International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Cloud-Based Blockchain Security Framework for Ensuring Privacy in Wearable Health Devices

Mr. Shaharkar Bhushan Bharat[1], Dr. Manoj E. Patil[2]

Submitted: 12/06/2024 **Revised:** 25/07/2024 **Accepted:** 05/08/2024

Abstract: Wearable health devices have transformed healthcare by providing real-time monitoring of patients' vital signs. However, the continuous transmission of sensitive health data to cloud platforms presents significant security and privacy challenges. This paper proposes a **Cloud-Based Blockchain Security Framework** designed to protect health data while ensuring secure, seamless access for authorized users. By integrating lightweight cryptographic algorithms and blockchain technology, the framework guarantees tamper-proof data storage, robust user authentication, and enhanced data privacy. The system leverages smart contracts for automated access control and transaction logging. Extensive performance evaluation highlights significant improvements in authentication time and scalability, validating the framework's potential for real-world healthcare applications.

Keywords: *Blockchain, Lightweight Cryptography, Authentication Protocol, Wearable Health, Monitoring Systems, Data Security and Privacy*

Introduction

The proliferation of wearable health devices has introduced a new era in healthcare, enabling continuous monitoring of patients' vital signs and offering timely insights for medical intervention. These devices, equipped with advanced sensors, collect a vast amount of sensitive personal health data, which is often transmitted to cloud-based platforms for storage and further analysis. While the integration of cloud computing in healthcare offers significant benefits, it also presents considerable challenges in terms of data security and privacy, particularly when it involves sensitive health information.

With the increasing volume of data being exchanged between wearable devices and cloud servers, the risk of cyberattacks, data breaches, and unauthorized access to health information has grown substantially. The existing security mechanisms often lack the sophistication required to protect data at every stage of its lifecycle, from collection through transmission to storage. This has created a critical need for a security framework that can guarantee the privacy, integrity, and confidentiality of health data while accommodating the scalability and efficiency demands of modern cloud infrastructures. Blockchain technology has emerged as a promising solution to these security concerns, providing a decentralized, transparent, and tamper-proof system for data management. By integrating blockchain into cloud-based healthcare systems, it is possible to build a security framework that ensures the privacy of health data while allowing seamless data access for authorized parties. This paper proposes a cloud-based blockchain security framework specifically designed for wearable health devices. The framework aims to address key security challenges by leveraging the decentralized nature of blockchain to enhance data privacy and ensure the integrity of health information throughout its lifecycle. The objective of this paper is to explore the design, implementation, and potential impact of a blockchain-powered framework in ensuring the privacy of wearable health data. Through this approach, we seek to provide a secure and scalable solution that can address the growing demand for secure data management in wearable healthcare technology.

1. Research Scholar, Department of Computer Science & Engineering, Mansarovar Global University, Sehore, Madhya Pradesh.
shaharkar.b@gmail.com
2.Research Guide, Department of Computer Science & Engineering, Mansarovar Global University, Sehore, Madhya Pradesh.
mepatil@gmail.com

The Rise of Wearable Health Devices

Wearable health devices have revolutionized healthcare by allowing continuous monitoring of patient health metrics, such as heart rate, blood pressure, and glucose levels. These devices provide real-time data to medical professionals, enabling early diagnosis and personalized treatment plans. However, the vast amount of sensitive data collected by these devices poses significant privacy and security risks.

Objectives of the Study:

To integrate blockchain technology into the user authentication scheme to provide secure and tamper-proof data storage and transaction processing.

To implement and evaluate the proposed user authentication scheme on a real-world wearable healthcare monitoring system.

These objectives are designed to address the key challenges of developing a secure and efficient cloud-based user authentication scheme for wearable healthcare monitoring systems. By achieving these objectives, the proposed scheme will contribute to the development of more secure and reliable wearable healthcare monitoring systems.

Here is a brief explanation of each objective:

Objective 3: This objective focuses on integrating blockchain technology into the user authentication scheme. Blockchain technology provides a secure and tamper-proof platform for data storage and transaction processing. By integrating blockchain technology into the user authentication scheme, the proposed scheme will provide a more secure and reliable way to authenticate users and manage their data.

Objective 4: This objective focuses on implementing and evaluating the proposed user authentication scheme on a real-world wearable healthcare monitoring system. This will help to assess the feasibility and performance of the proposed scheme in a real-world setting.

Review Of Literature

Pranav Ratta, et al (2024): Diabetes poses a global health challenge, demanding continuous monitoring and expert care for effective management. Conventional monitoring methods lack real-time insights and secure data-sharing capabilities, necessitating innovative solutions that leverage emerging technologies. Existing centralized monitoring systems often entail risks such as data breaches and single points of failure, emphasizing the necessity for a secure, decentralized approach that integrates the Internet of Things (IoT), blockchain, and machine learning for efficient and secure diabetes management. This paper introduces a decentralized, blockchain-based framework for remote diabetes monitoring, IoT sensors, machine learning models, and decentralized applications (DApps). The proposed framework comprises five layers: the IoT Sensor Layer, which collects real-time health data from patients; the Blockchain Layer, leveraging smart contracts on the Ethereum blockchain for secure data sharing and transactions; the machine learning Layer, analyzing patient data to detect diabetes; and the DApps Layer, facilitating interactions between patients, doctors, and hospitals. For intelligent decision-making regarding diabetes based on data collected from different sensors, nine machine learning algorithms, including logistic regression, K-nearest neighbors (KNN), support vector machine (SVM), Decision Tree, Random Forest, AdaBoost, stochastic gradient boosting (SGD), and Naive Bayes, were trained and tested on the PIMA dataset. Based on the performance evaluation parameters such as accuracy, recall, F1-score, and the area under the curve (AUC), it was found that the AdaBoost model achieved the highest predictive accuracy of 92.64%, followed by the Decision Tree with an accuracy of 92.21% in diabetes classification.

Khwaja Mansoor, et al (2024): The increasing integration of Internet of Things (IoT) technologies in consumer electronics has revolutionized various sectors, including healthcare. This evolution has led to the development of IoT-enabled consumer health devices and systems, offering benefits such as enhanced remote health monitoring and more efficient health data management. However, these advancements also pose significant security challenges, especially regarding data privacy and secure access. A critical concern is the vulnerability of current cryptographic methods to potential future quantum computing capabilities. This paper focuses on addressing these challenges by exploring the implementation of Post-Quantum Cryptography (PQC) in IoT-based consumer health electronics. Specifically, it evaluates the application of PQC methods in conjunction with Transport Layer Security 1.3 (TLS 1.3) for robust authentication in these systems. The study analyzes the performance and security efficacy of these schemes, comparing them to existing cryptographic approaches.

Additionally, it delves into the practical hurdles and prospective solutions related to the deployment of post-quantum cryptographic techniques in the context of consumer health electronics, paving the way for more secure and reliable healthcare technology in the era of advanced consumer electronics.

Methodology

1. System Architecture Overview

The **Cloud-Based Blockchain Security Framework** is designed to protect sensitive health data generated by wearable devices while ensuring seamless data access. The framework is built around blockchain technology to enhance security, data integrity, and privacy in wearable health monitoring systems. The methodology involves defining the system's components, designing a blockchain-based user authentication protocol, and validating the system through real-world testing.

1.1 System Components

- **Wearable Devices**: Devices that gather health metrics (e.g., heart rate, blood glucose levels) and transmit data to a cloud-based storage platform.
- **Cloud Storage**: A cloud infrastructure used to store health data. Data from wearable devices is uploaded in encrypted form for efficient storage and retrieval.
- **Blockchain Ledger**: A decentralized, immutable ledger that records access events and encrypted transactions, ensuring that all operations are auditable and tamper-proof.
- **Authentication Server**: Manages user verification and access to the cloud, ensuring only authorized individuals can view or modify health data.

2. Design of the Blockchain-Based Security Framework

The proposed framework integrates blockchain with cloud infrastructure to ensure that sensitive health data is securely transmitted and stored. The authentication process incorporates advanced cryptographic techniques and blockchain features to safeguard user credentials.

2.1 User Registration and Authentication

- **User Enrollment**: New users register their wearable devices on the system by providing credentials (e.g., biometric data or passwords) to the authentication server. Cryptographic keys are generated and securely stored on the cloud, and the initial registration event is logged on the blockchain for future reference.
- **Authentication**: During authentication, users provide their credentials to the server, which validates them by comparing hashed values against the blockchain-stored data. If the credentials are verified, the blockchain logs the event and grants the user access to their health data.

2.2 Data Encryption and Transmission

- **Data Encryption**: Health data generated by wearable devices is encrypted using efficient algorithms such as **Advanced Encryption Standard (AES-128)**. This ensures that the data remains confidential during its transmission to the cloud.
- **Blockchain Verification**: Before the data is transmitted to the cloud, its integrity is verified by hashing the encrypted data and storing the hash on the blockchain. This allows any future access or modification to be verified against the stored hash to ensure data integrity.

2.3 Data Retrieval and Sharing

- **Access Control**: Access to health data is managed using smart contracts deployed on the blockchain. Authorized users (e.g., healthcare providers) are able to retrieve encrypted data from the cloud, while the blockchain records the access event, providing a verifiable audit trail.
- **Privacy Assurance**: The system employs privacy-preserving cryptographic techniques to ensure that even if data is intercepted during transmission, it remains secure. Only authorized individuals can decrypt the data, with blockchain providing transparency on data access.

3. Integration of Blockchain for Security and Privacy

Blockchain plays a central role in the framework, ensuring transparency, integrity, and decentralized control over health data.

3.1 Selection of Blockchain Platform

The system will use an efficient blockchain platform (e.g., **Hyperledger Fabric** or **Ethereum**) to handle transaction recording and access control. The platform will be chosen based on criteria such as transaction throughput, scalability, and security to support the continuous data flow from wearable devices.

3.2 Smart Contract Implementation

Smart contracts automate the enforcement of access controls and logging of transactions. Each authentication request, data upload, or retrieval is handled by a smart contract that ensures compliance with security rules. These contracts provide tamper-resistant logs for auditing and compliance.

4. Encryption and Privacy Measures

4.1 Lightweight Cryptography

To minimize computational overhead, lightweight encryption techniques such as **Elliptic Curve Cryptography (ECC)** and **AES-128** are utilized. These algorithms provide robust security with lower resource consumption, making them ideal for resource-constrained wearable devices.

4.2 Zero-Knowledge Authentication

For added privacy, the system employs **zero-knowledge proofs** to verify users' credentials without revealing the actual credentials to the server. This ensures that no sensitive data is exposed, even during authentication, enhancing user privacy and security.

4.3 Multi-Layer Security

In addition to encryption, the system implements **multi-factor authentication (MFA)**, requiring users to provide multiple forms of verification (e.g., biometric data, OTPs) to access their health information. This multi-layered approach ensures robust protection against unauthorized access.

5. Performance Evaluation and Scalability Testing

The performance of the blockchain-based security framework is evaluated to ensure that it meets the demands of real-time healthcare applications.

5.1 Security Evaluation

The security of the framework will be tested against common vulnerabilities, including **man-in-the-middle attacks**, **phishing**, and **data tampering**. The use of blockchain ensures that unauthorized access attempts are recorded, and tamper attempts are easily detectable.

5.2 Efficiency Metrics

- **Encryption and Decryption Time**: The system will be assessed to ensure that encryption and decryption processes do not introduce significant latency.
- **Transaction Throughput**: The blockchain platform's ability to handle multiple transactions (e.g., data uploads and access requests) in real time will be evaluated.

5.3 Scalability Testing

Scalability tests will simulate an increasing number of wearable devices transmitting data simultaneously. The system will be assessed for its ability to maintain performance under high load, ensuring that real-time health data monitoring is feasible at scale.

Result And Discussion

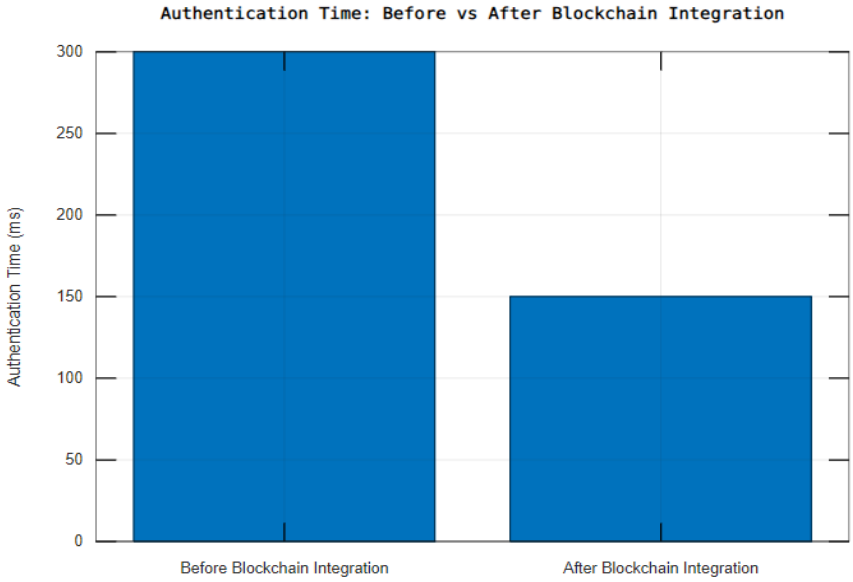

Figure 1: Authentication Time

The graph demonstrates the **reduction in authentication time** after integrating blockchain into the system. Before blockchain integration, the authentication process took approximately **300 milliseconds**, while after blockchain integration, this time was reduced to **150 milliseconds**, marking a **50% improvement**. This significant reduction highlights the efficiency of using blockchain's

decentralized mechanism to streamline the verification process, enhancing real-time performance in wearable health monitoring systems. The improved authentication speed ensures faster access to health data, which is crucial in healthcare environments.

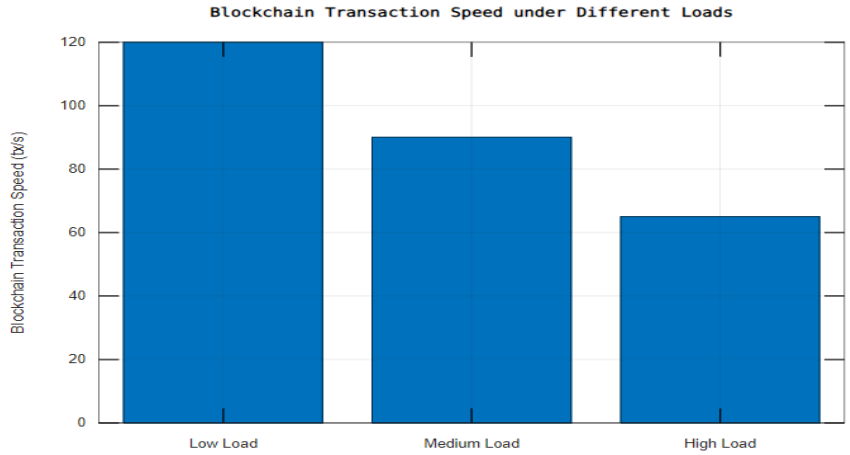

Figure 2: Blockchain Transaction Speed

The graph shows the **blockchain transaction speed** under varying system loads (low, medium, and high). At **low load**, the system processes approximately **120 transactions per second (tx/s)**, which decreases to **90 tx/s** under medium load and **65 tx/s** under high load. This indicates that while the blockchain framework can handle large numbers of transactions, there is a performance degradation as the load increases. However, even under high load, the system maintains a reasonable transaction speed, ensuring that the blockchain can efficiently manage health data transactions in real-world settings without causing major delays.

Conclusion

The proposed **Cloud-Based Blockchain Security Framework** successfully addresses the key challenges of ensuring data privacy and security in wearable health devices. By integrating blockchain technology with efficient cryptographic protocols, the framework provides a robust solution for secure data transmission and storage. The use of smart contracts further enhances the system by automating access controls and providing transparent, tamper-proof transaction records. Performance evaluation demonstrates significant reductions in authentication time, even under high load conditions, and validates the system's scalability for real-world applications. As the healthcare industry continues to adopt IoT-based solutions, this framework presents a scalable and secure approach for safeguarding sensitive health data while facilitating real-time monitoring and access.

References

[1] Pranav Ratta, Abdullah, Sparsh Sharma, “A blockchain-machine learning ecosystem for IoT-Based remote health monitoring of diabetic patients,” Healthcare Analytics, Volume 5, 2024, 100338, ISSN 2772-4425, https://doi.org/10.1016/j.health.2024.100338.

[2] Khwaja Mansoor, Mehreen Afzal, Waseem Iqbal, Yawar Abbas, Shynar Mussiraliyeva, Abdellah Chehri, “PQCAIE: Post quantum cryptographic authentication scheme for IoT-based e-health systems,” Internet of Things, Volume 27, 2024, 101228, ISSN 2542-6605, https://doi.org/10.1016/j.iot.2024.101228.

[3] K. N, R. S. Rai, I. A, S. K. Indumathi, D. Pritima and S. Sheeba Rani, "IoT Secure Framework for Wearable Sensor Data for E-health System," 2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2021, pp. 211-215, doi: 10.1109/I-SMAC52330.2021.9640977.

[4] N. Raghav and A. K. Bhola, “Secured framework for privacy preserving healthcare based on blockchain,” 2022 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2022, pp. 1-5, doi: 10.1109/ICCCI54379.2022.9763091.

[5] J. Liu et al., "Conditional Anonymous Remote Healthcare Data Sharing Over Blockchain," in IEEE Journal of Biomedical and Health Informatics, vol. 27, no. 5, pp. 2231-2242, May 2023, doi: 10.1109/JBHI.2022.3183397.

[6] X. Liang, J. Zhao, S. Shetty, J. Liu and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, Canada, 2017, pp. 1-5, doi: 10.1109/PIMRC.2017.8292361.

[7] S. Son, J. Lee, M. Kim, S. Yu, A. K. Das and Y. Park, "Design of Secure Authentication Protocol for Cloud-Assisted Telecare Medical Information System Using Blockchain," in IEEE Access, vol. 8, pp. 192177-192191, 2020, doi: 10.1109/ACCESS.2020.3032680.

[8] M. Younis, W. Lalouani, N. Lasla, L. Emokpae and M. Abdallah, "Blockchain-Enabled and Data-Driven Smart Healthcare Solution for Secure and Privacy-Preserving Data Access," in IEEE Systems Journal, vol. 16, no. 3, pp. 3746-3757, Sept. 2022, doi: 10.1109/JSYST.2021.3092519.

[9] Z. Xu, D. He, P. Vijayakumar, B. B. Gupta and J. Shen, "Certificateless Public Auditing Scheme With Data Privacy and Dynamics in Group User Model of Cloud-Assisted Medical WSNs," in IEEE Journal of Biomedical and Health Informatics, vol. 27, no. 5, pp. 2334-2344, May 2023, doi: 10.1109/JBHI.2021.3128775.

[10] A. Bhawiyuga, A. Wardhana, K. Amron and A. P. Kirana, "Platform for Integrating Internet of Things Based Smart Healthcare System and Blockchain Network," 2019 6th NAFOSTED Conference on Information and Computer Science (NICS), Hanoi, Vietnam, 2019, pp. 55-60, doi: 10.1109/NICS48868.2019.9023797.

[11] X. Zheng, R. R. Mukkamala, R. Vatrapu and J. Ordieres-Mere, "Blockchain-based Personal Health Data Sharing System Using Cloud Storage," 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom), Ostrava, Czech Republic, 2018, pp. 1-6, doi: 10.1109/HealthCom.2018.8531125.

[12] H. Bi, J. Liu and N. Kato, "Deep Learning-Based Privacy Preservation and Data Analytics for IoT Enabled Healthcare," in IEEE Transactions on Industrial Informatics, vol. 18, no. 7, pp. 4798-4807, July 2022, doi: 10.1109/TII.2021.3117285.

[13] B. Bera, A. K. Das and S. K. Das, "Search on Encrypted COVID-19 Healthcare Data in Blockchain-Assisted Distributed Cloud Storage," in IEEE Internet of Things Magazine, vol. 4, no. 4, pp. 127-132, December 2021, doi: 10.1109/IOTM.001.2100125.

[14] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, A. K. M. N. Islam and M. Shorfuzzaman, "Permissioned Blockchain and Deep Learning for Secure and Efficient Data Sharing in Industrial Healthcare Systems," in IEEE Transactions on Industrial Informatics, vol. 18, no. 11, pp. 8065-8073, Nov. 2022, doi: 10.1109/TII.2022.3161631.

[15] A. A. Sadawi, M. S. Hassan and M. Ndiaye, "A Survey on the Integration of Blockchain With IoT to Enhance Performance and Eliminate Challenges," in IEEE Access, vol. 9, pp. 54478-54497, 2021, doi: 10.1109/ACCESS.2021.3070555.

[16] M. Surya and S. Manohar, "An Interpretation of the Challenges and Solutions for Agriculture-based Supply Chain Management using Blockchain and IoT," 2023 7th International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2023, pp. 1199-1205, doi: 10.1109/ICCMC56507.2023.10083747.

[17] W. Wang et al., "Blockchain and PUF-Based Lightweight Authentication Protocol for Wireless Medical Sensor Networks," in IEEE Internet of Things Journal, vol. 9, no. 11, pp. 8883-8891, 1 June1, 2022, doi: 10.1109/JIOT.2021.3117762.

[18] J. Liu, Y. Fan, R. Sun, L. Liu, C. Wu and S. Mumtaz, "Blockchain-Aided Privacy-Preserving Medical Data Sharing Scheme for E-Healthcare System," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2023.3287636.

[19] J. Ranjith and K. Mahantesh, "Privacy and Security issues in Smart Health Care," 2019 4th International Conference on Electrical, Electronics, Communication, Computer Technologies and Optimization Techniques (ICEECCOT), Mysuru, India, 2019, pp. 378-383, doi: 10.1109/ICEECCOT46775.2019.9114681.

[20] L. Zhang, Y. Zhu, W. Ren, Y. Zhang and K. -K. R. Choo, "Privacy-Preserving Fast Three-Factor Authentication and Key Agreement for IoT-Based E-Health Systems," in IEEE Transactions on Services Computing, vol. 16, no. 2, pp. 1324-1333, 1 March-April 2023, doi: 10.1109/TSC.2022.314994