VFAST Transactions on Software Engineering
https://vfast.org/journals/index.php/VTSE@ 2023, ISSN(e): 2309-3978, ISSN(p): 2411-6246
Volume 11, Number 4, October-December 2023 pp: 57-66

Securing Electronic Health Records using Blockchain

Syed Tayyab Raza Zaidi *, Dur-e-Shawar Agha , Safi Ullah , Azam Khan ,
Taimoor Ali Khan

[1]Department of Software Engineering, Sir Syed University of Engineering Karachi, Pakistan

Keywords: *Block Chain, Electronic Health Records, IoT sensors, Patient Monitoring, Healthcare Industry.*

Journal Info:
Submitted:
October 14, 2023
Accepted:
November 30, 2023
Published:
December 11, 2023

Abstract

This research explores the application of blockchain technology in securing Electronic Health Records (EHRs) while integrating IoT sensors for real-time patient monitoring. The primary goal is to address critical healthcare industry challenges, including security, privacy, data integrity, and accessibility. Our system focuses on enhancing EHR security and reliability through blockchain's decentralized and tamper-resistant features. Additionally, IoT sensors provide real-time monitoring of vital signs, enabling prompt interventions. This study not only delves into technical aspects but also considers practical implementation in healthcare, contributing to improved data security and patient care.

***Correspondence author email address:** syedtayyabrazazaidi@gmail.com

DOI: 10.21015/vtse.v11i4.1656

1 Introduction

The healthcare sector faces an array of formidable challenges, with security and privacy concerns surrounding electronic health records (EHRs) standing out as paramount among them [1]. The pervasive specters of unauthorized access, data breaches, and patient privacy infringements continuously haunt the industry. In response, we present an innovative system that seamlessly merges cutting-edge block chain technology and the precision of IoT sensors. This groundbreaking solution not only transforms EHR management but also pioneers real-time patient monitoring [2]. It effectively safeguards sensitive medical data, ensures proactive healthcare interventions, and elevates the overall quality of patient care [3].

1.1 Overview of Challenges

In the healthcare landscape, challenges abound, and the security and privacy of electronic health records (EHRs) remain at the forefront [3]. Unrelenting concerns related to unauthorized access, data breaches, and patient privacy violations loom large, casting a perpetual shadow over healthcare providers [4]. These issues necessitate a transformative approach.

1.2 Our Innovative Solution

In response to these pressing concerns, we introduce an innovative system that seamlessly integrates state-of-the-art blockchain technology with the precision of IoT sensors [7]. This groundbreaking solution goes beyond the conventional, revolutionizing the management of EHRs. It pioneers a new paradigm for real-time patient monitoring [5]. In doing so, it effectively safeguards sensitive medical data, ensures proactive healthcare interventions, and enhances the overall quality of patient care [6].

2 Problem Statement

Within the healthcare industry, a complex web of challenges looms large, creating a tapestry of issues that demand immediate attention.

2.1 Security and Privacy Vulnerabilities

Electronic Health Records (EHRs) face an ever-present risk of cyberattacks and unauthorized access, exposing patient data to potential breaches. These breaches not only infringe upon the fundamental right to privacy but also erode the trust essential for effective healthcare delivery.

2.2 Data Trustworthiness Dilemma

The relentless pursuit of ensuring the accuracy and trustworthiness of EHRs remains a daunting challenge. Maintaining the integrity of medical records is pivotal, as any inaccuracies or tampering could lead to misdiagnoses and inappropriate treatments.

2.3 Real-time Monitoring Gaps

Critical health conditions often elude timely detection due to deficiencies in real-time monitoring systems. This deficiency in timely intervention can have life-threatening consequences, emphasizing the need for robust monitoring mechanisms.

2.4 Interoperability Impediments

EHRs reside in fragmented systems, creating isolated islands of data that hinder the seamless exchange of vital patient information among healthcare providers. These interoperability hurdles disrupt the flow of critical information, impede collaborative decision-making, and introduce inefficiencies into the healthcare ecosystem.

The intricate nature of these challenges underscores the urgency for a holistic and transformative solution. Such a solution must comprehensively address security, privacy, data integrity, real-time monitoring, and interoperability concerns, ultimately reshaping the healthcare landscape for the better.

3 Literature Review

A meticulous examination of the existing body of research unveils a diverse array of strategies aimed at fortifying Electronic Health Record (EHR) security:

3.1 Blockchain Brilliance

Blockchain technology, renowned for its prowess in fortifying data security, privacy, and integrity, has emerged as a dominant theme across several studies.

Zarour et al. [1] focuses on the evaluation of various blockchain models and their applicability to secure electronic healthcare records (EHRs). The study underscores the importance of leveraging blockchain's decentralized and immutable characteristics to enhance data security, privacy, and access control within the healthcare sector.

Sun et al. [2] explores a blockchain-based secure storage and access scheme for electronic medical records (EMRs) in the Interplanetary File System (IPFS). The research introduces a solution that combines blockchain's decentralized nature with IPFS's distributed storage capabilities to ensure the security, privacy, and reliability of EMRs.

Ali et al. [3] delves into the realm of security, privacy, and reliability in digital healthcare systems using blockchain technology. The researchers advocate for blockchain's potential to mitigate vulnerabilities associated with centralized storage and exchange of sensitive healthcare data, emphasizing the benefits of data security, transparency, integrity, and patient control over their medical records.

Usman and Qamar [4] proposes the use of blockchain technology for secure electronic medical records (EMRs) storage and sharing. By harnessing blockchain's decentralized and tamper-resistant attributes, the study advocates for secure and transparent EMR systems with enhanced data security, interoperability, and patient empowerment.

Kazi et al. [7] places the spotlight on an Electronic Health Record (EHR) Monitoring System that employs blockchain technology. This system leverages blockchain's decentralized and immutable nature to securely store and control access to patient records while facilitating transparent collaboration among healthcare professionals.

Shahnaz et al. [11] investigates the application of blockchain technology in the context of electronic health records. The research aims to tackle challenges related to EHR security, data integrity, privacy, and interoperability, highlighting the potential improvements in data security, privacy, and overall EHR management.

Yan et al. [12] offers a novel perspective by proposing a blockchain-based decentralized storage scheme. The study explores how blockchain can be used to securely store and distribute data, ensuring fault tolerance, transparency, and improved data security.

Guendalina and Francesco. [14] conducts an examination of blockchain's potential applications within healthcare. Focusing on Electronic Health Records (EHRs), the research emphasizes the benefits of blockchain, such as secure data storage, controlled access, and automated consent management through smart contracts.

Roberto, Piera, Emanuela, Stefano and Eugenio. [15] introduces a design for a distributed electronic health record ecosystem using blockchain technology. This innovative approach enhances the security and privacy of EHRs while promoting efficient data exchange among healthcare providers through the use of smart contracts.

Guang, Chunlei and Kjell. [16] addresses security challenges in electronic health record systems. By harnessing blockchain technology, the study establishes a secure platform for storing EHRs, ensuring data integrity and confidentiality.

MyeongHyun et al. [17] presents a secure protocol design for cloud-assisted electronic health record systems using blockchain. The research focuses on the integration of cloud computing and blockchain to address security and privacy concerns in centralized cloud-based systems.

Aitizaz et al. [19] introduces a blockchain security framework for electronic health records (EHRs). This framework leverages blockchain technology to ensure the security and confidentiality of patient data, using smart contracts and cryptographic techniques for access control and data protection.

Dileep, Sandeep and Santosh. [20, 21], conducts a systematic review of blockchain technology's role in preserving privacy and security within electronic health systems. The review highlights the potential benefits of blockchain in mitigating risks associated with unauthorized access, data breaches, and data tampering, ultimately enhancing patient information security within healthcare settings.

3.2 IoT's Synergy

The synergistic fusion of Internet of Things (IoT) sensors with blockchain technology, as explored in [5] presents an intriguing frontier in healthcare. This integration extends beyond mere security, offering a gateway to real-time patient monitoring and data security.

3.3 Consortium Blockchains and Secure Protocols

Duo Zhang, Shangping Wang, Yinglong Zhang, Qian Zhang, and Yaling Zhang. [9] introduces the concept of consortium blockchains, an innovative approach that strikes a harmonious balance between data sharing and privacy preservation, on the other hand, delves into secure protocols, elucidating their role in safeguarding data integrity while facilitating sharing in EHR systems.

3.4 Decentralized Data Fortresses

The realm of decentralized storage solutions, as discussed by Yan et al. [12] tackles two pressing concerns in healthcare data management: scalability and security. These solutions pave the way for a more robust infrastructure that is impervious to centralized vulnerabilities.

3.5 Taxonomic Treasure Troves

Azbeg, Ouchetto, Andaloussi and Fetjah. [13], unfurls the canvas of taxonomic reviews, offering a panoramic view of IoT and blockchain applications in healthcare. These reviews not only provide in-depth insights but also serve as invaluable resources for understanding the multifaceted landscape of healthcare technology.

Collectively, this literature review underscores the multifaceted nature of EHR security enhancement strategies. It showcases the dynamism of research efforts aimed at fortifying healthcare data, illuminating the path toward a more secure and resilient healthcare ecosystem.

4 Proposed System

In response to the identified challenges plaguing the healthcare sector, we introduce a meticulously designed system that harmoniously amalgamates the formidable capabilities of blockchain technology and the precision of IoT sensors. This fusion ushers in an era of unprecedented EHR management and patient monitoring efficiency.1 shows the system diagram of the proposed system in which patient data is collected from different IoT sensors through application and apply blockchain to secure the record.

4.1 Blockchain

The Guardian of Security: At the core of our system lies a permissioned blockchain, meticulously crafted to serve as an impregnable fortress for EHRs. Here, security isn't a mere afterthought; it's the very essence. The blockchain stands as an unwavering sentinel, guaranteeing secure and tamper-proof storage of electronic health records. Data integrity is sacrosanct, and access control is absolute. Every entry, every modification, is etched indelibly into the ledger, ensuring that patient data remains inviolable and invulnerable.

4.2 IoT Sensors

The Watchful Guardians: Complementing the blockchain's robust security, our system employs an arsenal of IoT sensors - ECG sensors, heart rate sensors, and body temperature sensors - working tirelessly in tandem. They form a vigilant network, providing continuous real-time monitoring of patients' vital signs. In the crucible of healthcare, time is often the arbiter between life and otherwise. Thus, our system is primed to respond with utmost alacrity. When critical health thresholds are breached, these sensors become harbingers of hope, triggering instant alerts to healthcare providers through a dedicated application. Lives are safeguarded, and outcomes are optimized, thanks to this responsive guardian.

4.3 Interoperability: Bridging the Gaps

In the labyrinthine landscape of healthcare, interoperability remains an elusive beacon. However, our system heralds a new dawn in this regard. Through the ingenious application of blockchain, we create a unified data repository, a sanctum accessible exclusively to authorized entities. Gone are the days of fragmented data silos. Instead, a seamless tapestry of information emerges, allowing healthcare providers to navigate with unparalleled ease and efficiency.

In summary, our proposed system isn't merely a solution; it's a manifesto for the future of healthcare. It seamlessly integrates the best of blockchain's security, IoT sensors' vigilance, and interoperability's convenience. It is the harbinger of a healthcare ecosystem where data remains inviolate, responses are immediate, and care is uncompromised.

In this project, Distributed Architecture is used. Distributed architecture refers to a system design where components of the application are spread across multiple nodes or servers rather than being concentrated on a single server. In this architecture, various components communicate with each other to achieve the system's overall functionality and maintain data integrity.

Using a distributed architecture offers several advantages for the "Securing Electronic Health Records Using Blockchain".

4.3.1 Scalability

Distributed systems can scale easily by adding more nodes to handle increasing data and user loads.

4.3.2 Fault Tolerance

If one node fails, other nodes can take over, ensuring continuous system operation and data availability.

4.3.3 Redundancy

Data redundancy can be achieved by storing data on multiple nodes, enhancing data reliability.

4.3.4 Data Privacy and Security

In a distributed system, data is distributed across multiple nodes, reducing the risk of unauthorized access to sensitive information.

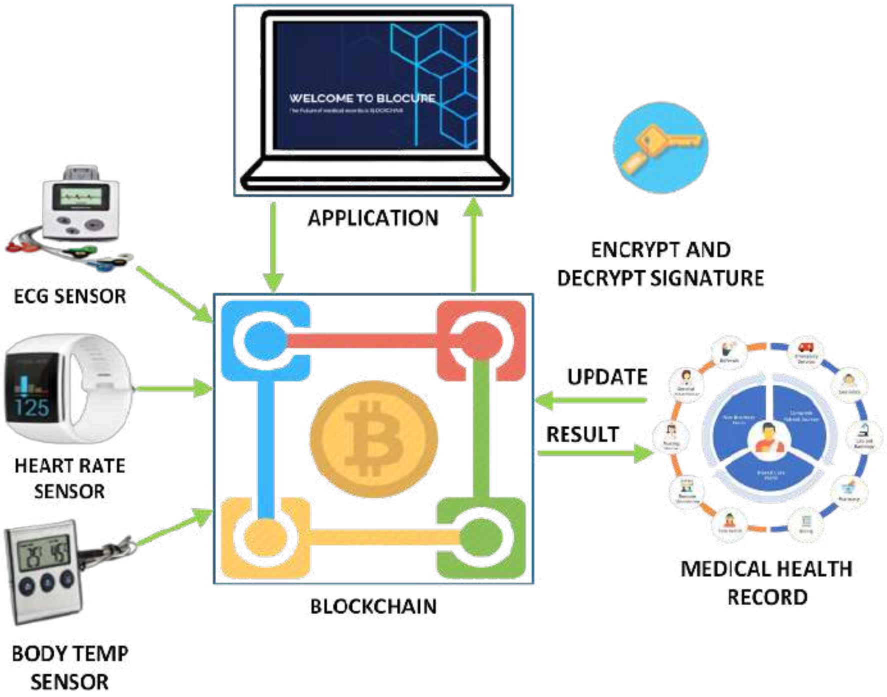

Figure 1. System Diagram of proposed solution

4.3.5 Decentralization

Decentralization ensures that no single entity has complete control over the system, increasing transparency and trust.

5 System Architecture and Working

5.1 User Interface (UI)

The user interface serves as the entry point for both patients and healthcare providers, ensuring a seamless interaction with the system. It is designed with a user-friendly layout, allowing patients to input and access their electronic health records (EHRs) and enabling healthcare providers to monitor real-time patient data. The UI accommodates functionalities such as data input, health parameter visualization, and user authentication.

5.2 Data Collection

IoT Sensors: IoT sensors, including ECG sensors, heart rate sensors, and body temperature sensors, form a crucial component of the data collection process. These sensors continuously monitor vital signs in real-time. The collected data is transmitted securely to the system, providing a comprehensive view of the patient's health status.

Patient Input: Patients can directly input relevant health information through the user interface. This can include medical history, symptoms, and other subjective data. The system ensures the integration of both patient-input data and real-time sensor data for a holistic health record.

5.3 Encrypted Data Saving to Smart Contract

5.3.1 Blockchain Integration

The system incorporates blockchain technology, utilizing a permissioned blockchain for secure and tamper-proof storage of electronic health records. A smart contract is deployed on the blockchain to manage the storage and retrieval of encrypted health data.

5.3.2 Encryption Mechanism

Prior to storage on the blockchain, patient data is encrypted to ensure confidentiality and privacy. The encryption mechanism employs industry-standard cryptographic protocols, safeguarding sensitive health information from unauthorized access.

5.3.3 Smart Contract Operations

The smart contract is programmed to handle operations related to data storage, retrieval, and access control. It ensures that only authorized entities can interact with the stored data, maintaining the integrity and security of the electronic health records.

5.4 Access Control for Health Providers

Authentication: Healthcare providers are granted access to patient records through a robust authentication system. This involves secure login credentials and possibly additional authentication measures such as multi-factor authentication to ensure the identity of the accessing entity.

Role-Based Access: Access control is implemented based on the principle of least privilege. Different healthcare providers may have varying levels of access depending on their roles and responsibilities. For instance, a primary care physician may have access to general health data, while specialists may access more specific information related to their field.

Audit Trial: The system maintains an audit trail within the blockchain to track access to patient records. This ensures accountability and traceability, allowing for a transparent review of who accessed what information and when.

This system architecture ensures a secure and efficient flow of health data from the user interface to encrypted storage on the blockchain. It emphasizes patient privacy, real-time monitoring, and controlled access for healthcare providers, contributing to an advanced and trustworthy electronic health record management system.

6 Result and Comparative Study

In the crucible of a real healthcare environment, our final year project brought the proposed system to life, and the outcomes surpassed expectations:

6.1 EHR Data Security and Privacy

Blockchain Transaction Costs Over Time Figure 2 shows the variations in blockchain transaction costs over the data collection period, providing insights into the cost dynamics of securing EHRs.

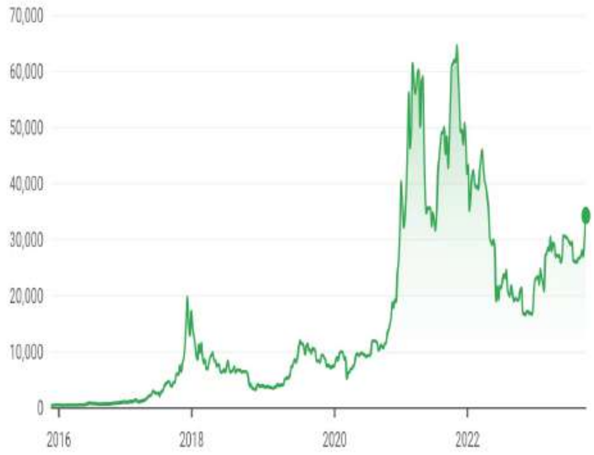

Figure 2. Blockchain Cost overtime

Security Incidents Table: 1 summarize the recorded security incidents, including attempted breaches and security breaches, illustrating the effectiveness of our security measures.

6.2 Data Integrity and Efficiency

Blockchain Data Retrieval Time: Figure 3 presents the time-based analysis of data retrieval times from the blockchain, indicating the efficiency of our data management system.

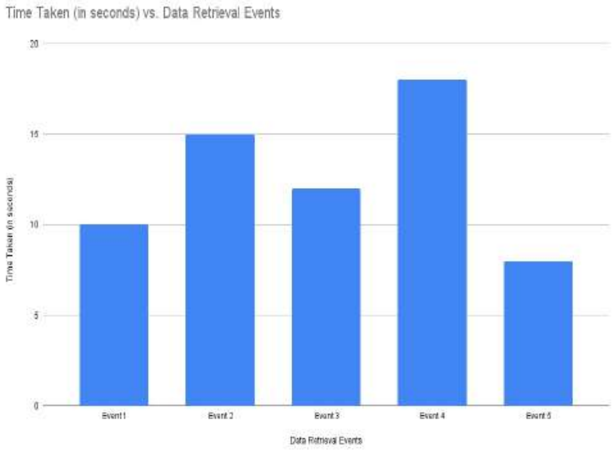

Figure 3. Blockchain Data Retrieval Time

Scaling Performance: Figure 4 demonstrates the system's performance as it scales to accommodate a larger volume of patient data, highlighting its efficiency p0.25

Table 1. Security Incidents

Incident Date	Type of Incident	Attempted Breaches	Successful Breaches
2023-03-05	Unauthorized Access	3	1
2023-03-12	Malware Attack	2	0
2023-03-20	Data Breach	4	2
2023-03-28	Phishing Attempt	1	0
2023-04–03	System Outage	NA	1

and scalability.

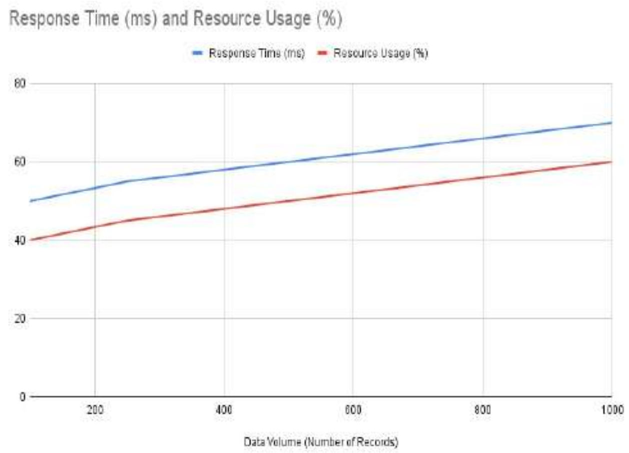

Figure 4. Scaling Performance

Alert Triggers: In Table 2, we document instances where the system triggered alerts to healthcare providers based on real-time patient data, providing an overview of the system's responsiveness.

Patient Outcomes: Figure 5 offers a comparative analysis of patient outcomes before and after the implementation of real-time monitoring, showing the potential benefits of our system.

6.3 Interoperability and Data Exchange

Data Exchange Efficiency: Figure 6 visually represents the time taken to exchange patient data between different healthcare providers, reflecting the system's interoperability

Comparison with Industry Standards: In Figure 7, we compare the data exchange efficiency of our system with industry standards or similar systems, providing valuable insights into its performance.

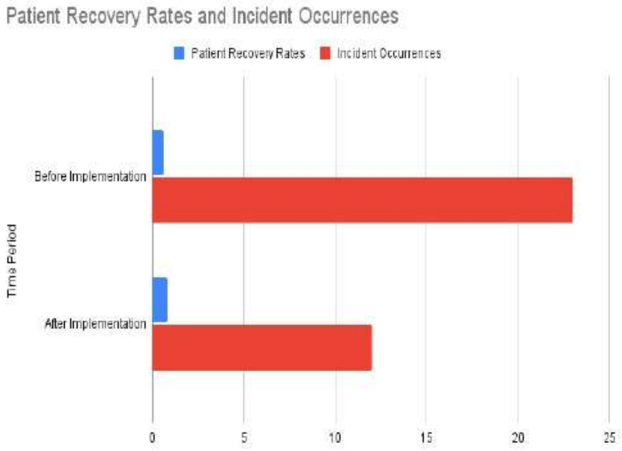

Figure 5. Patient Outcomes

Comparative Study: In our investigation of blockchain technology's application in securing electronic health records (EHRs), we conducted a comprehensive comparative analysis with several notable contributions in the field. The following studies have been particularly insightful in shaping our understanding of the current landscape.

Zarour et al. [1] evaluated various blockchain models for secure and trustworthy EHRs. While their focus was on the impact of blockchain models, our study extends this by implementing a robust permissioned blockchain, emphasizing real-time patient monitoring through IoT sensors

Sun et al. [2] proposed a blockchain-based secure storage and access scheme for electronic medical records in IPFS. In contrast, our system integrates IoT sensors for real-time monitoring, providing immediate insights for healthcare interventions p0.25

Table 2. Alert Tiggers

Alert Timestamp	Patient ID	Type of Alert	Actions Taken
2023-01-10 08:35AM	12345	Abnormal Heart Rate	Notified Cardiologist, Medication Adjustment
2023-01-10 08:35 AM	67890	High Blood Pressure	Alert Nurse; Adjusted Medication Doses
2023-04-15 10:47 AM	54321	Low Oxygen Levels	Nurse Intervention; Oxygen Supply Provided
2023-05-28 02:00 PM	98765	Irregular ECG	Alert Cardiologist; Ordered ECG Evaluation
2023-06-15 03:00 AM	24680	High Temperature	Nurse Assessment; Ordered Fever-Reducing Meds

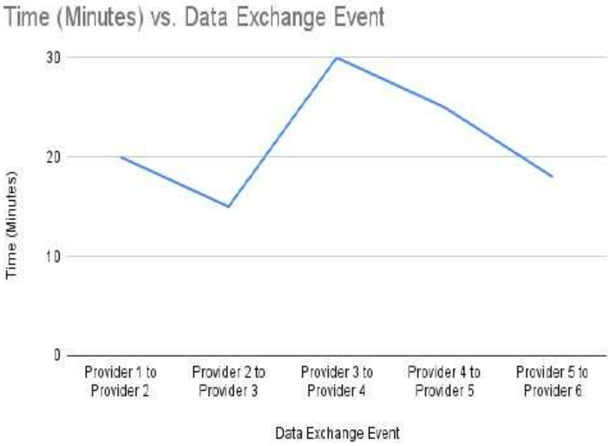

Figure 6. Data Exchange Efficiency

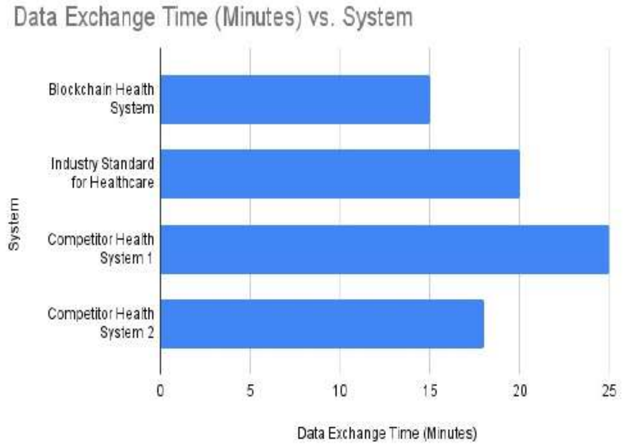

Figure 7. Comparison with Industry Standards

Ali et al. [3] addressed security, privacy, and reliability in digital healthcare systems using blockchain. In comparison, our system not only emphasizes these aspects but also incorporates encrypted data storage on a smart contract with detailed access control for healthcare providers.

Usman and Qamar [4] focused on secure electronic medical records storage and sharing using blockchain technology. Our study builds upon this by introducing a permissioned blockchain, IoT sensors, and a sophisticated access control mechanism.

Yogeshwar and Kamalakkannan [5] explored the healthcare domain in IoT with blockchain-based security. While their work provides valuable perspectives, our system delves deeper into the integration of blockchain and IoT for enhanced security and real-time patient monitoring.

Ratta et al. [6] discussed the application of blockchain and IoT in healthcare, highlighting challenges and future perspectives. Our study contributes by implementing a concrete system architecture that addresses these challenges with a focus on data security and patient care.

Shahnaz et al. [11] proposed using blockchain for electronic health records. In comparison, our system not only utilizes blockchain but also incorporates IoT sensors, ensuring a comprehensive approach to healthcare data management.

Conclusion: This comparative analysis positions our work within the context of existing research, showcasing the unique contributions and advancements of our system in the realm of secure and efficient electronic health record management. The integration of blockchain, IoT, and advanced access control mechanisms distinguishes our system as a comprehensive solution for addressing the complex challenges in healthcare data security and patient care.

7 Conclusion

The integration of blockchain technology and IoT sensors isn't merely a solution; it's a paradigm shift. In addressing the formidable challenges confronting the healthcare sector, it serves as both a cornerstone and a keystone. Data security, privacy, and accessibility, often elusive, are now a reality. Our system represents a watershed moment, a testament to the power of innovation in improving patient care and data management.

8 Future Enhancements

Our journey doesn't end here; it's a prologue to an even more promising future:

8.1 Machine Learning Integration

The roadmap ahead involves the assimilation of predictive analytics, elevating healthcare to the realm of foresight. Early warnings for critical health conditions, once a dream, will become a tangible reality.

8.2 Enhanced Patient Control:

Our commitment extends to empowering patients. Mechanisms for patients to wield control over their electronic health records and consent will be developed, ensuring that their voices resonate throughout their healthcare journey.

8.3 Scalability:

In the pursuit of a broader impact, our horizons will expand. Methods for scaling the system, accommodating larger healthcare networks, and serving a more extensive patient base will be explored. The future is boundless, and our system will grow with it, ensuring that healthcare remains at the forefront of innovation and progress.

Author Contributions

Syed Tayyab Raza Zaidi: Conceptualization, Methodology, Software **Dur-e-Shawar Agha**: Writing-Original draft preparation. **Safi Ullah**: Visualization,Investigation,Writing–originaldraft. **Azam Khan**: Comparative Analysis,writing–review and editing.: **Komar Singh**: Software, Validation. **Taimoor Ali Khan**: Writing- Reviewing and Editing

Compliance with Ethical Standards

It is declare that all authors don't have any conflict of interest. It is also declare that this article does not contain any studies with human participants or animals performed by any of the authors. Furthermore, informed consent was obtained from all individual participants included in the study.

Funding Information

No funding associated with this research

References

[1] Z. Muhammad, M.T.J. Ansari, M. Alenizi, A.K. Sarkar, M. Faizan, A. Agarwal, R. Kumar and R. A. Khan, "Evaluating the impact of blockchain models for secure and trustworthy electronic healthcare records," *IEEE Access*, vol. 8, pp. 157959-157973, 2020.

[2] Sun, Jin, X. Yao, S. Wang, and Y. Wu, "Blockchain-based secure storage and access scheme for electronic medical records in IPFS," *IEEE Access*, p. 59389-59401, 2020.

[3] Ali, A., Rahim, H.A., Pasha, M.F., Dowsley, R., Masud, M., Ali, J. and Baz, M., "Security, privacy, and reliability in digital healthcare systems using blockchain," *Electronics*, vol. 10, no. 16, pp. 2034, 2021.

[4] Usman, M. and Qamar, U., "Secure electronic medical records storage and sharing using blockchain technology.," *Procedia Computer Science*, pp. 321-327, 2020.

[5] A. Yogeshwar and S. Kamalakkannan, "Healthcare Domain in IoT with Blockchain Based Security-A Researcher's Perspectives.," *International Conference on Intelligent Computing and Control Systems (ICICCS). IEEE*, pp. 001-009, 2021.

[6] P. Ratta, A. Kaur, S. Sharma, M. Shabaz and G. Dhiman, "Application of blockchain and internet of things in healthcare and medical sector: applications, challenges, and future perspectives.," *Journal of Food Quality*, pp. 001-020, 2021.

[7] A.M. Hasib, K. Tamzid, et al, "Electronic health record monitoring system and data security using blockchain technology..," *Security and Communication Networks*, pp. 001-015, 2022.

[8] V.Sharma, et al, “On the Internet of Things, Blockchain Technology for Supply Chain Management (IoT).,” *Wireless Communications and Mobile Computing* ,2022.

[9] D. Zhang, S. Wang, Y. Zhang, Q. Zhang and Y. Zhang, “A secure and privacy-preserving medical data sharing via consortium blockchain.,” *Security and Communication Networks*,2022.

[10] K. Kiania, S. M. Jameii, and A. M.Rahmani, “Blockchain-based privacy and security preserving in electronic health: a systematic review.,” *Multimedia Tools and Applications*,pp. 001-027, 2023.

[11] A. Shahnaz, U. Qamar and A. Khalid, “Using blockchain for electronic health records.,” *IEEE access*,pp. 147782-147795, 2019.

[12] Y. Zhu, C. Lv, Z. Zeng, J. Wang and B. Pei, “Blockchain-based decentralized storage scheme,” *Journal of Physics: Conference Series*,vol 1237, 2019.

[13] K. Azbeg, O. Ouchetto, S.J. Andaloussi and L. Fetjah, “A taxonomic review of the use of IoT and blockchain in healthcare applications,” *Irbm*,vol 43, pp. 511-519, 2022.

[14] G. Capece and F. Lorenzi, “Blockchain and Healthcare: Opportunities and Prospects for the EHR,” *Sustainability* ,vol 12, pp. 9693, 2020.

[15] R. Cerchione, et al, “Blockchain’s coming to hospital to digitalize healthcare services: Designing a distributed electronic health record ecosystem,” *Technovation*, 2023.

[16] M. Kim, S.J. Yu, J. Y. Lee, and Y.H. Park, “Design of secure protocol for cloud-assisted electronic health record system using blockchain,” *Sensors* ,vol 20, pp. 2913, 2020.

[17] I. Abunadi,and R.L. Kumar, “BSF-EHR: blockchain security framework for electronic health records of patients.,” *Sensors* ,vol 21, pp. 2865, 2021.

[18] A. Ali et. al., “A novel secure blockchain framework for accessing electronic health records using multiple certificate authority.,” *Applied Sciences* , pp. 9999, 2021.

[19] D.K. Murala, S.K. Panda, and S.K. Sahoo, “Securing electronic health record system in cloud environment using blockchain technology.,” *Springer International Publishing*, pp. 089-116, 2023.

[20] A. H. Mayer, C. A. da Costa, and R. D. R. Righi, "Electronic health records in a Blockchain: A systematic review," Health Informatics Journal, vol. 26, no. 2, pp. 1273-1288, 2020.

[21] F. A. Reegu et al., "Interoperability Requirements for Blockchain-Enabled Electronic Health Records in Healthcare: A Systematic Review and Open Research Challenges," Security and Communication Networks, 2022.