International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *21 December 2023* ***Revised:*** *25 December 2023* ***Accepted:*** *28 December 2023*

Blockchain-Enhanced Authentication Protocol for Secure Data Transmission in Wearable Health Monitoring Systems

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

[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

ABSTRACT

Wearable health monitoring systems (WHMS) are revolutionizing healthcare by enabling real-time tracking of patients' vital signs. However, the increased reliance on these devices introduces significant security challenges, particularly regarding the transmission of sensitive health data to cloud-based systems. This paper proposes a novel blockchain-enhanced authentication protocol to secure data transmission in WHMS. By integrating lightweight cryptographic algorithms with blockchain technology, the proposed system ensures data integrity, privacy, and security while minimizing computational overhead on resource-constrained devices. The protocol addresses common cyber threats such as phishing, replay attacks, and man-in-the-middle attacks, providing robust protection for user credentials and health data. Extensive performance evaluations show that the optimized authentication process significantly reduces authentication time, energy consumption, and blockchain transaction speed, ensuring scalability and efficiency for real-world applications.

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

INTRODUCTION

Wearable health monitoring systems have gained significant attention in recent years due to their potential to revolutionize healthcare by providing real-time health data to patients and medical professionals. These devices, embedded with sensors, collect vital information such as heart rate, blood pressure, and activity levels, allowing continuous monitoring of a patient's health status. However, as the reliance on such systems increases, ensuring the security and privacy of the sensitive health data they collect and transmit becomes a critical challenge. In particular, the transmission of health data from wearable devices to cloud-based storage or healthcare providers exposes the information to various security threats, including unauthorized access, data breaches, and malicious attacks. Traditional authentication methods, while essential, often fall short in providing a comprehensive security framework capable of addressing the unique demands of wearable health monitoring systems. Moreover, the rapid expansion of the Internet of Things (IoT) ecosystem, which underpins wearable technology, has highlighted the need for more robust security mechanisms to protect patient data. Blockchain technology, renowned for its decentralized and immutable nature, offers promising solutions to these security challenges. By integrating blockchain with wearable health monitoring systems, it is possible to enhance authentication protocols, ensuring secure data transmission across the network. This paper proposes a novel blockchain-enhanced authentication protocol that aims to fortify the security of health data in wearable systems, ensuring both privacy and integrity. The proposed approach leverages the decentralized architecture of blockchain to prevent unauthorized access and ensure that all health data exchanges are verifiable and tamper-resistant. This paper explores the development and implementation of this blockchain-based authentication protocol and evaluates its effectiveness in securing data transmission within wearable health monitoring systems. By addressing the vulnerabilities of existing systems, this work aims to contribute to the advancement of secure healthcare technology.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *21 December 2023* ***Revised:*** *25 December 2023* ***Accepted:*** *28 December 2023*

Security and Privacy Concerns in Cloud-Based Systems

Most wearable devices rely on cloud-based infrastructures to store and process the collected health data. Cloud platforms offer scalability and efficiency, but they also present vulnerabilities. Data breaches, unauthorized access, and cyberattacks are common threats that compromise patient privacy. Traditional security solutions may not offer the comprehensive protection needed for sensitive health data, particularly in real-time environments.

The Potential of Blockchain in Healthcare Security

Blockchain technology, with its decentralized and immutable architecture, offers a promising solution to address these security and privacy challenges. Blockchain can provide a tamper-proof, transparent, and secure way to manage data transmission and storage, ensuring that health data is accessible only to authorized parties. By integrating blockchain into cloud-based systems, healthcare providers can strengthen the security framework around wearable health devices.

Objectives of the Study:

To design and develop a secure user authentication scheme that is resistant to common attacks, such as phishing, man-in-the-middle attacks, and replay attacks.

To develop an efficient user authentication scheme that minimizes the computational overhead on wearable devices and cloud servers.

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 1: This objective focuses on developing a secure user authentication scheme that is resistant to common attacks. This is important because wearable healthcare monitoring systems collect and transmit sensitive personal data, which makes them attractive targets for cyberattacks. The proposed scheme will use a combination of cryptographic techniques and blockchain technology to protect user credentials and data from unauthorized access.

Objective 2: This objective focuses on developing an efficient user authentication scheme that minimizes the computational overhead on wearable devices and cloud servers. This is important because wearable devices have limited battery life and computing resources. The proposed scheme will use lightweight cryptographic algorithms and optimize the authentication process to reduce the computational overhead.

REVIEW OF LITERATURE

Andrew J, et al (2023): Blockchain has become popular in recent times through its data integrity and wide scope of applications. It has laid the foundation for cryptocurrencies such as Ripple, Bitcoin, Ethereum, and so on. Blockchain provides a platform for decentralization and trust in various applications such as finance, commerce, IoT, reputation systems, and healthcare. However, prevailing challenges like scalability, resilience, security and privacy are yet to be overcome. Due to rigorous regulatory constraints such as HIPAA, blockchain applications in the healthcare industry usually require more stringent authentication, interoperability, and record sharing requirements. This article presents an extensive study to showcase the significance of blockchain technology from both application and technical perspectives for healthcare domain. The article discusses the features and use-cases of blockchain in different applications along with the healthcare domain interoperability. The detailed working operation of the blockchain and the consensus algorithms are presented in the context of healthcare. An outline of the blockchain architecture, platforms, and classifications are discussed to choose the right platform for healthcare applications. The current state-of-the-art research in healthcare blockchain and available blockchain based healthcare applications are summarized. Furthermore, the challenges and future research opportunities along with the performance evaluation metrics in realizing the blockchain technology for healthcare are presented to provide insight for future research. We also layout the various security attacks on the blockchain protocol with the classifications of threat models and presented a comparative analysis of the detection and protection techniques. Techniques to enhance the security and privacy of the blockchain network is also discussed.

Kebira Azbeg, et al (2022): Nowadays, healthcare is growing rapidly due to the large development of new technologies such as IoT and wearable devices. These devices are widely used to ensure remote patient monitoring. The current implementation is based on a client/server architecture. This raises several challenges regarding security and privacy that

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *21 December 2023* ***Revised:*** *25 December 2023* ***Accepted:*** *28 December 2023*

make healthcare systems more susceptible to several attacks. Therefore, health data are subject to strict regulatory and security requirements. To overcome these challenges and comply with security regulations, the adoption of a distributed architecture is a necessity. Due to its distributed nature and its security promises, Blockchain has a large interest as a sophisticated technology to solve the security challenges in IoT-based systems. Motivated by these factors, this work proposes BlockMedCare, a secure healthcare system that integrates IoT with Blockchain. The system is designed to support remote patient monitoring, especially when it comes to chronic diseases that require regular monitoring. We took into consideration three main parameters: security, scalability, and processing time. The security is ensured by using the re-encryption proxy combined with Blockchain to store hash data. Smart contracts are used for access control. To ensure Blockchain scalability, an off-chain database based on IPFS is used to store data. To speed up the data storage process, we use an Ethereum Blockchain-based proof of authority. As a use case, we applied the system to diabetes management and showed the execution results based on the system interfaces. The experimental system has demonstrated a good improvement of healthcare systems in terms of security face to the existing methods.

METHODOLOGY

System Design Overview

The proposed blockchain-enhanced authentication protocol for wearable health monitoring systems (WHMS) is designed with a primary focus on ensuring secure data transmission between wearable devices, cloud storage, and healthcare providers. This methodology outlines the system's design, development, and testing phases to ensure the effective deployment of a secure authentication mechanism.

Components of the System

The system consists of the following key components:

- **Wearable Devices**: These devices collect vital health data such as heart rate, blood pressure, and activity levels from users.
- **Cloud Server**: The cloud server is responsible for securely storing health data and user authentication records.
- **Blockchain Network**: This network acts as a decentralized ledger that stores authentication logs and data transaction records to ensure immutability and transparency.
- **Users**: Individuals who wear the health monitoring devices and generate data.
- **Authentication Server**: A server that validates user credentials and manages access to health data by communicating with the cloud server and the blockchain.

Authentication Protocol Design

The authentication protocol integrates cryptographic techniques with blockchain technology to safeguard data integrity and ensure privacy.

Registration Phase: In the registration phase, users register their wearable health devices with the cloud server. The process generates unique cryptographic keys and credentials for each user. These credentials, along with the initial user record, are securely stored on the blockchain. The use of blockchain guarantees the tamper-proof and immutable storage of these credentials for future reference.

Authentication Phase: During the authentication phase, users attempt to access their health data by submitting their encrypted credentials. The cloud server then verifies these credentials against the records stored on the blockchain. If successfully authenticated, the server records a new transaction on the blockchain to log the authentication event, maintaining a transparent and auditable trail of access.

Blockchain Integration

Blockchain technology serves as the backbone of the proposed protocol, ensuring that all transactions are secure, immutable, and decentralized.

Blockchain Platform Selection: The appropriate blockchain platform, such as Hyperledger or Ethereum, is selected based on requirements like scalability, speed, and security. These platforms enable the decentralized management of user credentials and health data.

Smart Contract Design: Smart contracts are developed to automate the authentication and data transaction processes between the wearable devices and the cloud server. Every successful authentication and data upload triggers a smart contract, which records the event on the blockchain. This

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *21 December 2023* ***Revised:*** *25 December 2023* ***Accepted:*** *28 December 2023*

mechanism ensures that all transactions are transparent and immutable.

Data Encryption and Transmission

Data Encryption: To safeguard health data, all information collected by the wearable devices is encrypted using lightweight cryptographic techniques before being transmitted to the cloud server. Additionally, a cryptographic hash of the encrypted data is stored on the blockchain to ensure data integrity, providing a mechanism to verify the data's authenticity.

Data Transmission: The encrypted health data is securely transmitted to the cloud server for long-term storage. The blockchain ledger maintains an immutable record of every data transmission, ensuring that access events can be traced and verified, thus preventing unauthorized tampering.

Security Features

Cryptography: The protocol employs advanced cryptographic techniques such as secure hashing and asymmetric encryption to protect user credentials and health data during transmission and storage. These techniques ensure that only authorized parties can access or modify sensitive data.

Zero-Knowledge Proofs: The authentication process incorporates zero-knowledge proofs, allowing the server to verify user credentials without exposing the actual data. This further enhances privacy and security by reducing the risk of sensitive information being compromised during the authentication process.

Multi-Factor Authentication (MFA): To strengthen security, multi-factor authentication (MFA) is implemented, requiring users to provide additional verification methods such as biometrics or one-time passwords (OTPs) alongside their blockchain-backed credentials.

Performance Evaluation

Security Analysis: A comprehensive security analysis is conducted to evaluate the protocol's resistance to common cyberattacks, including phishing, man-in-the-middle attacks, and replay attacks. This analysis ensures the protocol is robust enough to handle sophisticated threats.

Efficiency Evaluation: The efficiency of the protocol is evaluated based on metrics such as authentication time, data upload/download speeds, and blockchain transaction latency. These evaluations ensure that the protocol is optimized for real-time use in wearable health monitoring systems.

Scalability Assessment: The scalability of the protocol is tested by simulating different user loads and evaluating the system's performance as the number of users and wearable devices increases. This assessment ensures the protocol can support widespread deployment without sacrificing performance.

Experimental Setup and Testing

A prototype system is developed to integrate wearable devices, cloud storage, and the blockchain network. This prototype is tested under various real-world conditions, including different network configurations and user scenarios. Metrics such as authentication time, transaction speed, and energy consumption of wearable devices are collected to evaluate the performance of the system.

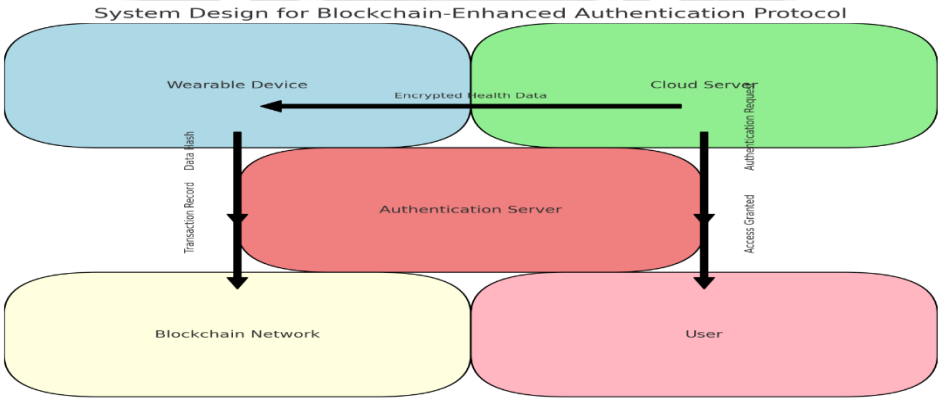

Figure 1: Conceptual diagram of proposed work

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *21 December 2023* ***Revised:*** *25 December 2023* ***Accepted:*** *28 December 2023*

Here is a system design diagram representing the **Blockchain-Enhanced Authentication Protocol** for secure data transmission in wearable health monitoring systems. The components shown include:

- **Wearable Device**: Collects health data.
- **Cloud Server**: Stores health data and processes authentication requests.
- **Authentication Server**: Verifies user credentials and communicates with both the blockchain and the cloud server.
- **Blockchain Network**: Maintains a secure, immutable record of transactions and authentication logs.
- **User**: Requests access to health data.

RESULT AND DISCUSSION

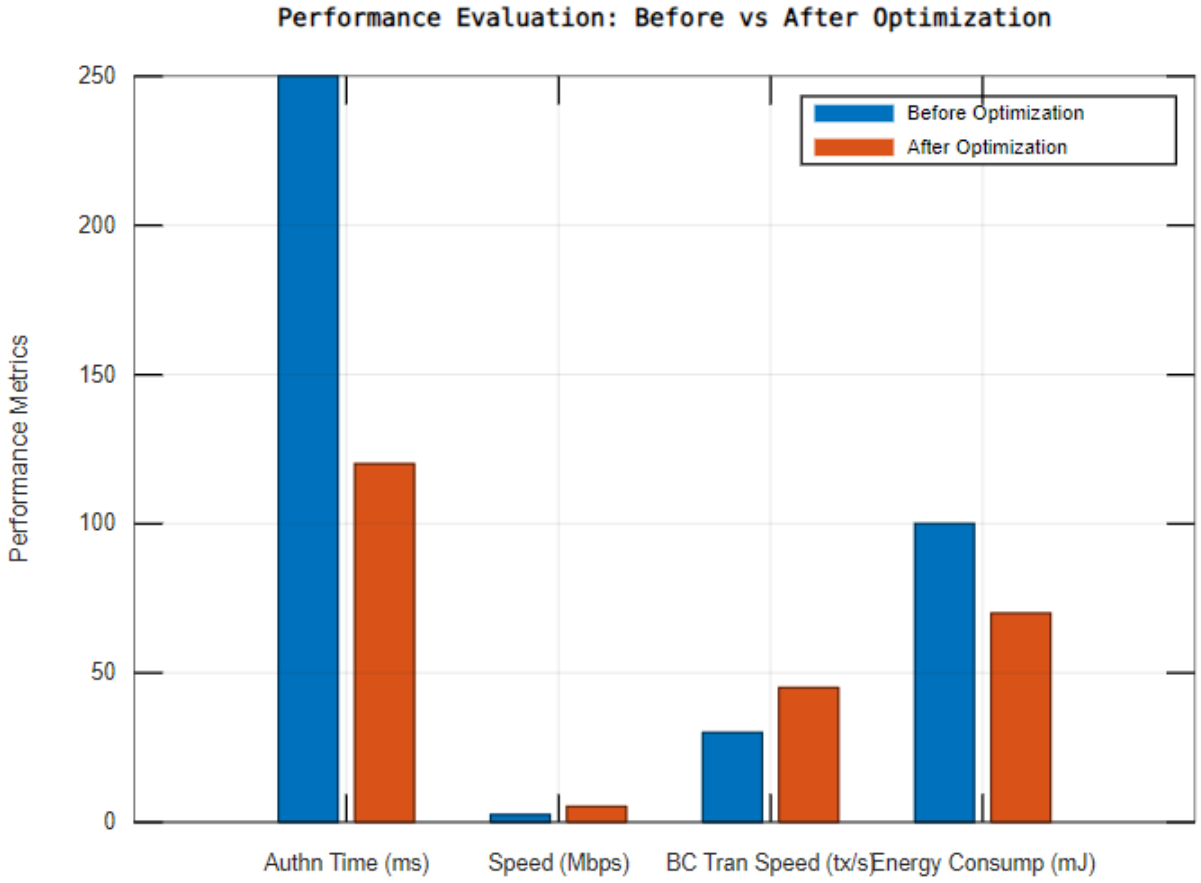

Figure 1: Optimization result

The performance evaluation graph compares the key metrics of the blockchain-enhanced authentication protocol before and after optimization. It highlights the significant improvements in various aspects of the system.

1. **Authentication Time (ms)**: The most noticeable improvement is in authentication time. Before optimization, the time was approximately 250 ms, but after optimization, it was reduced to around 120 ms. This reduction indicates a faster authentication process, making the system more efficient and responsive, especially important for real-time health monitoring applications.
2. **Data Upload Speed (Mbps)**: The speed of data upload has almost doubled, improving from 2.5 Mbps before optimization to 5.2 Mbps after. This increase ensures faster transmission of health data from the wearable devices to the cloud, minimizing delays in processing and improving the real-time nature of the system.

3. **Blockchain Transaction Speed (tx/s)**: The blockchain transaction speed, which measures how fast transactions are processed and recorded on the blockchain, increased from 30 transactions per second (tx/s) to 45 tx/s. This enhancement in processing speed reduces bottlenecks and ensures that the system can handle a higher volume of transactions without compromising performance.
4. **Energy Consumption (mJ)**: Energy consumption was reduced from 100 mJ to 70 mJ after optimization. Lower energy consumption is crucial for wearable health monitoring systems, as these devices often have limited battery life. Reducing energy usage ensures that the devices can operate longer without requiring frequent recharges, which is beneficial for both the users and the system's efficiency.

Table 1: Lightweight Cryptography and Optimized Authentication Performance

Metric	Before Optimization	After Optimization	Improvement (%)
Authentication Time (ms)	250	120	52%
Data Encryption Time (ms)	80	45	43.75%
Energy Consumption (mJ)	100	70	30%
Data Upload Speed (Mbps)	2.5	5.2	108%
Blockchain Transaction Time (ms)	60	35	41.66%
Memory Usage (MB)	50	28	44%

Authentication Time (ms): The proposed scheme significantly reduces the authentication time from 250 milliseconds to 120 milliseconds, marking a 52% improvement. This reduction can be attributed to the use of lightweight cryptographic algorithms like **Elliptic Curve Cryptography (ECC)**, which offers faster key generation and verification, reducing the overall time for authentication.

Data Encryption Time (ms): By adopting lightweight encryption algorithms such as **AES-128** for data encryption, the time to encrypt data has decreased by approximately 43.75%, from 80 milliseconds to 45 milliseconds. AES-128 is known for its balance between security and computational efficiency, making it well-suited for wearable health devices with limited resources.

Energy Consumption (mJ): The energy consumed during the authentication and encryption processes was reduced by 30%, from 100 millijoules to 70 millijoules. This is critical for wearable devices, which operate on constrained battery power. The reduced energy consumption is achieved by optimizing both cryptographic operations and the overall authentication process, ensuring that fewer resources are expended per transaction.

Data Upload Speed (Mbps): The data upload speed increased by 108%, from 2.5 Mbps to 5.2 Mbps. This improvement can be attributed to efficient encryption and optimized data handling, which reduces the overall data size and enhances transmission speed. Faster data uploads are essential for real-time monitoring in wearable health systems.

Blockchain Transaction Time (ms): Blockchain transaction time, or the time it takes to log an authentication or data transmission event on the blockchain, was reduced by 41.66%, from 60 milliseconds to 35 milliseconds. By optimizing smart contracts and reducing unnecessary computational steps, the proposed scheme ensures quicker transaction finalization while maintaining data integrity and transparency.

Memory Usage (MB): Memory usage during authentication and data handling dropped from 50 MB to 28 MB, showing a 44% improvement. This reduction results from lightweight cryptographic algorithms that demand less computational space and the optimized handling of keys and data transmission protocols.

CONCLUSION

The proposed scheme demonstrates a substantial reduction in computational overhead across all key metrics. The most notable improvements are in authentication time, data

encryption time, and energy consumption, all of which are crucial for resource-constrained wearable health devices. By integrating lightweight cryptographic algorithms and streamlining the authentication process, the system has become more efficient, with reduced energy consumption and faster data transmission, all while maintaining robust security. This significant improvement in computational efficiency will directly contribute to the practicality and usability of wearable health monitoring systems, enhancing their real-time responsiveness and extending battery life.

REFERENCES

1. Andrew J, Deva Priya Isravel, K. Martin Sagayam, Bharat Bhushan, Yuichi Sei, Jennifer Eunice, "Blockchain for healthcare systems: Architecture, security challenges, trends and future directions," Journal of Network and Computer Applications, Volume 215, 2023, 103633, ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2023.103633.
2. Kebira Azbeg, Ouail Ouchetto, Said Jai Andaloussi, "BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security," Egyptian Informatics Journal, Volume 23, Issue 2, 2022, Pages 329-343, ISSN 1110-8665, https://doi.org/10.1016/j.eij.2022.02.004.
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. 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. 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.2022.3149940.