RESEARCH PAPER

A Comprehensive Review of Hybrid Consensus Mechanisms for Energy-Efficient and Secure Blockchain-Based IoMT Healthcare Systems

Samrity[1], Dr. Kamaljit Kaur[2]

[1] PhD Research Scholar, Department of Computer Science, Sri Guru Granth Sahib World University, Fatehgarh Sahib, Punjab, India. Email: Samrity87@gmail.com

[2] Assistant Professor, Department of Computer Science, Sri Guru Granth Sahib World University, Fatehgarh Sahib, Punjab, India

Received: 12th Mar, 2026 | **Revised:** 24th Mar, 2026 | **Accepted:** 14th Apr, 2026 | **Available Online:** 30th Apr, 2026

ABSTRACT

The Internet of Medical Things has achieved rapid expansion which enables hospitals to execute real-time patient monitoring and data collection activities while using automated decision-making systems. The use of medical devices which connect to the internet creates substantial issues that affect data protection, personal information safety, device power usage, and system expansion capabilities. Blockchain technology has emerged as a promising solution to address these issues by providing decentralized, transparent, and secure data management. This review paper presents a comprehensive analysis of blockchain-based Internet of Medical Things healthcare systems with a particular focus on hybrid consensus mechanisms. The study examines existing literature on energy-efficient models, security frameworks, and hybrid approaches, along with the use of advanced technologies such as artificial intelligence, edge computing, and cryptographic techniques. The research employs a systematic methodology to categorize and assess studies according to their main performance indicators which include energy use, response time, system protection, and system capacity. The research results demonstrate that hybrid consensus mechanisms establish an equilibrium between system performance and security enhancements yet they face multiple challenges that include system complexity and device compatibility and practical implementation. This review highlights current research trends, identifies gaps, and suggests future directions for developing secure and energy-efficient IoMT healthcare systems.

Keywords: Blockchain, Internet of Medical Things, Hybrid Consensus Mechanisms, Energy Efficiency, Healthcare Security

How to cite this article: Samrity, Kaur K. A Comprehensive Review of Hybrid Consensus Mechanisms for Energy-Efficient and Secure Blockchain-Based IoMT Healthcare Systems. Int J Drug Deliv Technol. 2026;16(38s): 499-510. DOI: 10.25258/ijddt.16.38s.48

Source of support: Nil.

Conflict of interest: None

1. Introduction

The Internet of Medical Things (IoMT) system emerged from the fast development of digital healthcare which creates a system that combines smart medical equipment with sensors and communication technologies to provide hospitals with continuous patient monitoring capabilities and streamlined healthcare services. The rising adoption of IoMT technology creates major problems that involve power usage and protection of information and system expansion and management of confidence between users and systems.

Blockchain technology has emerged as a promising solution to overcome these limitations by offering decentralized, transparent, and tamper-resistant data management. The combination of IoMT and hybrid blockchain models has established a secure method for improving system security and operational performance according to its research results.(**Rehman et al. 2024) [1]** developed a hybrid blockchain model for IoMT healthcare systems that enables secure data sharing between devices while maintaining operational capabilities and system performance. The security

mechanisms based on blockchain technology which protect IoMT edge networks provide effective security solutions for healthcare monitoring systems through their ability to protect data transmission and detect cyber threats according to (**Pelekoudas-Oikonomou et al. 2022) [2]..**

1.1 Overview of IoMT in Healthcare

The Internet of Medical Things (IoMT) functions as a system that links medical devices and wearable sensors and healthcare applications through internet connections which gather and analyze and send patient information. The systems provide continuous health tracking and remote medical assessment and customized healthcare solutions which result in better healthcare services that become more widely available to patients. The researchers **(Razdan & Sharma, 2022) [3]** identified IoMT as a collection of different technologies that includes wearable health trackers and implantable devices and smart hospital equipment and cloud-based healthcare platforms. The technologies provide smooth data transfer from patients to healthcare professionals which allows doctors to identify health issues before they become critical and reduces the need for patients to go to hospitals.

The latest developments have increased the operational capabilities of Internet of Medical Things (IoMT) technologies. The researchers **(Shafiq et al., 2023) [4]** explained how IoMT systems benefit from advanced technologies that include artificial intelligence and machine learning and edge computing to enhance their data processing and decision-making and system performance. **1.2 Blockchain Integration in IoMT**

The integration of blockchain technology with the Internet of Medical Things creates a transformative solution for addressing key challenges in healthcare systems, particularly in terms of data security, reliability, and decentralized data management. IoMT systems generate large volumes of sensitive medical data that require secure storage, controlled access, and safe sharing among multiple stakeholders. The decentralized and immutable nature of blockchain ensures data integrity and transparency in distributed environments. According to **(Mazhar et al., 2024) [5]**, blockchain integration reduces dependency on centralized systems, thereby minimizing risks of data tampering and unauthorized access. Blockchain in healthcare can be broadly categorized into **public, private, and hybrid blockchain types**, each offering different levels of transparency, control, and efficiency.

However, several challenges remain, including scalability issues, high computational overhead, and complex system integration. Studies such as **(Uddin et al., 2025) [6]** highlight improvements in secure data sharing through blockchain-based IoMT systems, while **(Almalki et al., 2022) [7]** discuss integration strategies to address latency, storage, and network congestion in large-scale environments. The research also emphasizes combining blockchain with emerging technologies such as edge computing to enhance system efficiency and real-time performance.

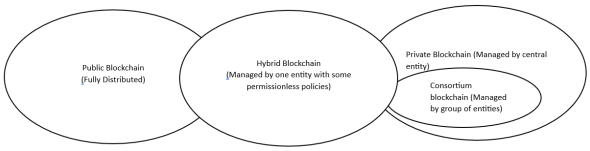

Figure 1: Types of Blockchain Used in Internet of Medical Things Healthcare Systems

1.3 Energy Efficiency Challenges in IoMT

Energy efficiency has become a fundamental issue for Internet of Medical Things systems because medical devices which include both wearable and implantable sensors function with their battery power limits. The process of continuous data collection which involves both data processing and data transmission leads to higher energy usage which subsequently impacts both device operational lifespan and system dependable performance. The study shows that energy-efficient routing and communication protocols become necessary for sustaining IoMT device operations according to the findings of (**Varun et al. 2019) [8]** which appear in reference 8. The study identifies major issues such as excessive communication overhead which leads to inefficient data transmission and medical networks experience rapid energy depletion because of their limited power resources.

The study by **(Zikria et al. 2020) [9]** presents IOMT systems research which shows that high energy usage occurs because of multimedia data processing and devices which maintain constant network connection. The authors emphasize the need for optimized network architectures and lightweight protocols to reduce energy usage while maintaining system performance.

1.4 Security and Privacy Issues

The healthcare systems which utilize IoMT technology face their biggest security and privacy problems because medical data remains highly sensitive. The interconnected devices which share patient data create an

increased possibility of cyberattacks and data breaches and unauthorized access. The healthcare system needs to protect data through its three essential elements which include confidentiality and integrity and availability to establish user trust in digital healthcare systems. The research conducted by **(Yakubu et al., 2024) [10]** demonstrates that traditional blockchain consensus mechanisms provide secure operation but they remain vulnerable to Sybil attacks and 51% attacks and insider threats which impact resource-constrained IoMT environments.

The study shows that current consensus protocols require better design because healthcare systems operate in both dynamic modes and distributed environments which create security vulnerabilities. The researchers from **(Alsadhan et al. 2024) [11]** demonstrate that IoMT systems require two different privacy protection methods to keep patient data safe during both transmission and storage and processing activities.

1.5 Motivation for Hybrid Consensus Mechanisms

Researchers required hybrid consensus solutions to develop blockchain systems which connect with Internet of Medical Things devices because traditional consensus methods consume excessive energy and fail to scale effectively while compromising system security. Hybrid consensus mechanisms combine the strengths of multiple protocols to achieve a balance between efficiency, security, and performance. The concept of hybrid approaches is supported by early work such as **(Tian et al., 2014) [12],** which introduced trust-based incentive mechanisms in hybrid networks to improve cooperation and system reliability. The study investigates hybrid models which increase network performance and trust between distributed entities although its main focus is not on Internet of Medical Things systems.

(Venkatesan & Rahayu, 2024) [13] showed that combining hybrid consensus algorithms with machine learning techniques results in better security and adaptability for blockchain systems. Their approach improves threat detection which helps select the best consensus method while reducing computational overhead to become useful in dynamic environments that have limited resources within Internet of Medical Things systems.

2. Literature Review

The rapid advancement of Internet of Medical Things and blockchain technologies has driven extensive research aimed at improving security, energy efficiency, and scalability in healthcare systems. Existing studies explore the integration of blockchain with IoMT to address challenges such as data privacy, secure communication, and decentralized data management, while also incorporating hybrid consensus mechanisms, artificial intelligence, and advanced cryptographic techniques. However, these approaches differ in methodology and performance, making it essential to systematically summarize and compare them, as presented in Table 1.

Table 1: Summary of Existing Studies in Blockchain-Based IoMT Healthcare

Ref No.	Author (Year)	Focus Area	Technique/Approach Used	Key Findings / Limitations
[14]	**(Abbas et al., 2026)**	Smart Healthcare with Blockchain	Blockchain + AI + IoT integration framework	Enhances interoperability, security, and data transparency; lacks real-time implementation and scalability validation
[15]	**(Alkhater et al., 2026)**	Scalable Healthcare Systems	Blockchain integrated with metaheuristic optimization algorithms	Improves system scalability and optimization efficiency; introduces higher computational complexity and processing cost
[16]	**(NA, 2026)**	Intrusion Detection in IoMT	Enhanced Artificial Bee Colony (E-ABC) + Deep Belief Network (DBN) with blockchain	Achieves high intrusion detection accuracy and secure data handling; requires high computational resources and training overhead

[17]	**(Datta et al., 2025)**	AI-Driven Healthcare Security	Blockchain combined with Artificial Intelligence models	Provides secure, transparent, and energy-efficient healthcare system; complexity increases due to AI integration
[18]	**(Nandanwar & Katarya, 2025)**	IoT Intrusion Detection Systems	Hybrid blockchain-based IDS framework	Strengthens intrusion detection and network security; faces scalability and real-time deployment challenges
[19]	**(Farooqi et al.)**	Privacy Preservation in IoMT	Federated Learning + Differential Privacy + Blockchain	Ensures strong privacy protection and decentralized learning; lacks experimental validation and performance evaluation
[20]	**(Al-awamy et al., 2025)**	Hybrid Consensus Mechanisms	Comprehensive analysis of hybrid consensus protocols	Demonstrates improved efficiency and fault tolerance; lacks specific implementation for IoMT healthcare systems
[21]	**(Datta & Namasudra, 2025)**	Energy-Efficient Healthcare Systems	Blockchain + Mobile Edge Computing (MEC)	Reduces energy consumption, latency, and improves data sharing efficiency; dependent on edge infrastructure availability
[22]	**(Kumar & Chatterjee, 2024)**	Secure IoMT Communication	Energy-efficient blockchain-based model	Enhances data security with reduced energy consumption; limited scalability for large IoMT networks
[23]	**(Bezanjani et al., 2024)**	Privacy-Preserving Healthcare Data	Machine Learning + Blockchain-based approach	Improves data privacy and secure access control; increases system complexity and processing overhead
[24]	**(Jonnapalli et al., 2024)**	AI-Based IoMT Security	Blockchain-driven AI security framework	Strengthens healthcare monitoring and threat detection; computational cost and latency remain concerns
[25]	**(Shetty & N, 2024)**	Energy Efficiency in IoT Healthcare	Data aggregation and optimization techniques	Improves energy efficiency and reduces communication overhead; lacks integration with blockchain technologies
[26]	**(Kunal et al., 2024)**	Secure Patient Data Management	Blockchain with advanced encryption protocols	Enhances data confidentiality and secure access; increased computational overhead
[27]	**(Kalra et al., 2024)**	Secure IoMT Communication	Hybrid signcryption with blockchain	Provides efficient encryption and authentication; implementation complexity remains high

[28]	**(Hu & Du, 2024)**	Medical Data Security	AES encryption integrated with blockchain	Improves secure storage and transmission; limited scalability analysis
[29]	**(Lodha et al., 2023)**	IoMT-based Healthcare Monitoring	Blockchain-based secure IoMT system	Enhances system security and monitoring; lacks energy efficiency optimization
[30]	**(Gupta et al., 2023)**	IoMT Healthcare Systems	Blockchain framework for healthcare	Provides comprehensive secure architecture; limited practical deployment
[31]	**(Alshammari, 2023)**	Predictive Security in IoMT	AI + Blockchain-based predictive framework	Improves threat prediction and system security; high computational cost
[32]	**(Pelekoudas-Oikonomou et al., 2022)**	IoMT Edge Security	Blockchain-based edge security mechanisms	Enhances secure communication at edge level; resource-intensive for IoMT devices
[33]	**(Liu & Li, 2022)**	Energy-Efficient Healthcare IoT	Permissioned blockchain + Deep Reinforcement Learning	Improves energy efficiency and security; complex model training required
[34]	**(Alam et al., 2022)**	IoMT with Fog Computing	Blockchain + Fog computing integration	Enhances reliability and reduces latency; infrastructure dependency
[35]	**(Elhachmi & Kobbane, 2022)**	IoMT Security Mechanisms	Blockchain-based security framework	Improves data integrity and authentication; lacks scalability evaluation
[36]	**(Lakhan et al., 2022)**	Privacy Preservation	Federated learning + Blockchain	Enhances privacy and fraud detection; increased system complexity
[37]	**(Nguyen et al., 2021)**	Data Offloading in Healthcare	Blockchain-based cooperative architecture	Improves data sharing efficiency; limited real-world validation
[38]	**(Biswas et al., 2020)**	Access Control in E-Healthcare	Blockchain-based access control (DAAC)	Strengthens data access control; scalability issues in large networks
[39]	**(Pavithran, 2020)**	Secure IoT Architecture	Blockchain-based IoT architecture	Provides secure system design; lacks IoMT-specific optimization

3. Research Methodology

This section presents the systematic approach adopted to collect, filter, classify, and analyze the literature related to blockchain-enabled IoMT healthcare systems with a focus on hybrid consensus mechanisms, energy efficiency, and security. The methodology is designed to ensure comprehensive coverage of the domain while maintaining relevance to the research objectives.

3.1 Data Sources and Study Selection

The selected studies were sourced from well-established academic databases to ensure credibility and research quality. The primary data sources include IEEE Xplore, SpringerLink, Elsevier (ScienceDirect), MDPI, and other reputed publishers.

Key contributions such as **(Pelekoudas-Oikonomou et al., 2022) [2]**, **(Razdan & Sharma, 2022) [3]**, **(Almalki et al., 2022) [7]**, and **(Elhachmi & Kobbane, 2022) [35]** were obtained from high-impact journals focusing on IoMT and blockchain security. Additionally, works

addressing system architectures and healthcare frameworks, including **(Lodha et al., 2023) [29]**, **(Nguyen et al., 2021) [37]**, and **(Pavithran, 2020) [39]**, were incorporated to provide a broader understanding of system design and implementation.

Advanced studies focusing on **privacy preservation and distributed learning**, such as **(Lakhan et al., 2022) [36]** and **(Farooqi et al.) [19]**, were included to analyze decentralized and privacy-aware healthcare solutions. Similarly, research on **intrusion detection and intelligent security mechanisms**, including **(NA, 2026) [16]** and **(Jonnapalli et al., 2024) [24]**, contributed to understanding threat detection in IoMT environments.

The study selection process involved keyword-based searching using terms such as *IoMT*, *blockchain healthcare*, *hybrid consensus*, *energy-efficient blockchain*, and *secure IoMT systems*. The collected papers were screened through title, abstract, and full-text evaluation to ensure alignment with the research objectives.

3.2 Classification of Literature (Energy, Security, Hybrid Models)

Table 2: Classification of Literature in Blockchain-Based IoMT Healthcare Systems

Category	Core Objective	Common Techniques Used	Representative Studies	Key Observations
Energy Efficiency	Reduce energy consumption and improve system performance in IoMT devices	Energy-efficient routing, Mobile Edge Computing (MEC), lightweight blockchain, reinforcement learning, data aggregation	**(Varun et al., 2019)** [8], **(Zikria et al., 2020)** [9], **(Datta & Namasudra, 2025)** [21], **(Liu & Li, 2022)** [33], **(Kumar & Chatterjee, 2024)** [22], **(Shetty & N, 2024)** [25]	Significant reduction in energy usage achieved; however, scalability and integration with complex IoMT systems remain challenging
Security & Privacy	Ensure data confidentiality, integrity, authentication, and privacy preservation in healthcare systems	Blockchain-based encryption (AES, ECC), access control, federated learning, AI-based threat detection, privacy-preserving frameworks	**(Yakubu et al., 2024)** [10], **(Alsadhan et al., 2024)** [11], **(Kunal et al., 2024)** [26], **(Hu & Du, 2024)** [28], **(Biswas et al., 2020)** [38], **(Elhachmi & Kobbane, 2022)** [35], **(Pelekoudas-Oikonomou et al., 2022)** [2], **(Bezanjani et al., 2024)** [23], **(Alshammari, 2023)** [31], **(Lakhan et al., 2022)** [36]	Strong improvements in data security and privacy; however, high computational overhead and lack of real-time deployment are major limitations
Hybrid Models	Achieve balance between energy efficiency, security, and scalability using integrated approaches	Hybrid consensus mechanisms, AI-integrated blockchain, metaheuristic optimization, hybrid cryptographic techniques (signcryption), IDS frameworks	**(Venkatesan & Rahayu, 2024)** [13], **(Al-awamy et al., 2025)** [20], **(Alkhater et al., 2026)** [15], **(Nandanwar & Katarya, 2025)** [18], **(Kalra et al., 2024)** [27], **(Datta et al., 2025)** [17], **(Abbas et al., 2026)** [14]	Provides a balanced solution for IoMT systems; however, increased system complexity, interoperability issues, and lack of standardization remain key challenges

3.3 Tools and Technologies Used in Existing Studies

Table 3: Tools and Technologies Used in Blockchain-Based Internet of Medical Things Healthcare Systems

Category	Subcategory	Tools / Techniques	Purpose in Internet of Medical Things Healthcare	Representative Studies
Blockchain Platforms	Public Blockchain	Ethereum	Decentralized data storage and smart contract-based secure transactions	**(Rehman et al., 2024)** [1], **(Kumar & Chatterjee, 2024)** [22]
	Permissioned Blockchain	Hyperledger Fabric	Controlled access, faster transaction processing, and secure data sharing	**(Liu & Li, 2022)** [33], **(Datta & Namasudra, 2025)** [21]
	Hybrid Blockchain	Combination of public and private blockchain models	Balance between data transparency and privacy requirements	**(Abbas et al., 2026)** [14], **(Alkhater et al., 2026)** [15]
Consensus Techniques	Proof-based Mechanisms	Proof of Stake, Delegated Proof of Stake	Reduce energy consumption compared to Proof of Work mechanisms	**(Al-awamy et al., 2025)** [20], **(Kumar & Chatterjee, 2024)** [22]
	Byzantine Fault Tolerance Mechanisms	Practical Byzantine Fault Tolerance	Provide fast and secure consensus in permissioned blockchain networks	**(Yakubu et al., 2024)** [10], **(Liu & Li, 2022)** [33]
	Hybrid Consensus Mechanisms	Combination of Proof of Stake and Byzantine Fault Tolerance, Artificial Intelligence-based consensus	Improve scalability, security, and overall system efficiency	**(Venkatesan & Rahayu, 2024)** [13], **(Nandanwar & Katarya, 2025)** [18]
Cryptographic Techniques	Symmetric Encryption	Advanced Encryption Standard	Secure data transmission and storage of medical information	**(Hu & Du, 2024)** [28], **(Kunal et al., 2024)** [26]
	Asymmetric Encryption	Elliptic Curve Cryptography	Lightweight encryption suitable for resource-constrained medical devices	**(Kunal et al., 2024)** [26], **(Alsadhan et al., 2024)** [11]
	Advanced Privacy Techniques	Zero-Knowledge Proof, Attribute-Based Encryption	Ensure privacy preservation and controlled data sharing	**(Alsadhan et al., 2024)** [11], **(Lakhan et al., 2022)** [36]

	Hybrid Cryptographic Techniques	Signcryption	Combine encryption and authentication for secure communication	**(Kalra et al., 2024)** [27]
Supporting Technologies	Artificial Intelligence Techniques	Machine Learning, Deep Learning, Reinforcement Learning	Enable threat detection, predictive analytics, and intelligent decision-making	**(Datta et al., 2025)** [17], **(Bezanjani et al., 2024)** [23], **(Alshammari, 2023)** [31]
	Edge Computing	Mobile Edge Computing	Reduce latency and energy consumption by processing data near devices	**(Datta & Namasudra, 2025)** [21], **(Alam et al., 2022)** [34]
	Fog Computing	Distributed fog-based processing	Improve scalability and real-time data processing in healthcare systems	**(Alam et al., 2022)** [34], **(Nguyen et al., 2021)** [37]

3.5 Evaluation Metrics Used in Literature

Table 4: Evaluation Metrics Used in Blockchain-Based Internet of Medical Things Healthcare Systems

Metric Category	Sub-Metric	Description	Measurement Parameters	Representative Studies
Energy Consumption	Device Energy Usage	Measures power consumed by medical sensors and IoMT devices during operation	Battery usage, energy per transaction, computational overhead	**(Varun et al., 2019)** [8], **(Datta & Namasudra, 2025)** [21], **(Liu & Li, 2022)** [33], **(Kumar & Chatterjee, 2024)** [22]
	Communication Energy	Energy consumed during data transmission between devices and network nodes	Transmission power, communication overhead	**(Zikria et al., 2020)** [9], **(Shetty & N, 2024)** [25]
Latency and Throughput	Latency	Time delay in processing and validating transactions in the blockchain network	Transaction delay, response time, block confirmation time	**(Rehman et al., 2024)** [1], **(Alam et al., 2022)** [34], **(Nguyen et al., 2021)** [37]
	Throughput	Number of transactions processed per unit time in the system	Transactions per second, processing rate	**(Abbas et al., 2026)** [14], **(Alkhater et al., 2026)** [15]
Security and Privacy Metrics	Data Confidentiality	Ensures that medical data is accessible only to authorized users	Encryption strength, key management efficiency	**(Kunal et al., 2024)** [26], **(Hu & Du, 2024)** [28]

	Data Integrity	Ensures that data is not altered during transmission or storage	Hash verification, immutability checks	**(Yakubu et al., 2024)** [10], **(Biswas et al., 2020)** [38]
	Authentication and Access Control	Verifies user identity and restricts unauthorized access	Authentication success rate, access control policies	**(Elhachmi & Kobbane, 2022)** [35], **(Pelekoudas-Oikonomou et al., 2022)** [2]
	Privacy Preservation	Protects sensitive patient data from exposure	Anonymization, differential privacy, secure sharing	**(Alsadhan et al., 2024)** [11], **(Lakhan et al., 2022)** [36]
Scalability	Network Scalability	Ability of the system to handle increasing number of devices and transactions	Number of nodes supported, network growth capacity	**(Al-awamy et al., 2025)** [20], **(Gupta et al., 2023)** [30]
	System Performance	Maintains efficiency under increased workload	Processing efficiency, load handling capability	**(Venkatesan & Rahayu, 2024)** [13], **(Nandanwar & Katarya, 2025)** [18]

4. Future Research Directions and Challenges

The healthcare systems which utilize blockchain technology together with Internet of Medical Things face three main obstacles: they cannot solve their energy consumption problems and they cannot achieve better scalability and their system complexity remains unsolved. The process of maintaining security while achieving energy efficiency proves challenging in all resource-limited environments. Hybrid consensus models require simplification to become usable but they display potential benefits according to their current state. The elements of data privacy and regulatory compliance and interoperability and real-world implementation requirements need additional research efforts.

5. Conclusion

The review analyzes blockchain-based Internet of Medical Things healthcare systems through its examination of hybrid consensus mechanisms that improve both energy consumption and system security. The study shows that blockchain technology boosts data integrity and transparency while enabling secure data sharing in distributed healthcare systems. Existing research demonstrates the effectiveness of integrating blockchain with advanced technologies such as artificial intelligence, edge computing, and privacy-preserving techniques to improve system performance and reliability.

The present situation contains multiple obstacles which include high computational requirements, limitations in system scalability, and the energy security balance problem. Hybrid consensus mechanisms provide a beneficial method to solve these challenges through their ability to merge different solutions, but the actual use of these methods remains restricted. Future research needs to create lightweight solutions which can scale according to needs and operate in healthcare environments while maintaining security and efficiency and meeting healthcare industry standards.

6. References

[1] Rehman, A. U., Tariq, N., Jan, M. A., Khan, F., Song, H., & Ibrahim, M. (2024). A blockchain-based hybrid model for iomt-enabled intelligent healthcare system. *IEEE transactions on network science and engineering*, *11*(4), 3512-3521.

[2] Pelekoudas-Oikonomou, F., Zachos, G., Papaioannou, M., De Ree, M., Ribeiro, J. C., Mantas, G., & Rodriguez, J. (2022). Blockchain-based security mechanisms for IoMT Edge networks in IoMT-based healthcare monitoring systems. *Sensors*, *22*(7), 2449.

[3] Razdan, S., & Sharma, S. (2022). Internet of medical things (IoMT): Overview, emerging technologies, and case studies. *IETE technical review*, *39*(4), 775-788.

[4] Shafiq, M., Choi, J. G., Cheikhrouhou, O., & Hamam, H. (2023). Advances in IoMT for healthcare systems. *Sensors*, *24*(1), 10.

[5] Mazhar, T., Shah, S. F. A., Inam, S. A., Awotunde, J. B., Saeed, M. M., & Hamam, H. (2024). Analysis of integration of IoMT with blockchain: issues, challenges and solutions. *Discover Internet of Things*, *4*(1), 21.

[6] Uddin, M. B., Hossain, M., Mahmud, T., & Das, S. (2025, June). Blockchain Integration in IoMT for Secure Healthcare: Challenges, Integration, and Solutions. In *2025 6th International Conference on Inventive Research in Computing Applications (ICIRCA)* (pp. 597-604). IEEE.

[7] Almalki, J., Al Shehri, W., Mehmood, R., Alsaif, K., Alshahrani, S. M., Jannah, N., & Khan, N. A. (2022). Enabling blockchain with IoMT devices for healthcare. *Information*, *13*(10), 448.

[8] Varun, C. R., Hakkalli, S., & Naik, P. (2019). Survey on energy efficient routing issues in IOMT. *Transportation*, *5*(5), 112-117.

[9] Zikria, Y. B., Afzal, M. K., & Kim, S. W. (2020). Internet of multimedia things (IoMT): Opportunities, challenges and solutions. *Sensors*, *20*(8), 2334.

[10] Yakubu, M. M., Hassan, F. B., Danyaro, K. U., Junejo, A. Z., Siraj, M., Yahaya, S., ... & Abdulsalam, K. (2024). A Systematic Literature Review on Blockchain Consensus Mechanisms' Security: Applications and Open Challenges. *Computer Systems Science & Engineering*, *48*(6).

[11] Alsadhan, A., Alhogail, A., & Alsalamah, H. (2024). Blockchain-based privacy preservation for the internet of medical things: a literature review. *Electronics*, *13*(19), 3832.

[12] Tian, C., Yang, B., Zhong, J., & Liu, X. (2014). Trust-based incentive mechanism to motivate cooperation in hybrid P2P networks. *Computer Networks*, *73*, 244-255.

[13] Venkatesan, K., & Rahayu, S. B. (2024). Blockchain security enhancement: an approach towards hybrid consensus algorithms and machine learning techniques. *Scientific Reports*, *14*(1), 1149.

[14] Abbas, S. R., Abbas, Z., Rehman, M. U., & Lee, S. W. (2026). Blockchain for smart healthcare: A systematic review of security, interoperability, and AI–IoT integration. *Digital Health*, *12*, 20552076261420985.

[15] Alkhater, K. H., Shanmugam, M., & Magalingam, P. (2026). A Systematic Review of Blockchain and Metaheuristic Algorithms for Secure and Scalable Healthcare Systems. *Fusion: Practice & Applications*, *21*(1).

[16] NA, B. (2026). Blockchain-Based intrusion detection system for IoMT utilizing an enhanced artificial bee colony (E-ABC) and deep belief network (DBN). *Peer-to-Peer Networking and Applications*, *19*(1), 21.

[17] Datta, S., Namasudra, S., Moparthi, N. R., Kumari, S., & Crespo, R. G. (2025). Transforming Healthcare With Artificial Intelligence and Blockchain: A Secure, Transparent and Energy-Efficient Approach. *Expert Systems*, *42*(8), e70101.

[18] Nandanwar, H., & Katarya, R. (2025). A hybrid blockchain-based framework for securing intrusion detection systems in internet of things. *Cluster Computing*, *28*(7), 471.

[19] Farooqi, S. A., Abd Rahman, A., & Saad, A. Federated Learning with Differential Privacy and Blockchain for Security and Privacy in IoMT A Theoretical Comparison and Review.

[20] Al-awamy, A. A., Al-shaibany, N., Sikora, A., & Welte, D. (2025). Hybrid consensus mechanisms in blockchain: a comprehensive review. *International Journal of Intelligent Systems*, *2025*(1), 5821997.

[21] Datta, S., & Namasudra, S. (2025). Energy-Efficient Blockchain-Based Secure Model to Share Medical Data Using Mobile Edge Computing. *Concurrency and Computation: Practice and Experience*, *37*(9-11), e70087.

[22] Kumar, A., & Chatterjee, K. (2024). Securing internet of medical devices using

energy efficient blockchain for healthcare 4.0. *Cluster Computing*, *27*(6), 8333-8348.

[23] Bezanjani, B. R., Ghafouri, S. H., & Gholamrezaei, R. (2024). Fusion of machine learning and blockchain-based privacy-preserving approach for healthcare data in the Internet of Things. *The Journal of Supercomputing*, *80*(17), 24975-25003.

[24] Jonnapalli, T. R., Deshai, N., Samatha, K., & Shekar, B. V. D. S. (2024). Algorithms in Advanced Artificial Intelligence Blockchain-driven Security Paradigm: A Robust System Harnessing the Internet of Medical Things (IoMT) Network for Enhanced E-Healthcare Monitoring 69. In *Algorithms in Advanced Artificial Intelligence* (pp. 462-470). CRC Press.

[25] Shetty, G. S., & N, R. (2024). Strategies for Achieving energy efficiency and data Security through data aggregation in IoT Healthcare Applications: A Comprehensive study. International Journal of Computer Networks and Applications, 11(2), 191. https://doi.org/10.22247/ijcna/2024/224440

[26] Kunal, S., Gandhi, P., Rathod, D., Amin, R., & Sharma, S. (2024). Securing patient data in the healthcare industry: A blockchain-driven protocol with advanced encryption. Journal of Education and Health Promotion, 13(1). https://doi.org/10.4103/jehp.jehp_984_23 .

[27] Kalra, H., Sevukamoorthy, L., Banchhor, C. O., Gajendran, P., & Faiz, A. (2024, December). A Hybrid Signcryption Approach for Blockchain-Based Secure Communication in IoMT Networks. In *2024 IEEE 4th International Conference on ICT in Business Industry & Government (ICTBIG)* (pp. 1-6). IEEE.

[28] Hu, X., & Du, Y. (2024). Securing Medical Data: the integration of advanced Encryption standard and blockchain. Journal of Information Analysis. https://doi.org/10.53964/jia.2024001

[29] Lodha, L., Baghela, V. S., Bhuvana, J., & Bhatt, R. (2023). A blockchain-based secured system using the Internet of Medical Things (IOMT) network for e-healthcare monitoring. *Measurement: sensors*, *30*, 100904.

[30] Gupta, S., Sharma, H. K., & Kapoor, M. (2023). *Blockchain for secure healthcare using Internet of Medical Things (IoMT)* (pp. 1-197). Cham: Springer.

[31] Alshammari, B. M. (2023). AIBPSF-IoMT: artificial intelligence and blockchain-based predictive security framework for IoMT technologies. *Electronics*, *12*(23), 4806.

[32] Pelekoudas-Oikonomou, F., Zachos, G., Papaioannou, M., De Ree, M., Ribeiro, J. C., Mantas, G., & Rodriguez, J. (2022). Blockchain-based security mechanisms for IoMT Edge networks in IoMT-based healthcare monitoring systems. *Sensors*, *22*(7), 2449.

[33] Liu, L., & Li, Z. (2022). Permissioned blockchain and deep reinforcement learning enabled security and energy efficient healthcare internet of things. *Ieee Access*, *10*, 53640-53651.

[34] Alam, S., Shuaib, M., Ahmad, S., Jayakody, D. N. K., Muthanna, A., Bharany, S., & Elgendy, I. A. (2022). Blockchain-based solutions supporting reliable healthcare for fog computing and internet of medical things (IoMT) integration. *Sustainability*, *14*(22), 15312.

[35] Elhachmi, J. A. M. A. L., & Kobbane, A. (2022). Blockchain-based security mechanisms for internet of medical things (IOMT). *International Journal of Computer Networks & Communications (IJCNC)*, *14*(14).

[36] Lakhan, A., Mohammed, M. A., Nedoma, J., Martinek, R., Tiwari, P., Vidyarthi, A., ... & Wang, W. (2022). Federated-learning based privacy preservation and fraud-enabled blockchain IoMT system for healthcare. *IEEE journal of biomedical and health informatics*, *27*(2), 664-672.

[37] Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2021). A cooperative architecture of data offloading and sharing for blockchain-based healthcare systems. *arXiv preprint arXiv:2103.10186*.

[38] Biswas, S., Sharif, K., Li, F., Alam, I., & Mohanty, S. P. (2020). DAAC: Digital asset access control in a unified blockchain based e-health system. *IEEE Transactions on Big Data*, *8*(5), 1273-1287.

[39] Pavithran, D. (2020). *Towards Building a Secure Blockchain-Based Architecture for Internet of Things (IoT)* (Doctoral dissertation, The British University in Dubai).