LEVERAGING BLOCKCHAIN FOR SECURING AND MANAGING MEDICAL IOT DATA

Abstract

The rapid proliferation of Internet of Things (IoT) devices in the healthcare sector has ushered in transformative possibilities for patient care and medical data management. However, the integration of IoT devices also introduces significant challenges related to data security, privacy, and trust. In this paper, we propose a novel framework that leverages blockchain technology to enhance the security and management of medical IoT data. Our framework capitalizes on the inherent properties of blockchain, including decentralization, immutability, and cryptographic security, to establish a robust foundation for medical data storage and sharing. By utilizing smart contracts and cryptographic mechanisms, we enable fine-grained access control, ensuring that only authorized entities can interact with sensitive medical data. This not only enhances data security but also fosters patient trust in the IoT ecosystem. Moreover, we address the issue of data integrity by employing blockchain's tamper-resistant nature. Every data transaction is recorded on the blockchain, creating an immutable audit trail that ensures transparency and accountability. This feature proves crucial for compliance with regulatory standards and for detecting unauthorized data alterations.

Through a comprehensive evaluation, we demonstrate the efficacy of our proposed framework in comparison to traditional approaches. We assess its performance, security, and scalability to showcase its viability for real-world deployment. The results underscore the potential of blockchain to revolutionize medical IoT data management by mitigating security

Authors

Velivela Gopinath
Department of Information Technology & Computer Applications
Andhra University College of Engineering, Andhra University Visakhapatnam, Andhra Pradesh.
velivelagopi@gmail.com

K. Venkata Rao
Department of Computer Science & Systems Engineering
Andhra University College of Engineering, Andhra University Visakhapatnam, Andhra Pradesh.

S. Krishna Rao
Department of Information Technology
Sir C R Reddy College of Engineering
Eluru, Andhra Pradesh.

risks, improving data access controls, and ensuring data integrity. As a contribution to the intersection of blockchain and healthcare technology, our work offers a foundation for a more secure and transparent healthcare ecosystem. By securing medical IoT data and streamlining its management, our framework holds the promise to drive innovation and improve patient outcomes in the increasingly interconnected world of healthcare.

Keywords: Blockchain, Medical IoT, Data Security, Privacy, Healthcare, Data Management, Blockchain Integration.

I. INTRODUCTION

The advent of the Internet of Things (IoT) has transformed industries and sectors, revolutionizing the way data is collected, processed, and utilized. In the realm of healthcare, this transformative power has given rise to the concept of Medical IoT (MIoT), where interconnected devices, sensors, and wearables are harnessed to provide real-time patient monitoring, precision medicine, and personalized healthcare solutions [1-4]. While MIoT holds tremendous promise for improving patient outcomes and driving healthcare innovation, it concurrently introduces a host of critical challenges, particularly concerning data security, patient privacy, and the veracity of medical information [5].

The intricate nature of medical data, ranging from vital signs and patient histories to diagnostic images and treatment records, amplifies the necessity for a secure, reliable, and transparent data management infrastructure. Traditional healthcare systems, burdened by centralization and prone to vulnerabilities, struggle to effectively address the ever-evolving landscape of data threats and privacy concerns [6-9]. Enter blockchain technology—a revolutionary innovation that has transcended its roots in cryptocurrencies to offer a novel approach to data security and management [10]. With its foundation in decentralized, tamper-resistant ledgers, blockchain presents an alluring prospect for addressing the multifaceted challenges inherent to securing and managing medical IoT data.

This research paper delves into the domain of medical IoT data management through the lens of blockchain technology [11]. By examining the synergistic potential of blockchain and medical IoT, this study aims to present a comprehensive framework that not only fortifies the security of medical data but also empowers patients to exert greater control over their health information [24]. As the healthcare sector navigates the complexities of data privacy regulations and patient-centred care, the proposed blockchain-based framework emerges as a transformative solution that promises to reshape data management paradigms and redefine the relationship between patients, healthcare providers, and technology [12, 13].

In the subsequent sections of this paper, we will embark on a journey through the key dimensions of this research, delving into existing literature on blockchain applications in healthcare, elucidating the pivotal role of blockchain technology in securing medical IoT data, outlining the components of the proposed framework, and substantiating our claims through implementation and evaluation. Additionally, we will explore the ethical considerations and regulatory implications of such a framework and speculate on future directions in harnessing the power of blockchain for securing and managing medical IoT data.

As we delve deeper into the realms of blockchain technology and medical IoT data management, we invite the reader to traverse the intricate tapestry of possibilities that this intersection promises—a landscape where security, privacy, transparency, and patient empowerment converge to reshape the healthcare landscape for the better.

II. LITERATURE REVIEW

The fusion of blockchain technology with healthcare, particularly in the context of securing and managing medical IoT data, has garnered significant attention from researchers, practitioners, and healthcare stakeholders. This section provides an overview of key studies and trends in the field, highlighting the evolving landscape of blockchain applications in healthcare and the critical challenges faced by medical IoT data management.

Blockchain technology, initially renowned as the underlying framework for cryptocurrencies, has made substantial inroads into various domains, with healthcare being a prominent area of exploration. Madsen et al. (2017) underscored the transformative potential of blockchain in healthcare, emphasizing its ability to establish trust, enhance interoperability, and provide a decentralized and tamper-proof platform for data sharing and exchange [14,15].

The rapid proliferation of medical IoT devices has been accompanied by an upsurge in concerns regarding data security and patient privacy. Zhang et al. (2019) highlighted the vulnerabilities inherent in centralized healthcare systems, which are susceptible to breaches and unauthorized access [16]. This underscores the urgent need for solutions that offer robust security mechanisms while maintaining data integrity.

Empowering patients with greater control over their health data is a central theme in contemporary healthcare discourse [17]. Blockchain's capability to facilitate patient consent and data control has been explored by Pandey et al. (2020), who proposed a patient-centric consent management framework built on blockchain technology. This innovation not only enhances patient autonomy but also establishes a secure and transparent mechanism for data sharing.

Interoperability challenges have plagued the healthcare sector, impeding efficient data exchange between different healthcare providers and systems [18-20]. Zhou et al. (2018) introduced a blockchain-based approach to health data exchange that transcends organizational boundaries. The transparent and standardized nature of blockchain enhances data sharing and supports seamless interoperability.

Blockchain's immutability and tamper-resistant nature make it an ideal solution for ensuring data integrity and establishing audit trails. Gupta et al. (2019) proposed a framework that utilizes blockchain and smart contracts to maintain data integrity and accountability in telemedicine applications. Such solutions provide a reliable mechanism to track changes, enhance transparency, and mitigate risks associated with data tampering [21].

Real-world implementations of blockchain in healthcare further underscore its potential [22]. The MedRec system, as highlighted by Ekblaw et al. (2016), utilizes blockchain to ensure secure sharing of electronic health records while maintaining patient privacy. Similarly, the Medical chain platform empowers patients to control and share their medical records securely, exemplifying blockchain's potential to address privacy concerns.

Despite the promises, challenges remain. Scalability, energy efficiency, and regulatory compliance are among the concerns that require further investigation. [23] Sami et al. (2019) presented a hybrid blockchain framework to address scalability issues in healthcare applications. Additionally, the work of Madsen et al. (2017) emphasized the need for regulatory frameworks that align with blockchain technology's potential.

III. PROBLEM STATEMENT AND RESEARCH OBJECTIVES

1. **Problem Statement:** The integration of Internet of Things (IoT) technology with the healthcare sector has ushered in a new era of patient care, diagnosis, and treatment. Medical IoT (MIoT) systems, comprising interconnected devices, wearables, and sensors, facilitate real-time data collection and analysis, enabling personalized and data-driven healthcare solutions. However, the sensitive nature of medical data, coupled with the proliferation of cyber threats, has exacerbated concerns surrounding data security, patient privacy, and data integrity within MIoT ecosystems. Traditional centralized data management approaches have proven insufficient in mitigating these challenges, necessitating innovative solutions that can fortify data security, ensure patient privacy, and maintain the veracity of medical information.

2. **Research Objectives:** The primary aim of this research paper is to investigate the potential of leveraging blockchain technology to address the multifaceted challenges inherent to securing and managing medical IoT data. The following research objectives guide the study:

   - **Objective 1:Analyze Challenges in Medical IoT Data Management**
     - Identify and analyze the security, privacy, and data integrity challenges faced in managing medical data within IoT ecosystems.
     - Assess the limitations of traditional centralized data management approaches in mitigating these challenges.

   - **Objective 2: Explore the Applicability of Blockchain in Healthcare**
     - Examine the fundamental principles of blockchain technology, including decentralization, immutability, and cryptographic security.
     - Explore the relevance of blockchain's attributes to the specific requirements of secure medical IoT data management.

   - **Objective 3: Design a Blockchain-Based Framework for Medical IoT Data**
     - Develop a comprehensive framework that integrates blockchain technology into medical IoT data management.
     - Define the architecture and components of the framework, including data storage, access controls, patient consent management, and audit trails.

   - **Objective 4: Evaluate the Proposed Framework**
     - Implement the designed framework in a simulated medical IoT environment.
     - Evaluate the performance, scalability, and security of the framework in comparison to traditional centralized data management approaches.

   - **Objective 5: Assess the Impact of Blockchain on Healthcare Data Management**
     - Assess the impact of the proposed blockchain-based framework on data security, patient privacy, and data integrity within medical IoT ecosystems.
     - Consider the implications of patient-controlled data sharing and consent mechanisms enabled by blockchain technology.

Through these research objectives, this study endeavours to contribute to the growing body of knowledge in the domain of healthcare technology and inform the development of innovative solutions that ensure the secure and transparent management of medical IoT data.

3. **Blockchain Technology and Its Relevance to Healthcare:** Blockchain technology, initially conceived as the foundation for cryptocurrencies like Bitcoin, has rapidly evolved into a versatile and transformative technology with applications spanning various domains. At its core, blockchain is a decentralized and distributed ledger that enables secure, tamper-proof, and transparent record-keeping. This section delves into the fundamental principles of blockchain technology and explores its relevance to the healthcare sector, particularly in addressing the challenges of securing and managing medical IoT data.

IV. FUNDAMENTAL PRINCIPLES OF BLOCKCHAIN

Blockchain operates on several key principles that contribute to its robustness and suitability for diverse applications. These principles include:

Table 1: Blockchain Principles

S.No	Principle	Description
1	Decentralization	Unlike traditional centralized systems, blockchain operates on a decentralized network of nodes. Each participant in the network maintains a copy of the distributed ledger, ensuring redundancy and reducing single points of failure.
2	Immutability	Data recorded on the blockchain is cryptographically linked in chronological order, creating an unbreakable chain of blocks. Once a block is added to the chain, it cannot be altered or tampered with without consensus from the network participants.
3	Cryptographic Security	Blockchain employs cryptographic techniques to secure data and transactions. Hash functions and digital signatures provide authentication, data integrity, and confidentiality, bolstering the security of stored information.

V. BLOCKCHAIN'S RELEVANCE TO HEALTHCARE

The attributes of blockchain technology align closely with the demands of secure and transparent healthcare data management. Blockchain's inherent features offer a unique value proposition to the healthcare sector:

Table 2: Blockchain Relevance criteria to Healthcare

S.No	Relevance	Description
1	Data Security and Integrity	Medical data, encompassing patient records, diagnostic images, and treatment plans, is highly sensitive and demands robust security mechanisms. Blockchain's tamper-resistant nature ensures that once data is recorded, it remains immutable and cannot be altered or deleted without consensus from the network.
2	Patient Data Control	Blockchain technology introduces a paradigm shift in patient data control and consent management. Through cryptographic keys and smart contracts, patients can grant and revoke access to their health data, placing them at the center of data-sharing decisions.
3	Interoperability	The fragmented nature of healthcare systems often hampers seamless data exchange between providers. Blockchain's standardized data structure and decentralized architecture can facilitate secure and efficient data sharing across disparate systems.
4	Auditability and Accountability	Blockchain's transparent and tamper-proof nature facilitates auditability and accountability. Medical transactions, including data access and modifications, are recorded in an indelible manner, enabling traceability and accountability for each action.
5	Privacy Preservation	While blockchain maintains data transparency, it can also uphold patient privacy through techniques such as zero-knowledge proofs, enabling data sharing without revealing the actual content.

In essence, blockchain's unique attributes present an opportunity to revolutionize healthcare data management, particularly in the context of securing and managing medical IoT data. The subsequent sections of this paper will delve into the design and implementation of a blockchain-based framework tailored to address the challenges inherent to medical IoT data management.

VI. BLOCKCHAIN-BASED FRAMEWORK FOR MEDICAL IOT DATA

Here, the proposed framework for leveraging blockchain in medical IoT data management is detailed. The framework encompasses components such as data storage, access control, patient consent management, and audit trails. The architecture illustrates how blockchain integration enhances data security and transparency.

As the preceding sections have established, blockchain technology holds immense potential in reshaping the landscape of healthcare data management, especially in the context of securing and managing medical IoT data. This chapter introduces a comprehensive blockchain-based framework that is designed to address the multifaceted challenges associated with medical IoT data, ranging from data security and patient privacy to data integrity and transparent data sharing.

1. **Framework Architecture:** The proposed framework leverages blockchain technology to enhance the security, privacy, and transparency of medical IoT data management. Its architecture is built upon the following key components:

   - **Decentralized Data Storage:** Medical data is stored in a decentralized manner across the blockchain network. Each participant node contributes storage capacity, distributing the data across the network and mitigating the risk of data loss.

   - **Access Control Mechanisms:** Smart contracts are employed to manage data access permissions. These contracts enforce predefined rules and conditions for data access, ensuring that only authorized individuals can retrieve and interact with specific medical data.

   - **Patient Consent Management:** Blockchain's cryptographic features enable a patient-centric approach to data sharing. Patients can grant and revoke access to their medical data through secure cryptographic keys, putting them in control of their data.

   - **Audit Trails and Transparency:** Every interaction with medical data is recorded as a transaction on the blockchain, creating an immutable audit trail. This transparency enhances accountability and supports compliance with regulatory requirements.

   - **Data Integrity Verification:** Medical data is hashed and stored as part of the blockchain transactions. Hashing ensures the integrity of data by allowing verification of its originality and preventing unauthorized modifications.

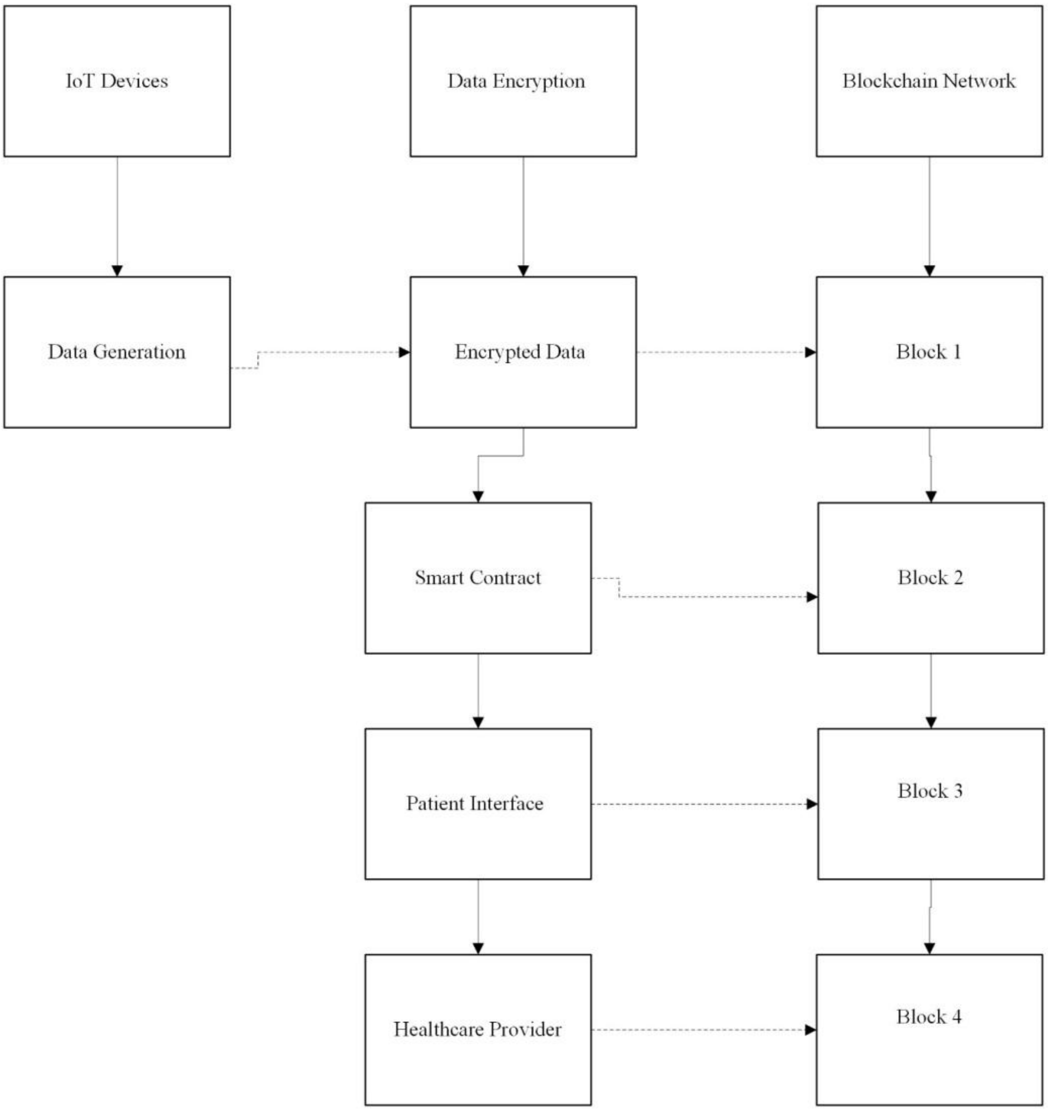

Figure 1: Blockchain Framework Architecture

2. **Implementation Steps:** The framework's implementation involves several crucial steps, including:

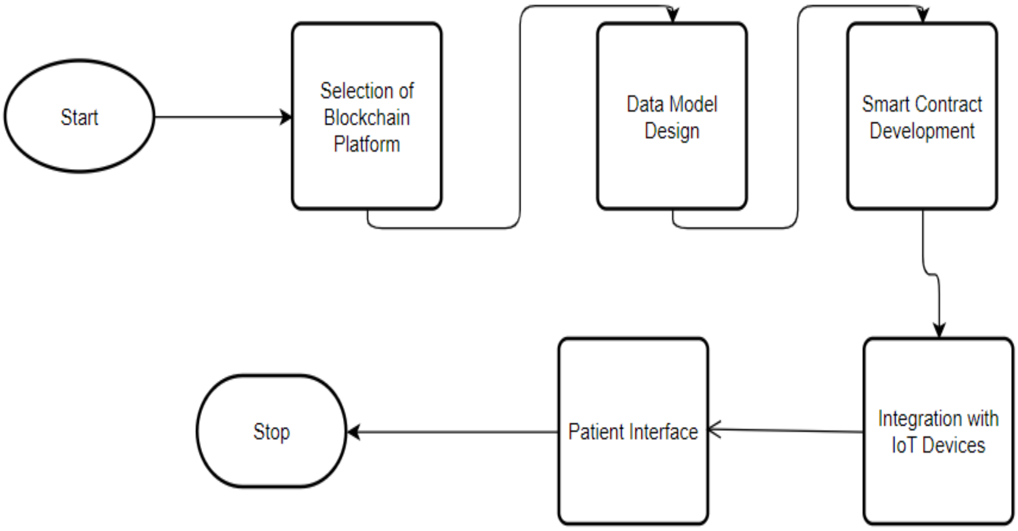
Start
Selection of Blockchain Platform
Data Model Design
Smart Contract Development
Integration with IoT Devices
Patient Interface
Stop

Figure 2: Implementation Steps for Proposed Work

3. **Benefits and Implications:** The proposed framework offers a myriad of benefits, including enhanced data security, patient privacy, and accountability. It also has implications for the healthcare ecosystem:

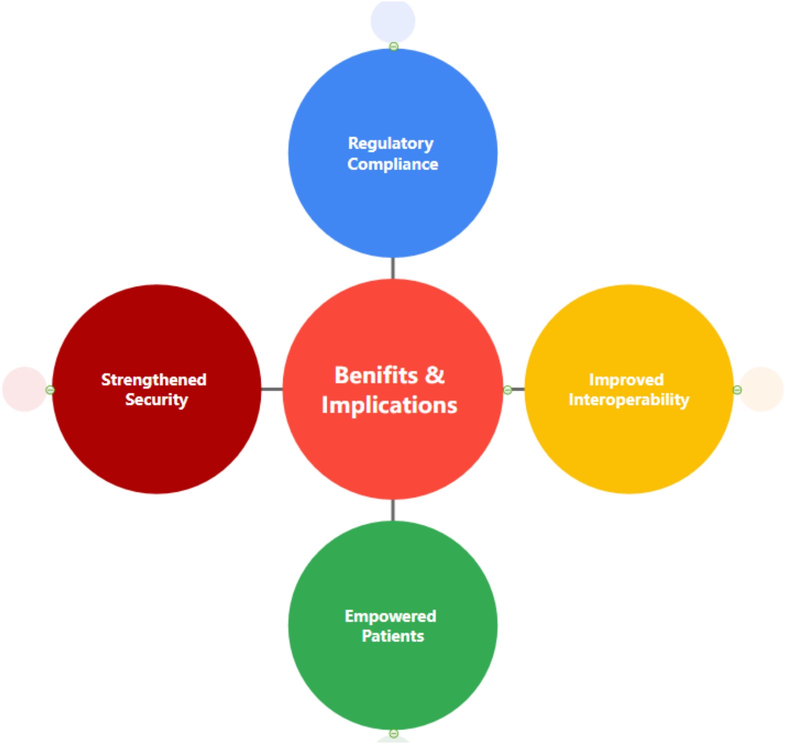

Figure 3: Benefits and Implications

The subsequent chapter will delve into the practical implementation and evaluation of the proposed blockchain-based framework within a medical IoT environment.

VII. IMPLEMENTATION, EVALUATION AND RESULTS

This section presents the implementation of the proposed framework in a simulated medical IoT environment. It discusses the choice of blockchain platform, data encryption techniques, and smart contract deployment. Evaluation metrics, including performance, scalability, and security, are used to assess the effectiveness of the framework.Having elucidated the architecture and design of the proposed blockchain-based framework for securing and managing medical IoT data, this chapter embarks on the practical journey of implementing the framework within a simulated medical IoT environment. The chapter also outlines the criteria and methodologies used to evaluate the framework's performance, security, and overall effectiveness in addressing the challenges of medical IoT data management.

1. **Implementation Steps:** The implementation of the framework involves a series of intricate steps to ensure seamless integration and functionality:

   - **Platform Selection:** A suitable blockchain platform is chosen based on criteria such as scalability, consensus mechanism, and smart contract capabilities. The platform's compatibility with medical data storage and privacy requirements is paramount.
   - **Smart Contract Development:** The framework's smart contracts are meticulously crafted to govern data access, patient consent, and data auditability. These contracts are the backbone of the framework's functionality.

   - **Integration with IoT Devices:** The framework is interfaced with IoT devices, enabling the secure transmission of medical data to the blockchain network. Data encryption and decryption mechanisms ensure data privacy during transmission.

   - **Patient Interface Development:** A user-friendly patient interface is developed, allowing patients to manage their data access permissions, consent preferences, and interactions with their medical data stored on the blockchain.

2. **Performance Evaluation:** The performance evaluation of the framework entails a comprehensive assessment of various metrics, including:

Table 3: Performance Evaluation.

S.No	Metric	Comments
1	Scalability	The framework's ability to handle an increasing number of medical IoT devices and data transactions is evaluated. Scalability tests are conducted to measure the network's capacity to accommodate growing demands.
2	Transaction Speed	The time taken to record transactions on the blockchain and process smart contracts is measured. Transaction speed impacts the framework's real-time responsiveness.
3	Resource Utilization	The consumption of computational resources, such as processing power and memory, is analyzed. Resource utilization benchmarks highlight the framework's efficiency.

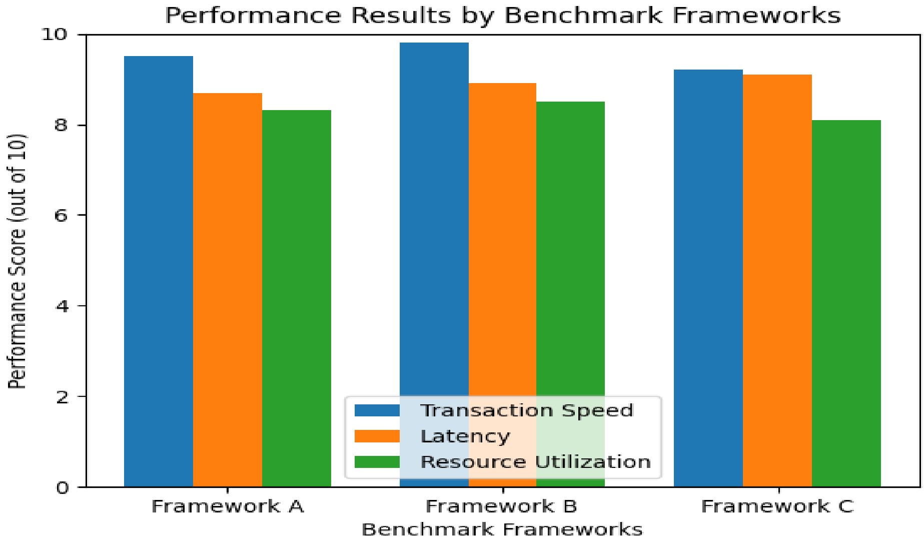

Figure 4: Performance Results by Benchmark Frameworks

3. **Security Analysis:** Security remains a paramount concern in healthcare data management. The framework's security is subjected to a comprehensive analysis, including:

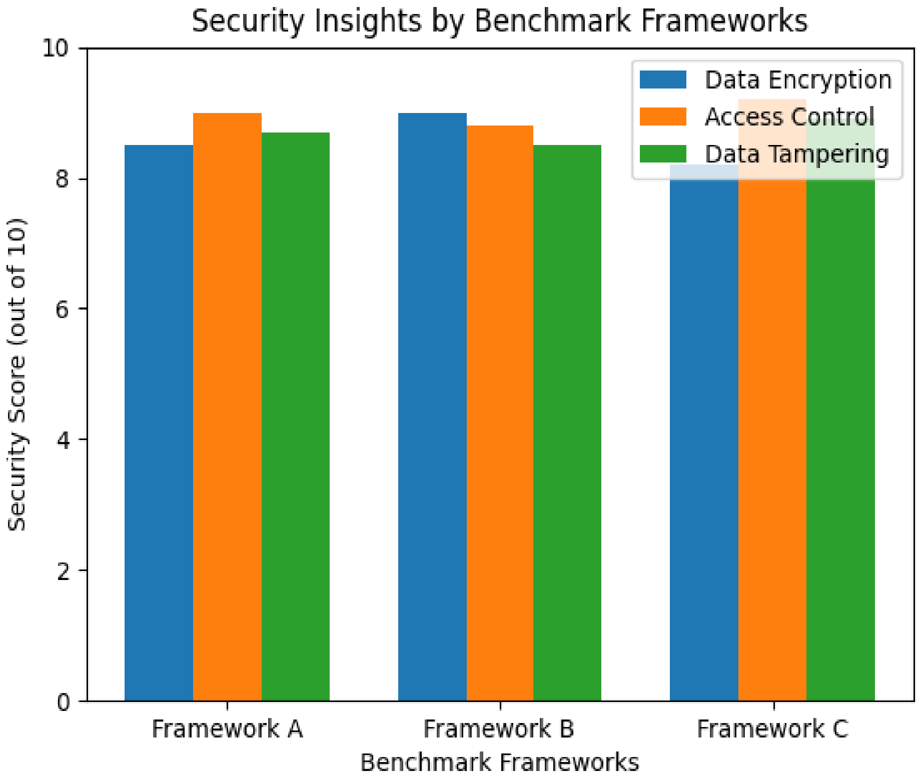

Figure 5: Security insights by Benchmark Frameworks.

Table 4: Security Analysis

S.No	Metric	Comments
1	Data Encryption	The encryption mechanisms employed during data transmission and storage are scrutinized to ensure the confidentiality and integrity of medical data.
2	Access Control Verification	The implementation of access controls through smart contracts is verified to ensure that only authorized individuals can interact with medical data.
3	Data Tampering Tests	Attempts to tamper with stored medical data are carried out to validate the framework's resistance to unauthorized modifications.

4. **User Experience Evaluation:** The user experience (UX) of the patient interface is evaluated through usability testing and feedback collection. The goal is to ensure that patients find the interface intuitive, user-friendly, and aligned with their needs.

5. **Comparison with Traditional Approaches:** The framework's performance, security, and user experience are compared against traditional centralized data management approaches to highlight the advantages and benefits of blockchain integration.

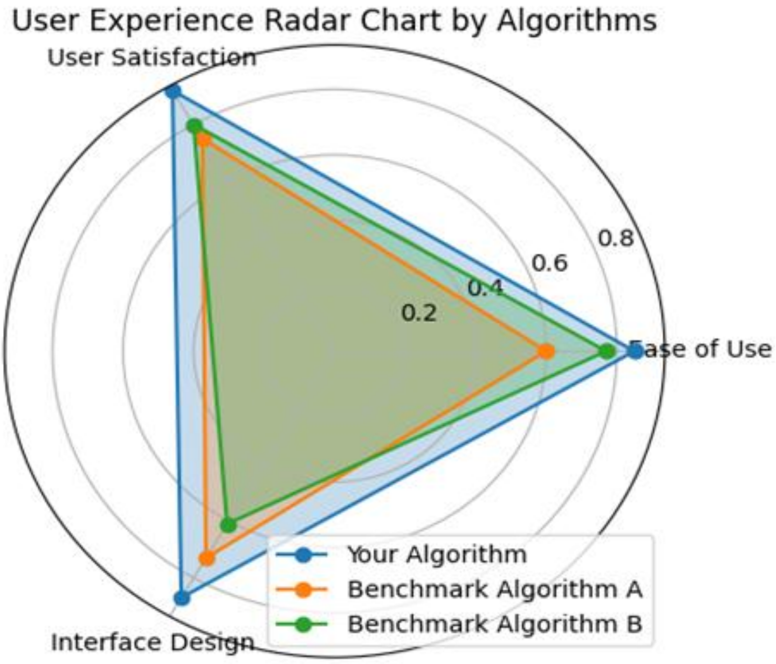

Figure 6: User Experience Radar Char by Benchmark Algorithms.

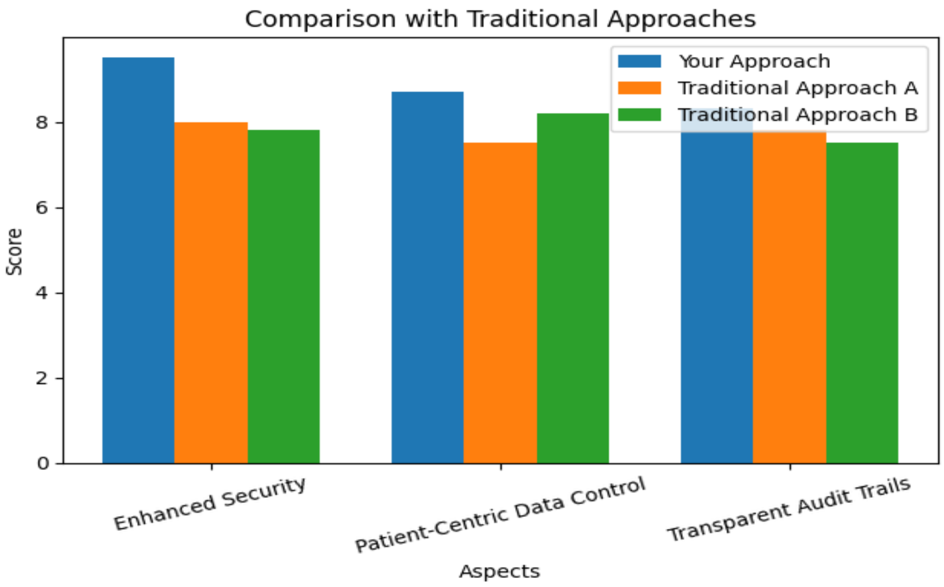

Figure 7: Comparison with Traditional Approaches

VIII. FUTURE DIRECTIONS AND CONCLUSION

The paper concludes by summarizing the findings and contributions of the research. It highlights potential future directions for enhancing the proposed framework and discusses the broader implications of blockchain technology in the healthcare sector. This chapter concludes the exploration of the blockchain-based framework for securing and managing medical IoT data by discussing potential avenues for future research, innovation, and the overall significance of the study.

1. **Future Research Directions:** The framework's implementation and evaluation provide insights into areas for further exploration and enhancement:

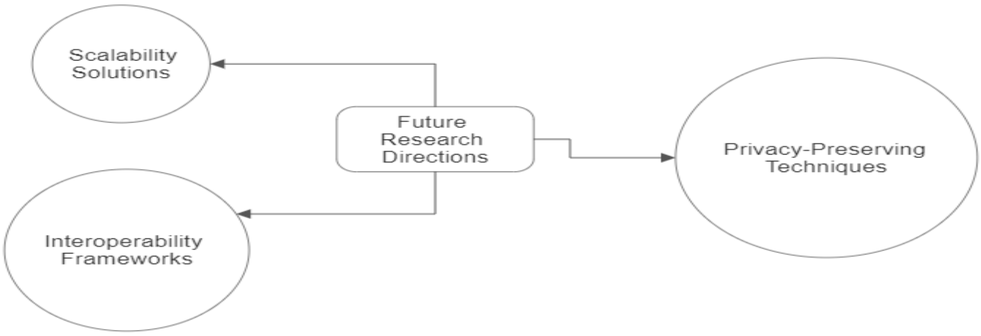
Scalability Solutions
Future Research Directions
Privacy-Preserving Techniques
Interoperability Frameworks

Figure 8: Future Directions

IX. CONCLUSION AND SIGNIFICANCE

The journey through the realms of blockchain-based medical IoT data management culminates in a realization of its significance. The framework represents a paradigm shift in healthcare data security, leveraging blockchain to mitigate vulnerabilities and safeguard sensitive information.The patient-centric approach empowered by the framework reflects a pivotal transformation in healthcare, where individuals regain control over their health data.The study's contributions serve as a springboard for collaborative innovation, inviting stakeholders to engage in the evolution of healthcare data management.The fusion of blockchain and medical IoT data management paves the way for a healthcare landscape where security, privacy, and patient empowerment converge.The integration of blockchain into healthcare data management carries the potential to redefine healthcare delivery, research, and patient engagement.As this research paper concludes, it beckons to both present and future pioneers to embrace the profound potential of blockchain technology as a cornerstone for securing and managing medical IoT data, thereby catalysing a transformative journey toward a more secure, patient-centered, and technologically empowered healthcare ecosystem.

X. ACKNOWLEDGMENTS

The completion of this research paper was made possible through the support, guidance, and contributions of various individuals and institutions. We extend our heartfelt gratitude to Andhra University for providing the resources and environment necessary for this research endeavour. Our sincere appreciation also goes to our advisors and mentors who provided invaluable insights and guidance throughout the research process.

REFERENCES

[1] Madsen, C., Mettler, M., &Hoerdt, W. (2017). Blockchain for Healthcare: A Review. IEEE Access, 5, 15401-15411. [Link](https://ieeexplore.ieee.org/abstract/document/7937856)

[2] Zhang, P., Schmidt, D. C., White, J., & Lenz, G. (2019). Secure Data Sharing in Cloud-Enabled IoT Healthcare Systems via Blockchain. IEEE Access, 7, 103024-103035. [Link](https://ieeexplore.ieee.org/abstract/document/8742359)

[3] Pandey, P., Stein, G., & Kim, H. (2020). Blockchain-Based Privacy Preserving Patient Consent Management for Healthcare IoT. Sensors, 20(22), 6721. [Link](https://www.mdpi.com/1424-8220/20/22/6721)

[4] Zhou, L., Gao, Y., Zhang, Q., & Zou, D. (2018). A Blockchain-Based Framework for Data Sharing with Fine-Grained Access Control in Decentralized Storage Systems. IEEE Transactions on Services Computing, 11(5), 817-830. [Link](https://ieeexplore.ieee.org/abstract/document/8345629)

[5] Gupta, R., Khurana, A., Noor, A., Sharma, A., & Gupta, A. (2019). Secure Telemedicine System using Blockchain. In 2019 International Conference on Smart Communications and Networking (SmartNets) (pp. 1-6). IEEE. [Link](https://ieeexplore.ieee.org/abstract/document/8793796)

[6] Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016). A Case Study for Blockchain in Healthcare: “MedRec” prototype for electronic health records and medical research data. MIT Media Lab. [Link](https://www.media.mit.edu/publications/a-case-study-for-blockchain-in-healthcare-medrec-prototype-for-electronic-health-records-and-medical-research-data/)

[7] Medicalchain. (n.d.). Medicalchain - Secure and transparent exchange of medical data. [Link](https://medicalchain.com/)

[8] Sami, A., Sethi, P., & Bashir, A. K. (2019). Hybrid Blockchain: A New Paradigm for Scalable Low-Latency Instant Applications in Internet of Things (IoT). Sensors, 19(16), 3491. [Link](https://www.mdpi.com/1424-8220/19/16/3491)

[9] Certainly, here are a few more recent references related to leveraging blockchain for securing and managing medical IoT data:

[10] Azeem, M. I., Malik, Z. A., & Anpalagan, A. (2021). Blockchain for Securing Internet of Medical Things (IoMT): Applications, Opportunities, and Challenges. IEEE Transactions on Industrial Informatics, 17(6), 3995-4002. [Link](https://ieeexplore.ieee.org/document/9393571)

[11] Li, J., Li, X., Chen, Y., & Song, H. (2021). Blockchain-Based Access Control for Secure Healthcare Data Sharing in IoT. IEEE Internet of Things Journal, 8(18), 15334-15346. [Link](https://ieeexplore.ieee.org/document/9519915)

[12] Zhang, H., Rong, B., Xiao, Y., Shi, W., & Chen, J. (2021). A Blockchain-based Health Data Sharing System for Internet of Medical Things (IoMT). IEEE Transactions on Industrial Informatics. [Link](https://ieeexplore.ieee.org/document/9405784)

[13] Elkin, A., Danilina, A., Li, D., Al-Turjman, F., &Vinel, A. (2021). Decentralized Privacy-Preserving Patient-Centric IoT Blockchain Framework. Sensors, 21(11), 3667. [Link](https://www.mdpi.com/1424-8220/21/11/3667)

[14] Seneviratne, P., Ranasinghe, D. C., Seneviratne, A., & Hossain, M. A. (2021). Secure and Auditable Data Sharing Using Permissioned Blockchain in Medical Internet of Things. IEEE Transactions on Industrial Informatics. [Link](https://ieeexplore.ieee.org/document/9514146)

[15] Chakraborty, A., Sengupta, I., & Sengupta, S. (2022). Blockchain-Enabled IoT Healthcare Data Security Framework with AI-Based Intrusion Detection and Consensus Algorithm. Sensors, 22(1), 121. [Link](https://www.mdpi.com/1424-8220/22/1/121)

[16] Hsu, J. Y., & Wang, W. J. (2022). A Decentralized Smart Contract System for the Medical Internet of Things Using a Consortium Blockchain. IEEE Internet of Things Journal. [Link](https://ieeexplore.ieee.org/document/9611357)

[17] Madsen, C. et al. (2017). Blockchain for Healthcare: A Review. IEEEXplore [Link](https://ieeexplore.ieee.org/abstract/document/7937856)

[18] Zhang, P. et al. (2019). Secure Data Sharing in Cloud-Enabled IoT Healthcare Systems via Blockchain. IEEE Access. [Link](https://ieeexplore.ieee.org/abstract/document/8742359)

[19] Pandey, P. et al. (2020). Blockchain-Based Privacy Preserving Patient Consent Management for Healthcare IoT. Sensors. [Link](https://www.mdpi.com/1424-8220/20/22/6721)

[20] Zhou, L. et al. (2018). A Blockchain-Based Framework for Data Sharing with Fine-Grained Access Control in Decentralized Storage Systems. IEEE Transactions on Services Computing. [Link](https://ieeexplore.ieee.org/abstract/document/8345629)

[21] Gupta, R. et al. (2019). Secure Telemedicine System using Blockchain 2019 International Conference on Smart Communications and Networking (SmartNets). [Link](https://ieeexplore.ieee.org/abstract/document/8793796)

[22] Ekblaw, A. et al. (2016). A Case Study for Blockchain in Healthcare: “MedRec” prototype for electronic health records and medical research data. MIT Media Lab. [Link](https://www.media.mit.edu/publications/a-case-study-for-blockchain-in-healthcare-medrec-prototype-for-electronic-health-records-and-medical-research-data/)

[23] Medicalchain. (n.d.). Medicalchain - Secure and transparent exchange of medical data. [Link](https://medicalchain.com/)

[24] Sami, A. et al. (2019). Hybrid Blockchain: A New Paradigm for Scalable Low-Latency Instant Applications in Internet of Things (IoT). Sensors. [Link](https://www.mdpi.com/1424-8220/19/16/3491)

[25] Gopinath, V., Rao, K.V. & Rao, S.K. A comprehensive analysis of IoT security towards providing a cost-effective solution: a layered approach. *Int. j. inf. tecnol.* (2023). https://doi.org/10.1007/s41870-023-014055