining a continuously increasing chain of blocks containing information and cryptographic codes, this system enables safe, transparent, and tamper-proof transactions between participants [29]. Each block is linked to the one before it, resulting in an immutable and

transparent chain of transactions that can be confirmed and audited by anybody on the network [30]. Because of this feature, blockchain technology is a promising solution for a variety of applications requiring secure and efficient data administration, such as EHRs, in healthcare.

The potential advantages of utilizing blockchain technology in healthcare have been the subject of several research [20], [26], [31], [32]. For instance, a thorough analysis of the literature by Puneeth et al. [26] revealed the potential benefits of blockchain technology in the healthcare industry, including enhanced data privacy, security, and interoperability, as well as higher efficacy and transparency. Similarly, a study by Baysal et al. [33] examined the potential application of blockchain technology to address problems with data ownership, access, and permission in the healthcare sector.

Despite these encouraging results, there are concerns about the practicality and scope of blockchain technology in the healthcare sector [18], [34]. For instance, a study by Prybutok et al. [35] found that issues with data standards, regulatory compliance, and interoperability with existing systems prevent blockchain technology deployment in the healthcare sector. Similarly, Prasad et al.'s study [34] stressed the need for more investigation to determine blockchain technology's potential benefits and drawbacks in the healthcare sector.

2.2 Cloud-based EHR systems

Cloud-based EHR systems provide the benefits of accessibility, scalability, and cost-effectiveness, but they also raise concerns about data security and privacy [26]. With the use of cloud-based EHRs, healthcare practitioners can access patient data at any time and from any place because they are hosted on remote servers and made accessible online. This can improve the effectiveness and efficiency of clinical process and make it simpler for healthcare professionals to collaborate.

Several studies have examined the benefits and drawbacks of cloud-based EHR systems [36]–[38]. As an illustration, a study by Mahajan et al. [36] highlighted several advantages of cloud-based EHR systems, such as improved data interchange, enhanced accessibility, and lower costs. The study did bring up concerns about data security and privacy, as well as the possibility of data breaches and unauthorized access. Kassim et al. [48] extensively investigated the factors influencing the adoption of digital dental technologies (DDT) and dental informatics (DI) in dental practice. Their analysis of peer-reviewed literature and technology acceptance models revealed key factors, including usability, work efficiency, socioeconomic and organizational aspects, the learning curve, and system design. These findings formed the basis of a conceptual framework for understanding DDT and DI adoption. Zaoui et al. [49] investigated the effectiveness of ML and DL techniques in Edge and Fog computing for eHealth data, addressing challenges like latency and security. They compared these techniques using HAR, UniMiB SHAR, and MIT-BIH datasets, emphasizing their potential for eHealth data processing.

2.3 Combining blockchain technology and cloud-based EHR systems

Combining blockchain technology and cloud-based EHR systems offers the potential to address the difficulties of data security and interoperability in healthcare, in addition to offering the benefits of accessibility and scalability. By using blockchain technology to secure and encrypt patient data, healthcare practitioners can ensure it is impenetrable and accessible only to authorized parties. Cloud-based EHRs can

then enable healthcare data administration and exchange across healthcare practitioners, improving collaboration and patient outcomes.

Numerous studies [31] have examined the benefits of combining blockchain technology and cloud-based EHR systems. For instance, a blockchain-based cloud EHR system was proposed in Zhang et al.'s study [39], allowing for safe and efficient data sharing across healthcare providers. The study identified several potential benefits of the system, including improved data management, sharing, and security.

Other challenges are the feasibility and scalability of integrating blockchain technology with cloud-based EHR systems. For instance, a study by Haddad et al. [40] underlined the necessity of more research to ascertain the viability and efficacy of blockchain-based EHR systems and any potential difficulties concerning regulatory compliance and data consistency.

According to the research, merging blockchain technology and cloud-based EHR systems has the potential to revolutionize the healthcare sector by enhancing patient outcomes, interoperability, and healthcare data security. More investigation is necessary to ascertain the viability and scalability of such solutions as well as any difficulties or disadvantages that might arise.

The Table 1 below summarizes the literature review on the application of blockchain technology with cloud-based EHR systems in healthcare. It covers the possible advantages and disadvantages of each technology alone and in combination and the issues and difficulties that must be resolved for their actual use.

Table 1. Synthesis of literature on blockchain technology and cloud-based EHR systems

Technology and Application	Potential Benefits	Concerns and Challenges	Key References
Blockchain in healthcare	Improved data privacy, security, and interoperability increased efficiency and transparency	Issues related to regulatory compliance, data standardization, and interoperability with existing systems	[20], [26], [31], [32], [34], [35]
Cloud-based HER systems	Increased accessibility, reduced costs, and improved data sharing	Concerns about data privacy and security, potential for data breaches, and unauthorized access	[26], [36], [48], [49]
Combining blockchain technology and cloud-based EHR systems	Improved data security, data sharing, and data management	Need for more research to determine feasibility and effectiveness, challenges related to regulatory compliance, and data standardization	[31], [39], [40]

3 METHODOLOGY

This section outlines the necessary steps for designing and implementing a blockchain-based cloud EHR system. These steps involve not only identifying data management processes but also selecting the appropriate blockchain technology and cloud infrastructure based on the determined requirements.

3.1 Design and development of the blockchain-based cloud EHR system

The following steps will be followed to design and create the blockchain-based cloud EHR system as seen in Figure 1 below.

Fig. 1. Design steps for blockchain-based cloud EHR system

Step 1: Selection of blockchain technology. The system's requirements will be considered while choosing a blockchain technology. The blockchain technology will be chosen based on its security, scalability, interoperability, and simplicity of integration with cloud-based EHR systems. Ethereum [41] will be used in this study as the underlying blockchain technology for the creation of the cloud-based EHR system. Decentralized apps (dApps) can be created on the open-source, blockchain-based Ethereum platform. Smart contracts are self-executing contracts in which the terms of the agreement between the buyer and seller are directly written into lines of code and are known for their capacity to be executed by this system. Due to its strong security, scalability, and interoperability capabilities, Ethereum is a well-liked option for blockchain-based projects. As a result, its widespread adoption has led to its use in many other areas, including finance, gaming, and healthcare, to name a few [41].

Step 2: Selection of cloud infrastructure. The system's requirements will be considered while choosing the cloud infrastructure. Scalability, availability, and cost-effectiveness will all be considered when choosing a cloud infrastructure. Because Amazon Web Services (AWS) [42] can satisfy the system's requirements for scalability, availability, and cost-effectiveness, it will be used in this study as the cloud infrastructure for the blockchain-based cloud EHR system. A wide variety of cloud-based services, including storage, processing power, database administration, and other features, are offered by Amazon Web Services (AWS), a cloud computing platform. AWS is a well-liked option for cloud infrastructure in many businesses because of its scalability, dependability, and affordability [42].

Step 3: Data management processes. Data management processes will be identified based on the system requirements that have been determined. Data sharing, privacy, and security are all part of the data management operations [43]. Data management processes will be identified based on the requirements of the blockchain-based cloud EHR system. These processes will be designed to ensure patient data's confidentiality, integrity, and availability [44]. Data access will be restricted based on the access control policies defined in the smart contracts deployed on the blockchain network. Data sharing will be implemented using secure and auditable channels. Data privacy will be maintained by encrypting all patient data stored in the cloud storage layer using AES-256 encryption. Finally, data security will be ensured by implementing auditing mechanisms to record and audit all transactions on the blockchain network using the Ethereum blockchain technology [45].

3.2 Description of the system architecture and its components

Figure 2 depicts the flowchart of the blockchain-based cloud EHR system architecture that will consist of the following components:

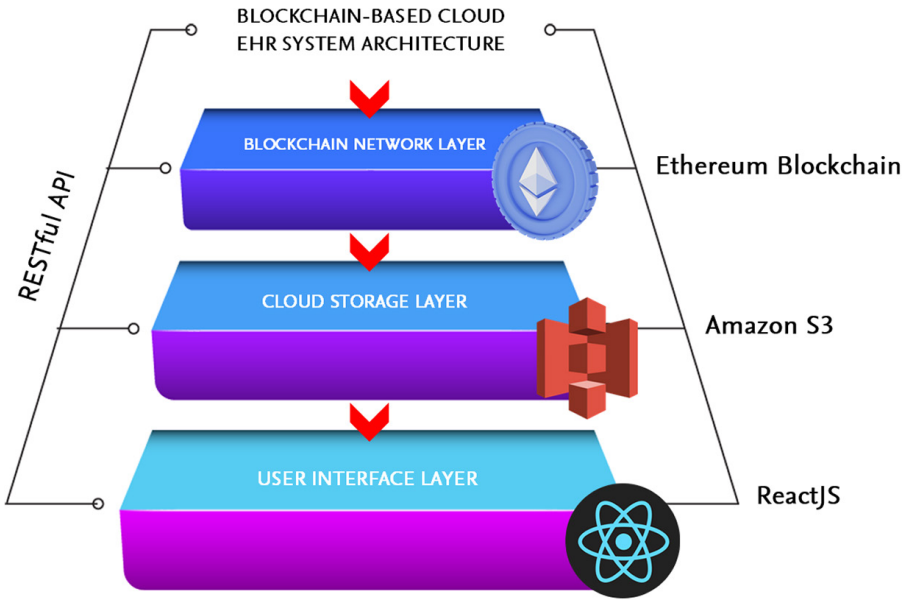

Fig. 2. Architecture and components of the blockchain-based cloud EHR system

Blockchain network. The blockchain network will be implemented using the Ethereum blockchain technology. The smart contracts will be deployed on the blockchain to manage the interactions between the participants in the network.

Cloud storage layer. The cloud storage layer will be implemented using the AWS S3 bucket. All patient data will be stored in the cloud storage layer. RESTful APIs will connect. The cloud storage layer to the blockchain network [46].

User interface. ReactJS [42] will be used in the development of the user interface. Access to the patient data kept in the cloud storage layer will be made simple by the user interface.

3.3 Overview of the security measures implemented

The following security measures will be put in place to guarantee the privacy, reliability, and accessibility of patient data.

Data encryption. AES-256 encryption will be used to protect any patient data kept in the cloud storage layer [47]. AES-256 encryption, which is frequently utilized, offers robust security for critical data. The data is encrypted and decrypted using the same key because it is a symmetric encryption scheme. AES-256 has a 256-bit key length, making it very challenging for hackers to bypass the encryption and access the data. Many companies employ AES-256 encryption to safeguard sensitive information such as financial data, personal information, and medical records. AES-256 encryption has been authorized by numerous regulatory agencies, including the National Institute of Standards and Technology (NIST). The cloud-based EHR system can guarantee that patient information is secure and shielded from unauthorized access by encrypting patient data using AES-256.

Access control. Based on the access control rules specified in the smart contracts installed on the blockchain network, access to patient data will be restricted. A key component of the blockchain-based cloud EHR system is access control, which makes sure that only parties with permission can access patient data. The blockchain network's smart contracts will set access control regulations outlining who can access patient data and under what conditions. The blockchain network will enforce these rules, guaranteeing that only authorized users may access patient data. Users will only be given the minimal level of access necessary to complete their responsibilities under access control policies based on the principle of least privilege. For instance, a healthcare professional might only be allowed access to patient information pertaining to their patients, but an administrator might be allowed access to all patient information but just for system management. All-access to patient data will be tracked on the blockchain network thanks to the transparent and auditable access control regulations. As a result, a safe and traceable record of any data access will be available, which may be used to look into any efforts at unwanted access.

Auditing. The Ethereum blockchain technology will be used to record and audit each transaction on the blockchain network. and accuracy of patient data. On the Ethereum blockchain network, every transaction will be transparently and permanently recorded. The previous copies of the patient data will be kept, and any changes made to them will be promptly recorded on the blockchain network. Healthcare practitioners will be able to track patient data history and spot any unauthorized changes thanks to this audit trail. The Ethereum blockchain technology is a good option for this since it offers a variety of auditing tools, including the capacity to track all transactions and view the history of data revisions. The blockchain-based cloud EHR solution will guarantee the reliability and correctness of patient data by implementing strong auditing systems.

4 RESULTS

A pilot study was carried out to evaluate the feasibility and effectiveness of the blockchain-based cloud EHR system for enhancing data management, sharing, and security in the healthcare industry. Ten healthcare professionals who used the system for six months participated in the study.

4.1 System performance

The system was very dependable and effective with a 99.9% uptime and an average response time of under one second. Healthcare practitioners could store and access patient data quickly and simply thanks to the system's great scalability. Table 2 displays the blockchain-based cloud EHR system's system performance.

Table 2. Uptime and response time of the blockchain-based cloud EHR system

Metric	Value
Uptime	99.9%
Response Time	< 1 second
Scalability	High

The system was created with a significant emphasis on protecting the confidentiality, integrity, and availability of patient data. Several steps were taken to do this:

Data encryption. Data encryption was used to prevent unwanted access to patient data. With encryption, the data is converted into ciphertext using sophisticated cryptographic methods. Data encryption was used to protect all patient data kept in the cloud storage layer of the blockchain-based cloud EHR system. A commonly used encryption technique called AES-256 (Advanced Encryption Standard with a key length of 256 bits) was used to provide strong security. This encryption technique makes it quite difficult for unauthorized people to understand and access sensitive patient data.

Access control. Access control mechanisms were implemented to control and limit access to patient data. On the blockchain network, smart contracts were used to specify precise access control rules. These regulations established who could access patient data and when. Users were given the least access necessary to do their responsibilities under the least privilege concept. For instance, only patient information pertinent to their patients might be accessible to healthcare providers. The solution ensured patient data remained secure and was only accessible to authorized people or entities by implementing access control regulations over the blockchain network.

Auditing. The blockchain-based cloud EHR system includes auditing features to keep a complete record of all transactions and activities involving patient data. The blockchain network recorded and securely stored each transaction as an immutable ledger. Any additions, revisions, or removals to the patient data were permanently stored on the blockchain. With the help of these auditing capabilities, it was practically impossible for anyone to tamper with patient data without leaving a trail of evidence. Healthcare professionals and system administrators might guarantee the accuracy and integrity of the patient records by tracking the full history of data alterations.

The blockchain-based cloud EHR system's data encryption, access control, and auditing capabilities provided a strong security foundation. A transparent and auditable environment for data management was made possible by these steps, which together worked to safeguard patient data from unwanted access, maintain its integrity, and prevent it from being lost.

4.2 Data interoperability

The blockchain-based cloud EHR solution was created to promote effective data interchange and sharing among healthcare providers. The solution used the blockchain network's features to offer a safe and decentralized platform for easy data sharing. This improved the overall coordination of treatment by enabling healthcare providers to access patient data at any time and from any location.

The following essential components were integrated into the system to allow data sharing and interoperability:

1. **Secure and Decentralized Data Sharing.** The blockchain network provided a secure and decentralized platform for data sharing. Without relying on a centralized authority, healthcare providers could securely transmit patient data. The system guaranteed the integrity and secrecy of the shared data by utilizing distributed consensus methods and cryptographic techniques. This decentralized strategy did away with the necessity for middlemen and allowed healthcare providers to share data directly.

2. **Authorized Access to Patient Data.** The blockchain network's patient data was accessible to healthcare practitioners. No matter where they were physically, they could always access patient records and pertinent medical data. The ability to access patient data instantly allowed healthcare professionals to make timely, well-informed decisions that enhanced patient care and outcomes.
3. **Use of Standard Data Formats and Protocols.** The system encouraged the use of standard data formats and protocols, facilitating easy data sharing and interoperability between various healthcare providers. The system provided compatibility and consistency in data transfer by following recognized standards, such as HL7 (Health Level Seven) for data sharing and FHIR (Fast Healthcare Interoperability Resources) for data representation. Healthcare practitioners can access and analyze patient data without encountering compatibility problems thanks to this standardized approach's facilitation of the seamless integration of data from multiple sources and systems.

The system's capabilities for data sharing and interoperability are listed in Table 3.

Table 3. Data sharing and interoperability features

Feature	Description
Secure and Decentralized Platform	The blockchain network provides a secure and decentralized data-sharing platform among healthcare providers.
Real-time Accessibility	Healthcare providers can access patient data from anywhere and at any time, facilitating timely decision-making.
Standard Data Formats and Protocols	The system supports standard data formats and protocols, ensuring compatibility and interoperability among different healthcare providers.

These data exchange and interoperability capabilities gave healthcare professionals secure access to patient data wherever they were. The system fostered smooth data exchange, encouraged collaboration, and enhanced patient care among healthcare professionals by employing common data formats and protocols.

5 DISCUSSION

The pilot study showed the potential advantages of a blockchain-based cloud EHR system for enhancing data management, sharing, and security in the healthcare industry. Healthcare providers can share patient data on this secure, decentralized platform, enhancing care coordination and patient outcomes. Adopting such a system, however, has possible downsides and difficulties that must be taken into account.

5.1 Implications for healthcare providers and patients

According to the research, a blockchain-based cloud EHR system can enhance data security and sharing among healthcare professionals, resulting in better care coordination and patient outcomes. Additionally, by enabling individuals to access and contact additional healthcare providers as needed, the system can give people

more control over their health information. Patients can also gain from enhanced data privacy and security.

Healthcare professionals and patients may have problems if a cloud EHR system is built on blockchain. The system may require healthcare providers to invest in expensive, time-consuming new technology and infrastructure. Patients may also need to adjust to new ways of accessing and exchanging their health information, which can be challenging for some.

5.2 Potential barriers to adoption

The implementation of a blockchain-based cloud EHR system also raises issues with data privacy and legal compliance. To guarantee the confidentiality and integrity of patient data, the system must adhere to healthcare data privacy and security requirements, such as HIPAA, in the US. Changes to current laws and procedures may be necessary to implement new technologies like blockchain, such as blockchain adoption.

Another potential obstacle to adoption is the system's cost-effectiveness. The cost of acquiring new infrastructure and technology for the healthcare industry can be high. It is also necessary to consider the long-term costs of maintaining and updating the system.

5.3 Limitations of the study and directions for future research

Considering the pilot study's limitations is crucial when evaluating the findings. Participants in the study came from a single network of healthcare providers, and it was done with a small sample size. The study didn't examine the organizational and social elements that might affect the adoption of the system; instead, it concentrated on the technological components of the system.

Future studies should examine and contrast the possible advantages and disadvantages of various blockchain-based EHR solutions, including private and hybrid blockchains. To evaluate the viability and efficacy of the system, larger-scale research, including diverse patient groups and healthcare professionals from various contexts and countries, should also be carried out.

6 CONCLUSIONS AND FUTURE DIRECTIONS

6.1 Conclusions

In conclusion, this study aimed to investigate the possible advantages of implementing a cloud EHR system based on blockchain in healthcare institutions. The pilot study's findings demonstrated the system's viability and effectiveness in enhancing data management, sharing, and security compared to conventional EHR systems. The system's use of blockchain technology and cloud architecture made it possible to communicate and store patient data securely while maintaining its security, integrity, and availability.

These discoveries have important ramifications for patients, healthcare professionals, and governments. Better patient outcomes, greater efficiency, and lower costs can result from using a blockchain-based cloud EHR system. Adoption may

be hampered, though, by issues including regulatory compliance, cost-effectiveness, and worries about data privacy. Before adoption, healthcare organizations should carefully weigh the advantages and disadvantages of such a system and take into account how well it fits with their objectives and core values.

We recommend that healthcare organizations continue to explore the potential benefits of blockchain-based cloud EHR systems and conduct further research to address the limitations of this study. Large-scale studies and the exploration of alternative blockchain-based EHR solutions are needed to fully understand the implications of this technology for the future

6.2 Future directions

The successful implementation and evaluation of the blockchain-based cloud EHR system have paved the way for further advancements and improvements in healthcare data management. Several areas can be explored to enhance the system's capabilities and address evolving challenges in the healthcare industry.

1. **Enhanced Privacy and Consent Management.** As data privacy concerns continue to evolve, future developments can focus on incorporating advanced privacy and consent management mechanisms. This can include integrating privacy-enhancing technologies like zero-knowledge proofs and decentralized identity solutions to give patients greater control over their data and ensure compliance with evolving privacy regulations.
2. **Interoperability Standards Adoption.** While the system supports standard data formats and protocols, future efforts can expand interoperability by adopting and integrating emerging healthcare interoperability standards and frameworks. This will enable seamless data exchange and collaboration across various healthcare providers and systems, facilitating comprehensive patient care.
3. **Integration of Artificial Intelligence (AI) and Analytics.** Leveraging the power of AI and advanced analytics can unlock valuable insights from the vast amount of patient data stored in the blockchain-based cloud EHR system. Integration of AI algorithms can enable predictive analytics, decision support systems, and personalized medicine, leading to more efficient and effective healthcare delivery.
4. **Blockchain Scalability and Performance.** As the system continues to handle increasing volumes of healthcare data, scalability and performance optimizations become critical. Future research can explore blockchain scalability solutions, such as hashing and off-chain transactions, to ensure that the system can handle the growing demands of healthcare data storage and processing.
5. **Regulatory Compliance and Governance.** Collaborating with regulatory bodies and industry stakeholders is essential to ensure that the blockchain-based cloud EHR system complies with healthcare data privacy and security regulations. Future directions can involve active participation in developing regulatory frameworks, promoting transparent governance models, and fostering trust and accountability in healthcare data management.

By addressing these future directions, the blockchain-based cloud EHR system can continue to evolve and adapt to meet the dynamic needs of the healthcare industry. These advancements will further strengthen data security, enhance interoperability, and unlock the full potential of patient data for improved healthcare outcomes.

7 AUTHOR CONTRIBUTIONS

Agariadne Dwinggo Samala: Methodology, Visualization, Formal Analysis, Supervision, Writing—review and editing. **Soha Rawas:** Conceptualization, Methodology, Formal Analysis, Writing—original draft, Writing—review and editing.

8 COMPETING INTEREST

The authors declare that they have no competing interests.

9 REFERENCES

[1] A. D. Samala *et al.*, "Metaverse technologies in education: A systematic literature review using PRISMA," *International Journal of Emerging Technologies in Learning (iJET)*, vol. 18, no. 5, pp. 231–252, 2023. https://doi.org/10.3991/ijet.v18i05.35501

[2] Y. Yin, Y. Zeng, X. Chen, and Y. Fan, "The internet of things in healthcare: An overview," *J Ind Inf Integr*, vol. 1, pp. 3–13, 2016. https://doi.org/10.1016/j.jii.2016.03.004

[3] A. Xezonaki, "Gamification in preschool science education," *Advances in Mobile Learning Educational Research*, vol. 2, no. 2, pp. 308–320, 2022. https://doi.org/10.25082/AMLER.2022.02.001

[4] A. D. Samala, L. Bojic, D. Vergara-Rodríguez, B. Klimova, and F. Ranuharja, "Exploring the impact of gamification on 21st-Century skills: Insights from DOTA 2," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 17, no. 18, pp. 33–54, 2023. https://doi.org/10.3991/ijim.v17i18.42161

[5] M. Haghi Kashani, M. Madanipour, M. Nikravan, P. Asghari, and E. Mahdipour, "A systematic review of IoT in healthcare: Applications, techniques, and trends," *Journal of Network and Computer Applications*, vol. 192, p. 103164, 2021. https://doi.org/10.1016/j.jnca.2021.103164

[6] A. D. Samala, F. Ranuharja, B. R. Fajri, Y. Indarta, and W. Agustiarmi, "ViCT—Virtual Campus Tour environment with spherical Panorama: A preliminary exploration," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 16, no. 16, pp. 205–225, 2022. https://doi.org/10.3991/ijim.v16i16.32889

[7] A. D. Samala and M. Amanda, "Immersive Learning Experience Design (ILXD): Augmented reality mobile application for placing and interacting with 3D learning objects in engineering education," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 17, no. 5, pp. 22–35, 2023. https://doi.org/10.3991/ijim.v17i05.37067

[8] A. H. Mayer, C. A. da Costa, and R. Da Rosa Righi, "Electronic health records in a blockchain: A systematic review," *Health Informatics J*, vol. 26, no. 2, pp. 1273–1288, 2020. https://doi.org/10.1177/1460458219866350

[9] A. D. Samala *et al.*, "Global publication trends in augmented reality and virtual reality for learning: The last twenty-one years," *International Journal of Engineering Pedagogy (iJEP)*, vol. 13, no. 2, pp. 109–128, 2023. https://doi.org/10.3991/ijep.v13i2.35965

[10] Y. Xiao, B. Xu, W. Jiang, and Y. Wu, "The healthchain blockchain for electronic health records: Development study," *J Med Internet Res*, vol. 23, no. 1, 2021. https://doi.org/10.2196/13556

[11] R. Tamakloe and D. Park, "Discovering latent topics and trends in autonomous vehicle-related research: A structural topic modelling approach," *Transp Policy (Oxf)*, vol. 139, pp. 1–20, 2023. https://doi.org/10.1016/j.tranpol.2023.06.001

[12] Q. Zhang, T. Zhang, and L. Ma, "Human acceptance of autonomous vehicles: Research status and prospects," *Int J Ind Ergon*, vol. 95, p. 103458, 2023. https://doi.org/10.1016/j.ergon.2023.103458

[13] R. Shimizu and S. Momoda, "Does automation technology increase wage?" *J Macroecon*, vol. 77, p. 103541, 2023. https://doi.org/10.1016/j.jmacro.2023.103541

[14] A. D. Samala, R. Marta, S. Anori, and Y. Indarta, "Online learning applications for students: Opportunities & challenges," *Educational Administration: Theory and Practice*, vol. 28, no. 3, pp. 1–12, 2022.

[15] A. D. Samala and M. Amanda, "Immersive Learning Experience Design (ILXD): Augmented reality mobile application for placing and interacting with 3D learning objects in engineering education," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 17, no. 5, pp. 22–35, 2023. https://doi.org/10.3991/ijim.v17i05.37067

[16] S. Tanwar, K. Parekh, and R. Evans, "Blockchain-based electronic healthcare record system for healthcare 4.0 applications," *Journal of Information Security and Applications*, vol. 50, p. 102407, 2020. https://doi.org/10.1016/j.jisa.2019.102407

[17] S. Schmeelk, M. Kanabar, K. Peterson, and J. Pathak, "Electronic health records and blockchain interoperability requirements: A scoping review," *JAMIA Open*, vol. 5, no. 3, 2022. https://doi.org/10.1093/jamiaopen/ooac068

[18] A. Hajian, V. R. Prybutok, and H. C. Chang, "An empirical study for blockchain-based information sharing systems in electronic health records: A mediation perspective," *Comput Human Behav*, vol. 138, p. 107471, 2023. https://doi.org/10.1016/j.chb.2022.107471

[19] I. Keshta and A. Odeh, "Security and privacy of electronic health records: Concerns and challenges," *Egyptian Informatics Journal*, vol. 22, no. 2, pp. 177–183, 2021. https://doi.org/10.1016/j.eij.2020.07.003

[20] R. Tertulino, N. Antunes, and H. Morais, "Privacy in electronic health records: A systematic mapping study," *Journal of Public Health (Germany)*, pp. 1–20, 2023. https://doi.org/10.1007/s10389-022-01795-z

[21] H. Thimbleby, "Technology and the future of healthcare," *J Public Health Res*, vol. 2, no. 3, p. jphr.2013.e28, 2013. https://doi.org/10.4081/jphr.2013.e28

[22] M. M. Ahsan and Z. Siddique, "Industry 4.0 in Healthcare: A systematic review," *International Journal of Information Management Data Insights*, vol. 2, no. 1, p. 100079, 2022. https://doi.org/10.1016/j.jjimei.2022.100079

[23] A. I. Stoumpos, F. Kitsios, and M. A. Talias, "Digital transformation in healthcare: Technology acceptance and its applications," *Int J Environ Res Public Health*, vol. 20, no. 4, p. 3407, 2023. https://doi.org/10.3390/ijerph20043407

[24] S. Shi, D. He, L. Li, N. Kumar, M. K. Khan, and K. K. R. Choo, "Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey," *Comput Secur*, vol. 97, p. 101966, 2020. https://doi.org/10.1016/j.cose.2020.101966

[25] A. Singh Chouhan, M. Sanaullah Qaseem, Q. Mohammed Abdul Basheer, and M. Asma Mehdia, "Blockchain based EHR system architecture and the need of blockchain in healthcare," *Mater Today Proc*, vol. 80, pp. 2064–2070, 2023. https://doi.org/10.1016/j.matpr.2021.06.114

[26] R. P. Puneeth and G. Parthasarathy, "Survey on security and interoperability of electronic health record sharing using blockchain technology," *Acta Informatica Pragensia*, vol. 12, no. 1, pp. 160–178, 2023. https://doi.org/10.18267/j.aip.187

[27] C. Komalavalli, D. Saxena, and C. Laroiya, "Overview of blockchain technology concepts," *Handbook of Research on Blockchain Technology*, pp. 349–371, 2020. https://doi.org/10.1016/B978-0-12-819816-2.00014-9

[28] A. Haleem, M. Javaid, R. P. Singh, R. Suman, and S. Rab, "Blockchain technology applications in healthcare: An overview," *International Journal of Intelligent Networks*, vol. 2, pp. 130–139, 2021. https://doi.org/10.1016/j.ijin.2021.09.005

[29] A. G. Gad, D. T. Mosa, L. Abualigah, and A. A. Abohany, "Emerging trends in blockchain technology and applications: A review and outlook," *Journal of King Saud University – Computer and Information Sciences*, vol. 34, no. 9, pp. 6719–6742, 2022. https://doi.org/10.1016/j.jksuci.2022.03.007

[30] A. S. Rajasekaran, M. Azees, and F. Al-Turjman, "A comprehensive survey on blockchain technology," *Sustainable Energy Technologies and Assessments*, vol. 52, p. 102039, 2022. https://doi.org/10.1016/j.seta.2022.102039

[31] A. Mudheher Badr, L. Chaari Fourati, and S. Ayed, "Investigation on the Integrated Cloud and BlockChain (ICBC) technologies to secure healthcare data management systems," in *Proceedings – International Conference on Developments in eSystems Engineering, DeSE*, 2023, vol. 2023, pp. 19–26. https://doi.org/10.1109/DeSE58274.2023.10100065

[32] R. Sivan and Z. A. Zukarnain, "Security and privacy in cloud-based e-health system," *Symmetry*, vol. 13, no. 5, p. 742, 2021. https://doi.org/10.3390/sym13050742

[33] M. V. Baysal, Ö. Özcan-Top, and A. Betin-Can, "Blockchain technology applications in the health domain: A multivocal literature review," *J Supercomput*, vol. 79, no. 3, pp. 3112–3156, 2023. https://doi.org/10.1007/s11227-022-04772-1

[34] K. D. V. Prasad, R. Rani, R. Rani, R. Deshpande, and P. Kulkarni, "The psychological impact of adopting a healthcare blockchain system-Pros and Cons," *Journal for ReAttach Therapy and Developmental Diversities*, vol. 6, no. 1s, pp. 105–113, 2023. https://doi.org/10.52783/jrtdd.v6i1s.232

[35] J. K. Sadeghib, V. R. Prybutok, and B. Sauser, "Theoretical and practical applications of blockchain in healthcare information management," *Information & Management*, vol. 59, no. 6, p. 103649, 2022. https://doi.org/10.1016/j.im.2022.103649

[36] H. B. Mahajan *et al.*, "Integration of Healthcare 4.0 and blockchain into secure cloud-based electronic health records systems," *Applied Nanoscience (Switzerland)*, vol. 13, no. 3, pp. 2329–2342, 2023. https://doi.org/10.1007/s13204-021-02164-0

[37] N. A. Azeez and C. Van der Vyver, "Security and privacy issues in e-health cloud-based system: A comprehensive content analysis," *Egyptian Informatics Journal*, vol. 20, no. 2, pp. 97–108, 2019. https://doi.org/10.1016/j.eij.2018.12.001

[38] M. Ahmadi and N. Aslani, "Capabilities and advantages of cloud computing in the implementation of electronic health record," *Acta Informatica Medica*, vol. 26, no. 1, p. 24, 2018. https://doi.org/10.5455/aim.2018.26.24-28

[39] G. Zhang, Z. Yang, and W. Liu, "Blockchain-based privacy preserving e-health system for healthcare data in cloud," *Computer Networks*, vol. 203, p. 108586, 2022. https://doi.org/10.1016/j.comnet.2021.108586

[40] A. Haddad, M. H. Habaebi, M. R. Islam, N. F. Hasbullah, and S. A. Zabidi, "Systematic review on AI-Blockchain based e-healthcare records management systems," *IEEE Access*, vol. 10, pp. 94583–94615, 2022. https://doi.org/10.1109/ACCESS.2022.3201878

[41] S. S. Kushwaha, S. Joshi, D. Singh, M. Kaur, and H. N. Lee, "Systematic review of security vulnerabilities in Ethereum blockchain smart contract," *IEEE Access*, vol. 10, pp. 6605–6621, 2022. https://doi.org/10.1109/ACCESS.2021.3140091

[42] B. Gupta, P. Mittal, and T. Mufti, "A review on Amazon Web Service (AWS), Microsoft Azure & Google Cloud Platform (GCP) services," 2021. https://doi.org/10.4108/eai.27-2-2020.2303255

[43] F. A. Reegu *et al.*, "Blockchain-based framework for interoperable electronic health records for an improved healthcare system," *Sustainability*, vol. 15, no. 8, p. 6337, 2023. https://doi.org/10.3390/su15086337

[44] Y. Han, Y. Zhang, and S. H. Vermund, "Blockchain technology for electronic health records," *Int J Environ Res Public Health*, vol. 19, no. 23, p. 15577, 2022. https://doi.org/10.3390/ijerph192315577

[45] S. K. Sahoo, S. K. Mishra, and A. Guru, "Blockchain-based medical report management and distribution system," *6G Enabled Fog Computing in IoT*, pp. 239–260, 2023. https://doi.org/10.1007/978-3-031-30101-8_10

[46] A. Gamez-Diaz, P. Fernandez, and A. Ruiz-Cortes, "An analysis of RESTful APIs offerings in the industry," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, LNCS, vol. 10601, pp. 589–604, 2017. https://doi.org/10.1007/978-3-319-69035-3_43

[47] D. A. McGrew, "The use of AES-192 and AES-256 in Secure RTP," *RFC*, vol. 6188, pp. 1–16, 2011. https://doi.org/10.17487/rfc6188

[48] Kassim, Azleena, and Alotaibi, Khalid, "Factors that influence the adoption of digital dental technologies and dental informatics in dental practice," *International Journal of Online and Biomedical Engineering (iJOE)*, vol. 19, 2023. https://doi.org/10.3991/ijoe.v19i15.43015

[49] C. Zaoui, F. Benabbou, and A. Ettaoufik, "Edge-Fog-Cloud data analysis for eHealth-IoT," *International Journal of Online & Biomedical Engineering*, vol. 19, no. 7, 2023. https://doi.org/10.3991/ijoe.v19i07.38903

10 AUTHORS

Agariadne Dwinggo Samala is a professional educator, futurologist, dedicated researcher, and an Assistant Professor at the Faculty of Engineering, Universitas Negeri Padang (UNP), Indonesia, specializing in Informatics and Computer Engineering Education. He graduated from the Department of Computer Engineering, Faculty of Information Technology, Universitas Andalas, Indonesia. In 2015, he completed a Master's in Technology and Vocational Education from the Faculty of Engineering at UNP, focusing on Informatics Engineering Education. In 2023, he received his Ph.D. from UNP, Indonesia, focusing on the convergence of technology and education. Additionally, Agariadne is the Founder and Coordinator of EMERGE (Emerging Technologies, Multimedia, and Education Research Group) at Digital Lab, where he contributes to advancing research initiatives. He is an external collaborator of the Digital Society Lab at the Institute for Philosophy and Social Theory (IFDT), University of Belgrade, Serbia. In addition, he is a member of the International Society for Engineering Pedagogy (IGIP) in Austria. With a deep passion for education, he has conducted impactful research on Technology-Enhanced Learning (TEL), Emerging Technologies in Education, Flexible Learning, 21st Century Learning, and Technology, Vocational Education and Training (TVET). He has also fostered collaborative partnerships with other experts worldwide to drive education progress. He holds certifications as a Microsoft Certified Educator (21st Century Learning), Microsoft Certified: Power BI Data Analyst Associate, and Google Certified Educator. These certifications underscore his commitment to innovative teaching and learning practices, integrating technology to enhance education and research (E-mail: agariadne@ft.unp.ac.id).

Soha Rawas holding a Doctor of Philosophy degree (Ph.D.) in Mathematics and Computer Science, graduated from Beirut Arab University (BAU) in 2019. Dr. Rawas possesses a broad spectrum of expertise spanning several domains, notably artificial intelligence, deep learning, internet of medical things (IOMT), cloud computing, and image processing. With unwavering dedication to her research pursuits, she currently serves as an Assistant Professor within the Faculty of Science, Department of Computer Science, at Beirut Arab University (BAU). In addition, she holds a supervisory role at the Center for Continuing and Professional Education (CCPE) at BAU (E-mail: soha.rawas2@bau.edu.lb).