An Approach Towards the Security Management for Sensitive Medical Data in the IoMT Ecosystem

Pushpita Chatterjee*
Department of EE and CS
Howard University
Washington, DC, USA
pushpita.c@ieee.org

Debashis Das
Department of CSE
Narula Institute of Technology
Agarpara, West Bengal, India
debashis.das@ieee.org

Sourav Banerjee
Department of CSE
Kalyani Govt. Engineering College
Kalyani, West Bengal, India
mr.sourav.banerjee@ieee.org

Uttam Ghosh
Department of CS and DS
Meharry Medical College
Nashville, TN, USA
ghosh.uttam@ieee.org

Armando B. Mpembele
Department of CS
Tennessee State University
Nashville, TN, USA
ampembel@tnstate.edu

Tamara Rogers
Department of CS
Tennessee State University
Nashville, TN, USA
trogers@tnstate.edu

ABSTRACT

The Internet of Medical Things (IoMT) is a network of interconnected medical devices, wearables, and sensors integrated into healthcare systems. It enables real-time data collection and transmission using smart medical devices with trackers and sensors. IoMT offers various benefits to healthcare, including remote patient monitoring, improved precision, and personalized medicine, enhanced healthcare efficiency, cost savings, and advancements in telemedicine. However, with the increasing adoption of IoMT, securing sensitive medical data becomes crucial due to potential risks such as data privacy breaches, compromised health information integrity, and cybersecurity threats to patient information. It is necessary to consider existing security mechanisms and protocols and identify vulnerabilities. The main objectives of this paper aim to identify specific threats, analyze the effectiveness of security measures, and provide a solution to protect sensitive medical data. In this paper, we propose an innovative approach to enhance security management for sensitive medical data using blockchain technology and smart contracts within the IoMT ecosystem. The proposed system aims to provide a decentralized and tamper-resistant platform that ensures data integrity, confidentiality, and controlled access. By integrating blockchain into the IoMT infrastructure, healthcare organizations can significantly enhance the security and privacy of sensitive medical data.

CCS CONCEPTS

• **Security and privacy → Database and storage security**; • **Applied computing → Health care information systems**.

MobiHoc '23, October 23–26, 2023, Washington, DC, USA

ACM ISBN 978-1-4503-9926-5/23/10…$15.00
https://doi.org/10.1145/3565287.3623388

KEYWORDS

Internet of Medical Things, Data Security, Privacy, Authentication, Healthcare, Big Data Analytics.

ACM Reference Format:
Pushpita Chatterjee, Debashis Das, Sourav Banerjee, Uttam Ghosh, Armando B. Mpembele, and Tamara Rogers. 2023. An Approach Towards the Security Management for Sensitive Medical Data in the IoMT Ecosystem. In *The Twenty-fourth International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing (MobiHoc '23), October 23–26, 2023, Washington, DC, USA.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3565287.3623388

1 INTRODUCTION

The Internet of Medical Things (IoMT) ecosystem is a network of interconnected medical devices and systems that generate and exchange patient data in real-time [20]. The proliferation of IoMT devices has led to a surge in sensitive medical data, including patient records, diagnostics, treatment plans, and more. This data, if mishandled or accessed by unauthorized parties, could lead to severe privacy breaches and compromise patient safety [18]. However, these devices are incorporated into healthcare systems to facilitate healthcare operations and better patient outcomes. IoMT has the potential to completely transform the healthcare business by improving data-driven decision-making, personalized treatment, and accessibility to healthcare services. It is possible to monitor patients remotely, do predictive analytics, and make advances in telemedicine with this technology, among other advantages. To fully realize the potential benefits of IoMT, it is necessary to take precautions to protect the confidentiality and security of sensitive medical information.

Several vulnerabilities and data privacy risks could threaten medical data security in the context of IoMT [2]. Unencrypted IoMT-central system communication channels allow attackers to grab data. Data breaches and privacy violations arise from weak authentication and authorization procedures. Unprotected IoMT devices enable attackers to tamper with or steal sensitive data. Cybercriminals may attack IoT devices with obsolete firmware or default passwords. Data leakage and improper data reduction lead to data breaches. Unauthorized data change raises data integrity and patient safety issues. Healthcare providers outsource services to

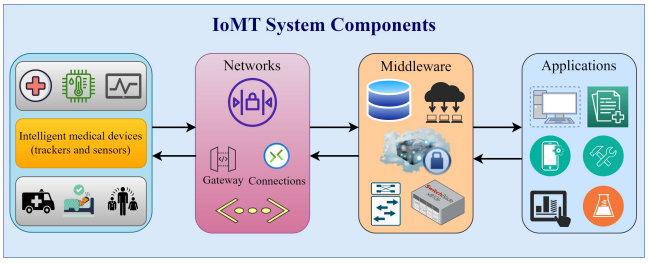

Figure 1: An overview of IoMT system.

companies with poor security risk data breaches [4]. These vulnerabilities and threats demand a thorough IoMT security management process. Strong encryption, authentication, and frequent software upgrades can secure sensitive medical data and patient privacy in the IoMT ecosystem.

Traditional centralized data management systems have proven vulnerable to data breaches and cyberattacks. Blockchain technology offers an innovative solution to address these vulnerabilities by introducing decentralization, transparency, and immutability to data management [10]. Combining blockchain with smart contracts [9] provides an automated way to enforce access controls and data-sharing permissions. Therefore, in this paper, we present a blockchain-enabled IoMT system to address the critical challenges of security and privacy in handling sensitive medical data. The proposed work aims to enhance the security management of sensitive medical data in the IoMT ecosystem using blockchain technology and smart contracts. The system utilizes a private blockchain network to ensure data privacy and permissioned access. It provides a robust and decentralized framework to securely manage medical data access while preserving patient confidentiality [8]. With these measures in place, healthcare providers and patients can confidently share and access medical data within the IoMT ecosystem. The main objectives of this research are as follows:

- To identify the specific security threats and vulnerabilities associated with the IoMT ecosystem.
- To analyze the effectiveness of different security measures in preserving the confidentiality, integrity, and availability of medical data.
- To strengthen the security of sensitive medical data by using blockchain's cryptographic hashing and immutability features.
- To implement robust access controls using smart contracts to grant permissioned access to authorized stakeholders.
- To develop a scalable solution to manage a high volume of data transactions in the IoMT ecosystem by allowing healthcare providers to access patient data quickly and efficiently.

The rest of the paper is organized as follows: Section 2 describes security threats and vulnerabilities associated with the IoMT ecosystem. In section 3, the proposed system model is described and implemented. Section 4 gives the experiment results of the proposed method. Section 5 depicts some performance metrics of the proposed system. Finally, Section 6 concludes the paper by giving future directions.

2 THREATS AND SECURITY REQUIREMENTS IN IOMT

2.1 Threats

Existing IoMT applications face several threats that can compromise data security, patient privacy, and the overall integrity of healthcare systems [13, 19, 23].

Data Breaches: Data breaches occur when unauthorized individuals gain access to sensitive medical data stored within IoMT applications. This could include patient health records, medical histories, treatment plans, and other personally identifiable information. Data breaches can have severe consequences, such as identity theft, financial fraud, and damage to the reputation of healthcare providers.

Cyber-Attacks: IoMT devices are susceptible to various cyberattacks, including ransomware, malware, and DDoS attacks. Ransomware can encrypt data on IoMT devices and demand payment for decryption, disrupting healthcare operations and patient care. Malware can compromise the confidentiality and integrity of medical data. DDoS attacks can overwhelm IoMT systems, causing service outages and rendering them inaccessible.

Data Tampering: Manipulating medical data within IoMT applications can lead to incorrect diagnoses or treatment plans. Data tampering may alter vital signs, lab results, or medication dosages, compromising patient safety and care quality.

IoMT Device Vulnerabilities: Weaknesses in IoMT devices' security, such as default passwords or outdated firmware, can make them susceptible to exploitation. Attackers can gain unauthorized access to devices and the data they collect, leading to potential data breaches and misuse of sensitive information.

Lack of Encryption: Insufficient data encryption leaves sensitive medical data vulnerable to interception during transmission or storage. Without encryption, attackers may eavesdrop on data exchanges and gain access to patient's private health information.

Lack of Authentication and Authorization: Inadequate authentication and authorization mechanisms allow unauthorized individuals to access and modify medical data. Without proper access controls, malicious actors can gain entry to sensitive information and manipulate it for malicious purposes.

2.2 Effectiveness of Security

The deployment, setup, and ongoing monitoring of security measures in IoMT applications are essential to determine how well these measures work. The efficacy of security measures in IoMT applications relies on various factors [6, 12, 24]. Regarding the efficiency of the security measures used in IoMT, the following are some important considerations to take into account:

Encryption: Data encryption is the process of converting sensitive information into a coded form that can only be accessed with the correct decryption key. Proper data encryption ensures that even if unauthorized individuals gain access to the data, they cannot interpret its content without the decryption key. Strong encryption algorithms, such as Advanced Encryption Standard (AES), combined with secure key management practices, significantly reduce the risk of unauthorized access and help safeguard sensitive medical data during storage.

Table 1: A comparison analysis of existing blockchain-based IoMT methods

Ref.	Year	Method	Description	Pros	Cons
[5]	2010	MedRec	Decentralized patient health record management.	Improved data integrity, and patient control over data.	Scalability challenges, reliance on blockchain consensus.
[21]	2022	FarmaTrust	Drug supply chain tracking and verification.	Increased transparency, reduced counterfeiting risk.	Data privacy concerns, potential adoption barriers in the industry.
[17]	2016	Gem Health	Health data exchange and consent management.	Interoperability, patient consent control.	Integration complexity, regulatory compliance.
[15]	2019	Mediledger	Pharmaceutical supply chain traceability.	Provenance and audibility of drug transactions.	Integration with legacy systems, tokenization challenges.
[16]	2017	Patientory	Secure health data storage and sharing platform.	Enhanced data security, and patient engagement.	Adoption barriers, regulatory compliance.
[1]	2019	EncrypGen	Genetic data marketplace with privacy control.	Patient-controlled data sharing, data monetization.	Data accuracy concerns, potential legal complexities.
[14]	2019	Tierion	Anchoring data to the blockchain for verification.	Tamper-proof audit trails, data verification.	Limited scalability for high-frequency data.
[11]	2021	Iryo	Decentralized health data storage and access.	Data security, patient-controlled access.	Technical barriers, adoption challenges in the healthcare sector.
[3]	2021	Coral Health	Health data exchange for providers and patients.	Improved interoperability, and data access control.	Regulatory compliance, network consensus overhead.
[25]	2018	SimplyVital Health	Care coordination and data sharing platform.	Data integrity, streamlined healthcare workflows.	Scalability concerns, potential resistance from existing systems.
[22]	2018	MediBloc	Health data ecosystem with patient control.	Data ownership, medical data sharing efficiency.	Integration challenges, data standardization.

Authentication and Authorization: Authentication is the process of verifying the identity of a user or device trying to access the system, while authorization determines what actions that authenticated user or device is allowed to perform. Implementing robust authentication and authorization mechanisms ensures that only authorized users with valid credentials can access and modify medical data.

Access Controls: Granular access controls enable healthcare organizations to define precisely which users or user groups have access to specific data or functionalities within IoMT applications. This fine-grained control minimizes the potential for data breaches and unauthorized access, as users are granted access only to the information they need to perform their roles.

Auditing and Monitoring: Regular security audits and continuous monitoring of IoMT systems are essential to identify real-time vulnerabilities and security gaps. Security audits assess the effectiveness of implemented security measures, while continuous monitoring detects and alerts for any suspicious activities in real time. This proactive approach allows for timely responses to security threats, helping to prevent or mitigate potential breaches.

3 PROPOSED METHODOLOGY

3.1 System Model

The proposed system utilizes a private blockchain network to ensure data privacy and permissioned access. The blockchain will store hashed medical data, and access controls will be governed by smart contracts. Healthcare providers, patients, doctors, and authorized stakeholders will be granted unique cryptographic keys to access specific data segments. Fig. 2 shows the overall system model. Each entity is described in the following:

3.1.1 Private Blockchain Network. The system will employ a private blockchain network rather than a public one to ensure data privacy and control over network participants. In a private blockchain, only authorized entities can join the network participate in the consensus process, and maintain a high level of confidentiality. This is required in the healthcare domain, where sensitive patient data must be protected from unauthorized access.

3.1.2 Hashed Medical Data Storage. Sensitive medical data (i.e., patient records, test results, and treatment plans), stored in Interplanetary File Systems (IPFS), will be converted into cryptographic hashes before being stored on the blockchain. Hashing is a one-way cryptographic function that converts data into a fixed-length string of characters. It represents the original data without revealing its content. By storing only the hashes on the blockchain, the actual sensitive data remains off-chain for enhancing data security.

3.1.3 Access Controls Through Smart Contracts. Smart contracts are self-executing scripts with predefined rules and conditions written in code. In the proposed system, smart contracts will be used to manage data access controls. These smart contracts will be deployed on the blockchain and act as automated intermediaries between data providers and consumers. They will enforce data-sharing permissions based on predefined rules to ensure that only authorized individuals can access specific medical data. However, authorization will be done by smart contracts automatically.

3.1.4 Data Encryption and Decryption. Before sensitive medical data is uploaded to the blockchain, it will undergo encryption using advanced encryption algorithms. Encryption transforms the data into an unreadable format, and only those with the correct decryption keys can access and read the original data. This step

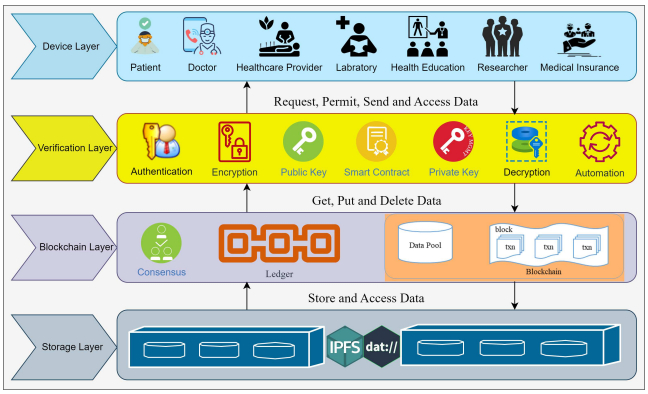

Figure 2: Proposed system model.

adds another level of protection to the data, ensuring that even if unauthorized parties manage to access the data, they will not be able to understand it without the decryption keys.

3.1.5 Data Ownership and Consent Management. With the help of smart contracts, patients will have more control over their medical data. They can specify who can access their data, for what purposes, and for how long. Patients can grant or revoke access to specific healthcare providers, doctors, insurance companies, or hospitals. This can help promote transparency and patient-centric data management.

3.1.6 Transaction Validation and Consensus Mechanism. In a private blockchain network, a consensus mechanism can be employed to validate and agree on the transactions to be added to the blockchain. The choice of consensus mechanism depends on the specific requirements of the system, but common ones include Proof-of-Authority (PoA) or Practical Byzantine Fault Tolerance (PBFT). These mechanisms ensure that data integrity is maintained, and all participants in the network reach a consensus on the validity of medical records and transactions.

3.2 Data Security Management

This section provides an overview of how data encryption, decryption, and access control using smart contracts can be implemented in the proposed system. The process of converting sensitive medical data into cryptographic hashes can be represented using a hashing function. One commonly used hashing function is the SHA-256 (Secure Hash Algorithm 256-bit). SHA-256 takes an input message and produces a fixed-length 256-bit (32-byte) hash value.

3.2.1 Data Encryption and Decryption. To explain the process of data encryption, decryption, and access control using smart contracts, we'll break it down step by step. Let's consider three stakeholders in the system (see Fig. 2): patient (P), healthcare provider (H), and researcher (R).

Assume we have an encryption algorithm represented as E() for encryption and D() for decryption. P wants to encrypt their sensitive medical data ($D_patient$) before storing it on the blockchain. H and R have their respective encryption keys ($K_H and K_R$) for data access. data encryption can be represented as equation (1), where $Encrypted_{Data_P}$ is the encrypted medical data of P.

Algorithm 1: Data access granted or denied

Input: address
Output: Access granted / denied;
$Request_Address = Address_H$;
$Requested_{Data_Hash} = Hash_{Encrypted_{Data_H}}$;
if $Request_Address$ *in* $SC_P.Permissions$ **then**
  $Decrypt(Encrypted_{Data_P, K_P})$;
  allowedAccess[H] = true;
  Access granted;
else
  Access Denied;
  allowedAccess[H] = false;
end

$$Encrypted_{Data_P} = E(D_{patient}, K_P) \quad (1)$$

Similarly, the healthcare provider (H) and researcher (R) can also encrypt their data shown in equations 2 and 3 respectively.

$$Encrypted_{Data_H} = E(D_{healthcare_provider}, K_H) \quad (2)$$

$$Encrypted_{Data_R} = E(D_{researcher}, K_R) \quad (3)$$

3.2.2 Access and Permissions Using Smart Contracts. Now, we implement smart contracts to enforce access controls and permissions. The smart contracts will define who can access specific encrypted data and under what conditions.

a) Patient (P) Smart Contract (SC_P): The patient will deploy a smart contract (SC_P) on the blockchain that contains the following information (see equation 4):

- $Address_P$: The blockchain address of P.
- $Hash_{Encrypted_{Data_P}}$: The hash of the encrypted data stored off-chain.
- Permissions: A list of authorized addresses (addresses of H and R) allowed to access the data.

$$SC_P(Address_P, Hash_{Encrypted_{Data_P}}, [Address_H, Address_R]) \quad (4)$$

b) Healthcare Provider (H) and Researcher (R) Smart Contracts ($SC_H and SC_R$): Similarly, the healthcare provider and researcher will deploy their respective smart contracts ($SC_H and SC_R$) (see equations 5 and 6)on the blockchain specifying their addresses, their encrypted data hashes, and any other relevant permissions.

$$SC_H(Address_H, Hash_{Encrypted_{Data_H}}, [Address_P]) \quad (5)$$

$$SC_R(Address_R, Hash_{Encrypted_{Data_R}}, [Address_P]) \quad (6)$$

3.2.3 Data Access. When H or R needs to access the patient's data, they must interact with the respective smart contract (SC_P) deployed by P. The smart contract will verify their address and permissions before granting access. let's say H wants to access the patient's data. The smart contract will check if the requesting address ($Address_H$) is authorized to access the data and then allow or deny access accordingly. The decryption key (K_P) required for decrypting the data will only be possessed by the patient (see Algorithm 1). It ensures that only authorized parties can access the original sensitive medical data.

(a) Smart contacts is deployed successfully.

(b) P grants data access to H.

(c) Setting the bool value to allow access.

(d) P revokes data access from H.

(e) Unauthorized access to P's account.

(f) P doesn't have access to this feature.

Figure 3: Data access management in the proposed system.

4 EXPERIMENT RESULTS

We experiment with our proposed system using Remix IDE for smart contract development [7]. We can write, compile, deploy, and interact with smart contracts using Solidity language within the Remix IDE. In this experiment, we create a basic smart contract to represent a patient's medical data record. The contract allows the patient to grant access to healthcare providers and researchers. We use the contract to store the patient's hashed medical data and manage access permissions.

We deploy the "MedicalData" smart contract (as shown in Fig. 3a), which has the functionality to manage access permissions for the patient's medical data. Assume that the contract is successfully deployed and the contract address is stored in a variable called "medicalDataContractAddress" (see in Figure 3a). The patient (P) (see in Figure 3b) wants to grant access to their medical data to the healthcare provider (H). For this, P will call the "grantAccess" function by passing the address of H as an argument, as shown in Fig. 3b. The "grantAccess" function allows the P to grant access to the H by setting the "allowedAccess" mapping value for H to true. After calling this function, H will have access to the patient's medical data, as shown in Fig. 3c. H can now access the patient's medical data by calling the "getHashedData" function of the MedicalData smart contract. If at any point, P wants to revoke access from H, they can call the revokeAccess function, which would set the "allowedAccess" mapping value for H to false (see Fig. 3d). Fig. 3e shows that P can only grant access to his own data to the H. And, Fig. 3f depicts that Unauthorized H cannot access P's medical data.

However, our experiment focuses on the basic functionality of granting access to the healthcare provider. In a real-world scenario, we would need to consider additional security measures, data encryption, and validation checks to ensure the proper management of permissions and access to sensitive medical data broadly.

5 SECURITY AND PRIVACY CONSIDERATIONS

Let's explain the security and privacy considerations related to data integrity, confidentiality, scalability, and performance in the proposed system.

5.1 Data Integrity

Data integrity is the accuracy and consistency of data throughout its lifecycle. In the proposed system, data integrity is maintained through the immutability of the blockchain. Once sensitive medical data is hashed and added to the blockchain, it becomes a part of the distributed ledger and cannot be altered or deleted without consensus from the network participants. Any attempt to tamper with the data after it has been added will result in a change in the hash value. The cryptographic nature of blockchain ensures that each block is linked to its previous block through a cryptographic hash. This linkage ensures that any modification to a previous block will break the chain. This tamper-resistant property of the blockchain provides a robust solution for maintaining data integrity in the IoMT ecosystem.

5.2 Confidentiality

Confidentiality is crucial when dealing with sensitive medical data. To ensure that only authorized individuals can access the data, the proposed system employs encryption and smart contracts. As discussed earlier, sensitive medical data is encrypted before being stored on the blockchain. This encryption ensures that even if unauthorized parties manage to gain access to the blockchain, they will only see the encrypted data that is meaningless without the decryption keys. Smart contracts play a central role in controlling data access. Each stakeholder (patient, healthcare provider, and researcher) has their respective smart contracts specifying who

can access their data. Access permissions are enforced through these contracts. Only individuals with the correct keys and authorized addresses listed in the smart contracts can decrypt and access sensitive medical data. This strict access control mechanism helps maintain the confidentiality of the data and prevents unauthorized access.

5.3 Scalability and Performance

Scalability and performance are crucial aspects when considering the implementation of blockchain in the IoMT ecosystem. Healthcare systems generate vast amounts of data, and blockchain must handle a high volume of transactions efficiently to remain practical. To address scalability, the proposed system should focus on the following approaches:

- Sharding: Sharding involves breaking the blockchain network into smaller, more manageable pieces called shards, each capable of processing its transactions. This approach can significantly improve transaction throughput in our proposed system.
- Off-chain solutions: Not all data needs to be stored on the main blockchain. Off-chain solutions, like state channels or sidechains, can be utilized to handle less critical or real-time data. It reduces the load on the main blockchain.

6 CONCLUSION

In this paper, we proposed an approach to enhance security management for sensitive medical data within the IoMT ecosystem using blockchain technology and smart contracts. By utilizing the advantages of decentralization, data integrity, and access controls, our system offers a robust solution to safeguard patient data and maintain privacy. The proposed system can evolve into a robust and transformative solution that enhances data security, patient privacy, and healthcare collaboration in the IoMT ecosystem. Ultimately, this improves the quality of healthcare services in the digital age. Future research could focus on optimizing blockchain protocols and exploring layer 2 scaling solutions to handle the ever-increasing volume of medical data generated by IoMT devices. Solutions like sharding, state channels, or sidechains could be investigated to improve transaction throughput.

7 ACKNOWLEDGEMENT

This work was supported by the National Science Foundation, under award number 2219741.

REFERENCES

[1] Eman Ahmed and Mahsa Shabani. 2019. DNA data marketplace: an analysis of the ethical concerns regarding the participation of the individuals. *Frontiers in genetics* (2019), 1107.

[2] M Aruna, S Ananda Kumar, B Arthi, and Uttam Ghosh. 2022. Smart security for industrial and healthcare IoT applications. In *Intelligent Internet of Things for Healthcare and Industry*. Springer, 353–371.

[3] Seyed Mojtaba Hosseini Bamakan, Shima Ghasemzadeh Moghaddam, and Sajedeh Dehghan Manshadi. 2021. Blockchain-enabled pharmaceutical cold chain: Applications, key challenges, and future trends. *Journal of Cleaner Production* 302 (2021), 127021.

[4] Siddharth Banyal, Deepanjali Mehra, Amartya, Siddhant Banyal, Deepak Kumar Sharma, and Uttam Ghosh. 2022. Computational Intelligence in Healthcare with Special Emphasis on Bioinformatics and Internet of Medical Things. In *Intelligent Internet of Things for Healthcare and Industry*. Springer, 145–170.

[5] Jesdeep Bassi, Francis Lau, and Stan Bardal. 2010. Use of information technology in medication reconciliation: a scoping review. *Annals of Pharmacotherapy* 44, 5 (2010), 885–897.

[6] Bharat Bhushan, Avinash Kumar, Ambuj Kumar Agarwal, Amit Kumar, Pronaya Bhattacharya, and Arun Kumar. 2023. Towards a Secure and Sustainable Internet of Medical Things (IoMT): Requirements, Design Challenges, Security Techniques, and Future Trends. *Sustainability* 15, 7 (2023), 6177.

[7] Debashis Das, Sourav Banerjee, Pushpita Chatterjee, Uttam Ghosh, and Utpal Biswas. 2022. A secure blockchain enabled v2v communication system using smart contracts. *IEEE Transactions on Intelligent Transportation Systems* 24, 4 (2022), 4651–4660.

[8] Debashis Das, Sourav Banerjee, Pushpita Chatterjee, Uttam Ghosh, Wathiq Mansoor, and Utpal Biswas. 2022. Design of an automated blockchain-enabled vehicle data management system. In *2022 5th International Conference on Signal Processing and Information Security (ICSPIS)*. IEEE, 22–25.

[9] Debashis Das, Sourav Banerjee, Kousik Dasgupta, Pushpita Chatterjee, Uttam Ghosh, and Utpal Biswas. 2023. Blockchain enabled sdn framework for security management in 5g applications. In *Proceedings of the 24th International Conference on Distributed Computing and Networking*. 414–419.

[10] Debashis Das, Kousik Dasgupta, and Utpal Biswas. 2023. A secure blockchain-enabled vehicle identity management framework for intelligent transportation systems. *Computers and Electrical Engineering* 105 (2023), 108535.

[11] Beyhan Adanur Dedeturk, Ahmet Soran, and Burcu Bakir-Gungor. 2021. Blockchain for genomics and healthcare: a literature review, current status, classification and open issues. *PeerJ* 9 (2021), e12130.

[12] Taher M Ghazal, Mohammad Kamrul Hasan, Ghassan F Issa, Nidal A Al-Dmour, Saif EA Alnawayseh, Waleed T Al-Sit, and Rashed Aldhaheri. 2022. Security Threats and their Mitigations on the Operating System of Internet of Medical Things (IoMT). In *2022 14th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS)*. IEEE, 1–7.

[13] Ali Ghubaish, Tara Salman, Maede Zolanvari, Devrim Unal, Abdulla Al-Ali, and Raj Jain. 2020. Recent advances in the internet-of-medical-things (IoMT) systems security. *IEEE Internet of Things Journal* 8, 11 (2020), 8707–8718.

[14] Syed Saud Hasan, Nazatul Haque Sultan, and Ferdous Ahmed Barbhuiya. 2019. Cloud data provenance using IPFS and blockchain technology. In *Proceedings of the Seventh International Workshop on Security in Cloud Computing*. 5–12.

[15] Jens Mattke, Axel Hund, Christian Maier, and Tim Weitzel. 2019. How an Enterprise Blockchain Application in the US Pharmaceuticals Supply Chain is Saving Lives. *MIS Quarterly Executive* 18, 4 (2019).

[16] Chrissa McFarlane, Michael Beer, Jesse Brown, and Nelson Prendergast. 2017. Patientory: A healthcare peer-to-peer EMR storage network v1. *Entrust Inc.: Addison, TX, USA* 3 (2017), 19.

[17] Matthias Mettler. 2016. Blockchain technology in healthcare: The revolution starts here. In *2016 IEEE 18th international conference on e-health networking, applications and services (Healthcom)*. IEEE, 1–3.

[18] Senthil Murugan Nagarajan, Ganesh Gopal Deverajan, Puspita Chatterjee, Waleed Alnumay, and Uttam Ghosh. 2021. Effective task scheduling algorithm with deep learning for Internet of Health Things (IoHT) in sustainable smart cities. *Sustainable Cities and Society* 71 (2021), 102945.

[19] Maria Papaioannou, Marina Karageorgou, Georgios Mantas, Victor Sucasas, Ismael Essop, Jonathan Rodriguez, and Dimitrios Lymberopoulos. 2022. A survey on security threats and countermeasures in internet of medical things (IoMT). *Transactions on Emerging Telecommunications Technologies* 33, 6 (2022), e4049.

[20] Dukka Karun Kumar Reddy, HS Behera, Janmenjoy Nayak, Ashanta Ranjan Routray, Pemmada Suresh Kumar, and Uttam Ghosh. 2022. A fog-based intelligent secured iomt framework for early diabetes prediction. In *Intelligent Internet of Things for Healthcare and Industry*. Springer, 199–218.

[21] Sven Rojnic. 2022. Blockchain Application in Healthcare: The Example of Farmatrust, Medicalchain and E-Hcert. *Amsterdam LF* 14 (2022), 69.

[22] Thein Than Thwin and Sangsuree Vasupongayya. 2018. Blockchain based secret-data sharing model for personal health record system. In *2018 5th International conference on advanced informatics: concept theory and applications (ICAICTA)*. IEEE, 196–201.

[23] WAEL Toghuj and NIDAL Turab. 2022. A Survey on Security Threats in the internet of medical things (IoMT). *J. Theor. Appl. Inf. Technol* 100, 10 (2022), 3361–3371.

[24] Thavavel Vaiyapuri, Adel Binbusayyis, and Vijayakumar Varadarajan. 2021. Security, privacy and trust in IoMT enabled smart healthcare system: A systematic review of current and future trends. *International Journal of Advanced Computer Science and Applications* 12, 2 (2021).

[25] Jayneel Vora, Anand Nayyar, Sudeep Tanwar, Sudhanshu Tyagi, Neeraj Kumar, Mohammad S Obaidat, and Joel JPC Rodrigues. 2018. BHEEM: A blockchain-based framework for securing electronic health records. In *2018 IEEE Globecom Workshops (GC Wkshps)*. IEEE, 1–6.

Received 22 August 2023; revised 02 September 2023; accepted 06 September 2023