THE ASIAN BULLETIN OF BIG DATA MANAGEMENT
Vol.4. Issue4 (2024)
https://doi.org/ 10.62019/abbdm.v4i4.279

A Survey on the Internet of Medical Things (IOMT) Privacy and Security: Challenges Solutions and Future from a New Perspective

Mubbara Maqsood*, Muhammad Mohtisham Dar, Syed khawar Hussain Shah, M. Aetsam Javed, Hamayun Khan

Chronicle

Article history

Received: Oct 12, 2024
Received in the revised format: Oct 29, 2024
Accepted: Nov 11, 2024
Available online: December 20, 2024

Mubbara Maqsood is currently affiliated with Department of Computer Science, Faculty of Computer Science & IT Superior University Lahore, 54000, Pakistan
Email: mubbara2244@gmail.com

Muhammad Mohtisham Dar, M. Aetsam Javed, and Hamayun Khan are currently affiliated with Department of Computer Science, Faculty of Computer Science & IT Superior University Lahore, 54000, Pakistan
Email: mohtashamdar199@gmail.com
Email: SU92-PHCSW-F24-023@superior.edu.pk
Email: hamayun.khan@superior.edu.pk

Syed khawar Hussain Shah is currently affiliated with Department of Computer Engineering, Bahria University, Islamabad, Pakistan
Email: skhawar.h11@bahria.edu.pk

Corresponding Author*

Abstract

The Internet of Medical Things (IoMT), an application of the Internet of Things (IoT) in the medical domain, allows data to be transmitted across communication networks. In particular, IoMT can help improve the quality of life. With the advent of the Medical Internet of Things or MIOT, billions of people's health, safety, and care are being improved. Rather than requiring patients to visit the hospital for assistance, their health-related parameters can be tracked remotely, continuously, and in real-time., which significantly improves the effectiveness, convenience, and cost performance of healthcare. Data transmission over communication networks is made possible by the Internet of Medical Things (IOMT), an application of the Internet of Things (IoT) in the medical field. Specifically, IOMT can enhance citizens' and senior citizens' quality of life by tracking and controlling the vital signals of the body, such as heart rate, temperature, and blood pressure, among others. IOMT has emerged as the primary forum for exchange. A total of 187 articles in all, published between 2010 and 2022, are gathered and arranged based on the variety of applications, year of publication, type of applications, and other unique viewpoints. This study provides a broad overview of the state-of-the-art methods by reviewing the security and privacy issues, requirements, risks, and future research objectives in the field of IOMT.

Keywords: Security, privacy, Internet of Medical Things, IOMT, MIOT, healthcare systems, survey.

INTRODUCTION

The third wave of Internet expansion is thought to be the Internet of Things (IoT). The medical internet of things is a collection of Internet-connected devices used to carry out procedures and provide services that aid in healthcare [1]. With the use of tiny wearable devices or implanted sensors. MIOT has become a new e-healthcare technology that gathers patients' essential bodily data and tracks their pathological information. MIOT covers a wide range of applications, from wireless body area networks (WBAN) to implantable medical devices, and has demonstrated considerable promise in improving people's health. The Internet of Medical Things, or IOMT, is a global network of interconnected medical devices that anybody, anywhere, at any time, can access [2, 3]. Its development and growth are revolutionizing the healthcare sector. In terms of wellness services that inspire millions of people worldwide to adopt healthier lifestyles, the e-health IOMT-based application landscape has taken a stunning lead [4, 5].

In this regard, healthcare services have evolved into user-centered, accurate,

pervasive, and customized services, such as 24-hour private healthcare. The wide range of advancements in the Internet of Things (IoT), also known as the Internet of Healthcare Things (IOHT) or the Internet of Medical Things (IOMT) are anticipated to significantly improve the efficiency and quality of care in the healthcare sector [6, 7]. Due to advancements in microelectronics, materials, and biosensor designs, smart wearable and implantable medical devices have garnered a lot of attention in recent years. However, due to IOMT's quick development, these IOMT-based healthcare systems' security and privacy have frequently gotten little attention. Inadequate security in IOMT healthcare systems can have the following effects. Since its beginnings, the IOMST has been at risk from cyber-attacks. Due to the absence of necessary security protection, various threats and attacks have the potential to cause major catastrophes for both individuals and the network. As a result, IOMST security and administration become very important. The doctor uses his digital signature and access credentials to recover the secure data [8, 9].

The suggested system is put into practice with inexpensive hardware and effective software, and it is safe for sending medical records. Data transmission over communication networks is made possible by the Internet of Medical Things (IOMT), an application of the Internet of Things (IOT) in the medical field. By tracking and controlling the body's vital signs, such as blood pressure, temperature, heart rate, and others, IOMT can specifically help residents and senior citizens live better lives. IOMT has emerged as the primary platform for exchanging information and reaching important decisions, therefore ensuring its security and dependability is essential [10, 11]. Many researchers are interested in the growth of IOMT in recent decades. Because IOMT technology is still in its infancy and has not developed sufficiently, there are security issues because of low standards, poor maintenance, and a lack of user education. With malware for ransom, hackers and opponents can quickly take over IOMT devices with inadequate protection. Through unencrypted transmission, hackers can gain access to unencrypted IOMT equipment [12].

Table 1.

A systematic breakdown of IoMT Healthcare Technology [13]

Technology	Description	Features	Platforms	Open Issues
Electronic Health Records (EHR)	Digital systems that store and manage patient health information	Secure sharing of information between healthcare providers	Modernizing medicine, Greenway health, GE centricity, and NextGen healthcare	Interoperability and data exchange between different systems
Medical imaging	Digital methods for visualizing and analyzing medical images	Integration with Electronic Health Records (EHRs) and remote monitoring	Cloud-based platforms, Mobile devices (smartphones, tablets), and Wearables (smartwatches)	Data privacy and security, interoperability, and the integration with existing healthcare infrastructure
Artificial intelligence	Machine learning to enhance health outcomes	Predictive analysis and early detection of potential health issues	Health applications and portals for patients and healthcare providers	Regulation and standardization of AI in medical applications
Blockchain	Technology for secure health data management through distributed ledgers	Eliminates the need for a central authority to manage the data	Ethereum, hyperledger, and corda	The decentralized characteristic of blockchain technology presents challenges in regulating data privacy, which is a significant issue in the healthcare sector
Telemedicine	Remote medical treatment through technology	Patients are able to track their essential vital signs, including blood pressure, heart rate, and oxygen levels, through the use of wearable devices	Telemedicine services can be accessed by both healthcare providers and patients through web-based portals	Guarantee the preservation of data privacy and security

IOMT edge networks could seriously jeopardize patient safety and privacy because they are susceptible to a variety of security risks. In light of this and the fact that security is a crucial component that is heavily reliant on the dependability of the IOMT devices involved, new security mechanisms are desperately needed to maintain the security of the IOMT edge networks to successfully integrate IOMT technology into widespread healthcare systems [14]. Many of the security schemes created for IOMT devices may also be used to protect medical devices. However, because of their small size and power requirements, wearable and implantable devices are typically constructed with very little funding, and they might not have enough to put those schemes into practice [15, 16]. To ensure the security of this new wave of medical technology, industry, academia, and standards groups must collaborate closely to develop new policies, guidelines, and standards in addition to increasing research into the privacy and security of IOMT devices computational and resource limitations of IOMT devices while maintaining security in IOMT edge networks, this work aims to better understand the threats to IOMT edge networks and the defenses against them, and provide a foundation for coordinating research efforts. We anticipate that this research will contribute to the development and implementation of secure IOMT. The following is a summary of our primary contributions [17-21].

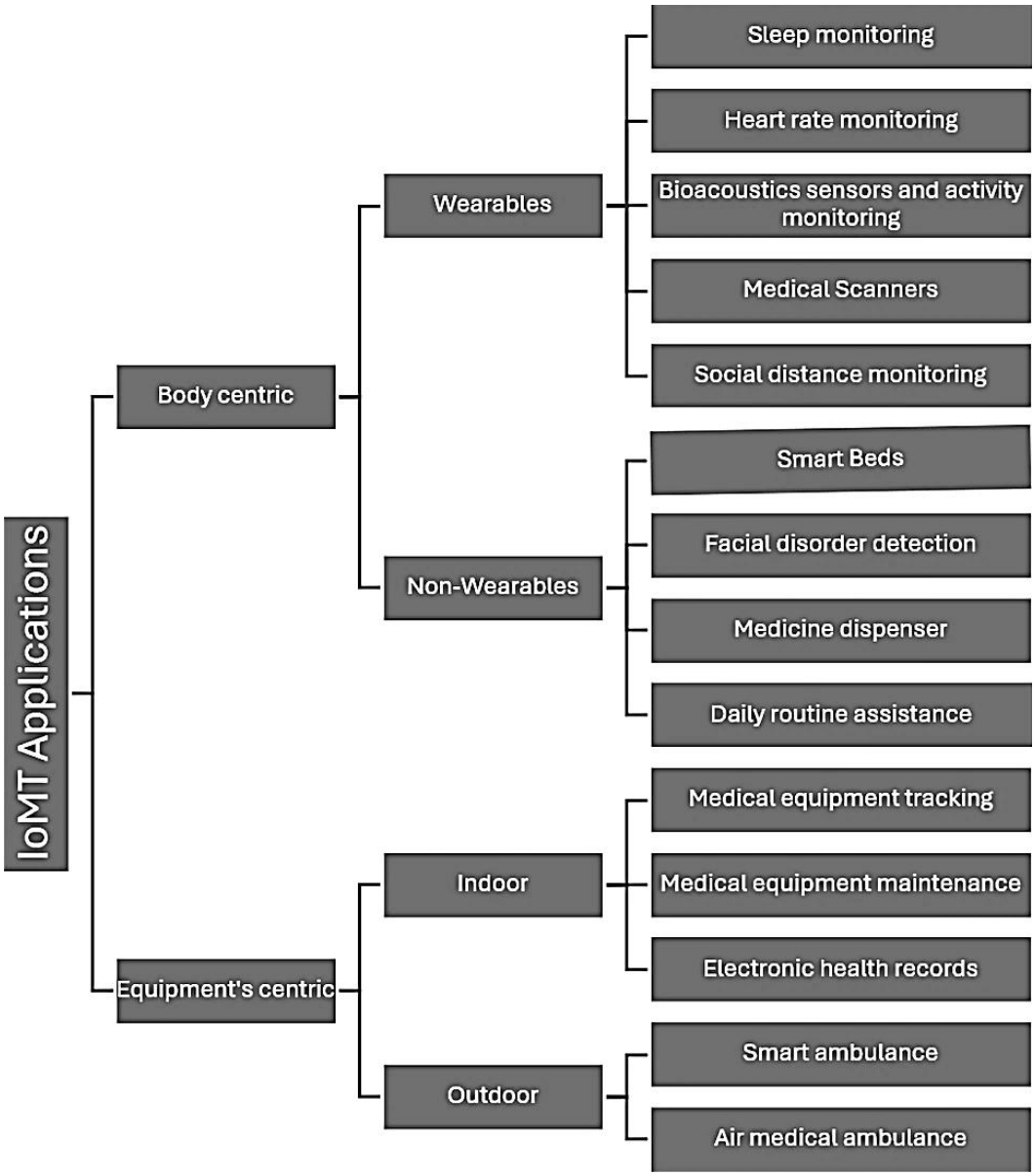

Figure 1.
Service-oriented IOMT architecture of IoT [22]

To design and develop suitable lightweight security mechanisms that overcome the We go over the security specifications required for IOMT systems and the various methods for ensuring safe data gathering as well as storage. We go over the various security methods that are available and how resilient they are to various kinds of attacks. We contend that no single method can offer complete defense against the majority of known assaults that target these systems. We examine the attack surface of IOMT and demonstrate how robust these security measures are against various assaults. This covers fresh assaults on IOMT systems that have surfaced recently. For the IOMT system, we provide a security architecture that makes use of some of these methods' characteristics. The security of IOMT systems during data collection, transmission, and storage is covered by this framework [23].

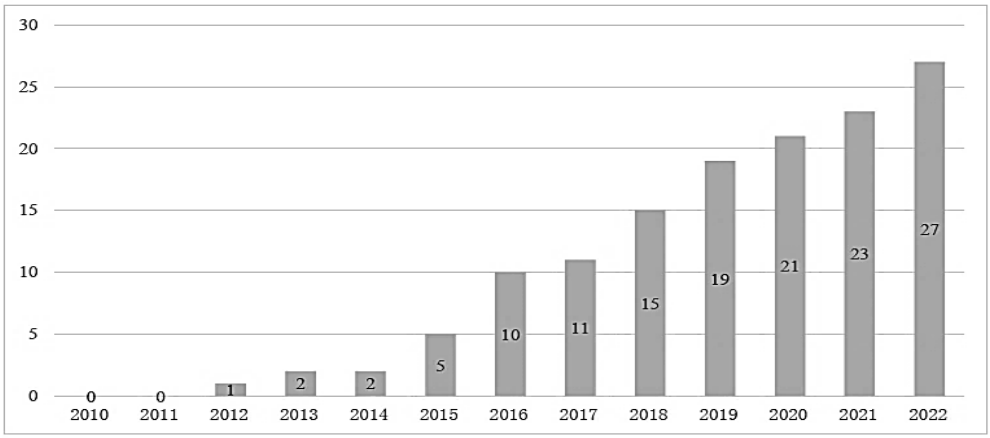

Figure 2.
IoT Enhancement [24]

Table 2.
A systematic breakdown of IoMT security risks [25]

Challenge	Description	Impact	Examples
Device Vulnerabilities	Limited computational capacity for robust security	Enables hacking and unauthorized access	Insulin pumps, pacemakers
Network Vulnerabilities	Insecure communication protocols between IoMT devices	Eavesdropping and data manipulation	Wi-Fi and Bluetooth
Data Integrity	Unintended data alteration or corruption	Loss of reliable medical records	Sensor data modification

LITERATURE REVIEW

A component of the larger Internet of Things (IoT), the Internet of Medical Things (IoMT) refers to the collection, storage, and transmission of health data via medical equipment and apps that are connected to the Internet. Through better patient management, diagnosis, treatment, and monitoring, this networked system improves the delivery of healthcare. IoMT includes technologies that help improve patient outcomes and healthcare efficiency, including as wearables, sensors, diagnostic equipment, and remote monitoring tools [26, 27]. Ensures that private information is not shared or made accessible to unapproved parties. Confidentiality in the context of the IOMT edge network refers to safeguarding patient medical information that has been shared with a therapist, doctor, or medical staff from being revealed to unapproved third parties who could endanger the patient or misuse it. An adversary could, for instance, obstruct communication between the sender (such as a medical IOT device) and the recipient (such as a smartphone gateway) to intercept medical data transmissions and obtain illegal information if the confidentiality of the data is not maintained. There are many different ways to guarantee confidentiality, from physical security to data rendered incomprehensibly by cryptographic methods [28, 29].

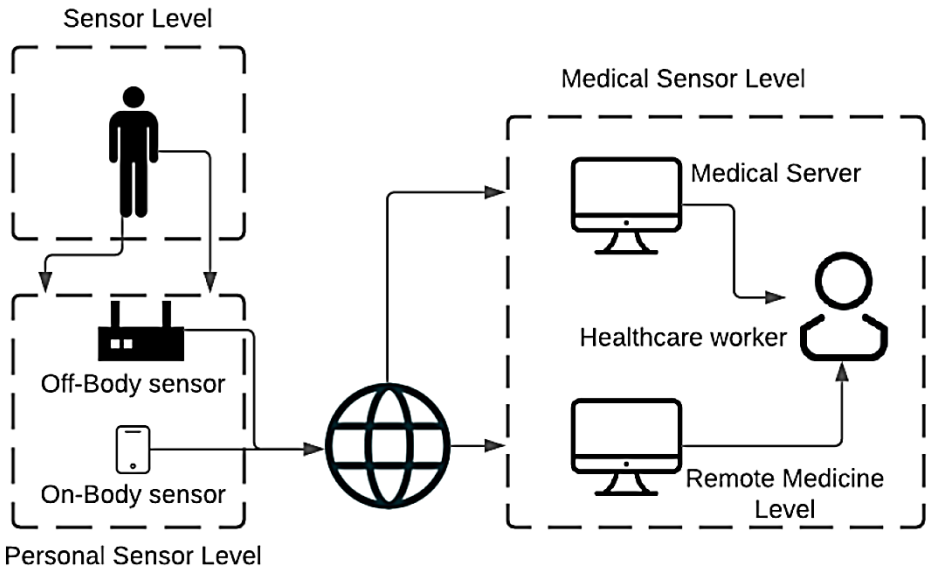

Figure 3.
IOMT Architectures [30]

Integrity

Guarantees that information hasn't been illegally changed or erased. Integrity, when applied to IOMT edge networks, maintains the veracity of patient-related data, including test results, clinical notes, health summaries, and personal medical information. Healthcare businesses now more than ever understand the value of data integrity, especially as a result of the growing reliance on networked data brought about by the integration of developing IOT technology in the healthcare industry. In addition to data integrity, the ideas of device and software integrity have also gained attention in the context of the IOMT edge network. The integrity of the equipment involved, such as wearable or implanted sensors, is also crucial to the healthcare industry's effective adoption of IOMT edge networks [31, 32]. Stops a party from retracting earlier promises or deeds during a conversation. For example, information taken from a patient's sensors may be sent, but the patient may later claim that the information is not his. Alternatively, a developer with permission may change the firmware in a few sensors and then reject its validity. It is necessary to provide a way to settle conflicts that develop when an entity denies prior commitments or specific approved actions. To settle such disagreements, a certain process including a reliable third party is frequently required [33].

Authentication

Pertains to both transmitted data message authentication and entities (identity authentication). The procedure by which one communicating entity is certain of the claimed identity of another entity engaging in the interaction and that the latter has truly participated is known as entity authentication or identification. The procedure by which an entity is confirmed to be the source of data generated at a certain point in the past is known as message authentication. Since many IoT devices lack the memory and CPU capacity to perform the cryptographic operations necessary for conventional authentication protocols, there is currently a trend toward lightweight authentication protocols [34]. Guarantee that systems function correctly and that authorized users are not denied access to services. As a result, medical data is always available and usable when a genuine organization requests it. Ensuring uninterrupted

device and network resource availability when a patient requires care services is crucial in the context of IOMT edge networks [35]. As more resource-constrained medical devices are linked to IoMT-based networks via wireless networks, there is a risk of security breaches by malevolent actors who take advantage of potential flaws in the system to launch attacks, obtain private data, or alter device operations and extract results. The generalized attack types that could potentially target IoMT edge networks are briefly described in this section [36]

Eavesdropping attacks

An attack that uses unprotected network connections to obstruct two entities' (like cellphones or sensor nodes') communication without their permission. To obtain valuable information that they can utilize to later pose as the claimant, the attacker surreptitiously listens in on the conversation. Since eavesdropping attacks don't alter network transmission, they are challenging to identify [37, 38].

Spoofing attacks

Intentionally causing a resource or item to behave incorrectly. An attacker might, for example, fabricate the transmission data's sending address to gain unauthorized access to a secure system. Both mimicking and piggybacking are seen as forms of spoofing [39].

Traffic Analysis Attacks

a type of passive attack where an attacker uses observable data flow features to infer information about the transmitted data. For example, when the data is encrypted, the information might not be readable or accessible. These attributes could include the names and locations of the entities participating in the data flow (i.e., its origins and destinations), as well as the presence, absence, amount, direction, frequency, and duration of the flow [40]. An attacker creates and runs malicious firmware or software to compromise a system's security. This firmware or software is frequently secretly added to another program to erase data, execute harmful or invasive programs, or jeopardize the privacy, correctness, or dependability of the system's data, apps, or operating system as a whole. Malicious mobile code, trojans, worms, and virus programs are common methods of malware attacks, horses, rootkits, or other malicious programs that effectively compromise a system [41]. This type of active attack occurs when a malevolent actor intercepts, compromises, or even hides messages sent back and forth between two authenticated entities (such as the claimant and the authentication protocol verifier). The hacker might change some of the transmitted data to pass for one or more of the relevant legal entities [42].

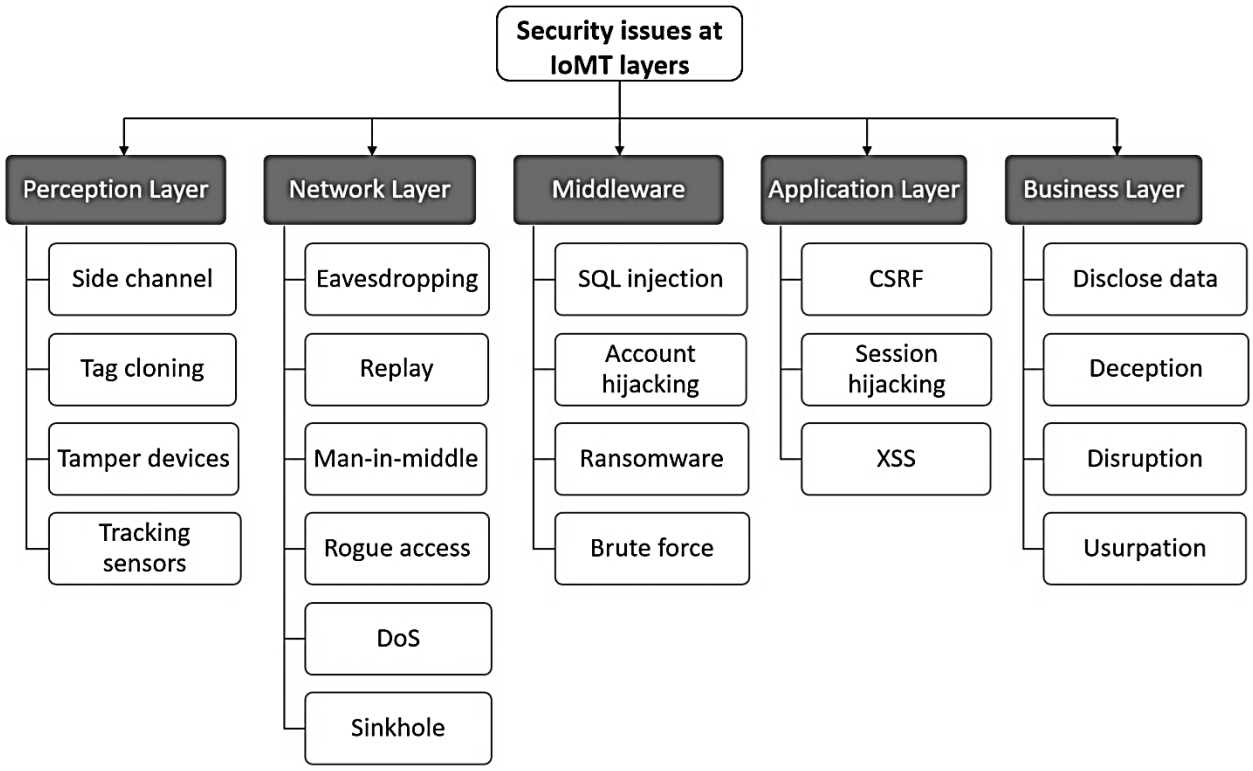

Figure 4.
IOMT Architectures with Security Issues [43]

RESEARCH METHODOLOGY

This To find security flaws, test innovative fixes, and assess their effectiveness, this study takes a multidisciplinary approach. The methodology, which focuses on machine learning, blockchain integration, and lightweight cryptography, consists of technical simulations, literature study, and prototype testing. The following sources were analyzed to ensure a thorough understanding of IoMT security challenges:

- Sources: We reviewed 187 articles spanning the period 2010–2022, analyzing topics related to IoMT security, including encryption, authentication, and network vulnerabilities.
- Scope: Studies on encryption techniques, blockchain adoption, and AI use in IoMT systems.
- Collected data from cybersecurity reports of healthcare organizations experiencing IoMT attacks.
- Notable cases include ransomware in IoT-connected hospital networks and attacks on wearable devices like fitness trackers.

The security challenges in IoMT were categorized as follows:

- Device Vulnerabilities: Issues in wearable devices and implantable sensors.
- Network Vulnerabilities: Threats during data transmission, such as eavesdropping and unauthorized access.

- Data Integrity Concerns: Risks associated with tampering or loss of sensitive data.

Table 3.
Security Aspects for IoMT systems [44]

Aspect	Protection mechanism	Description
Confidentiality	Confidentiality	Guarantees that a processed asset is not becoming known outside the interacting entities
	Authentication	Challenges credentials on the basis of identification and authorization
	Resilience	Preserves protection in case of failure
Integrity	Integrity	Guarantees that the interacting entities know when an asset has been changed
	Subjugation	Guarantees that transactions occur based on a defined process, removing freedom of choice and liability in the case of disclosure
	Nonrepudiation	Prevents the interacting entities from denying their role in an interaction
Availability	Continuity	Preserves interactivity in the case of failure
	Alarm	Informs that an interaction is happening or has happened
	Indemnification	Includes a contract between the asset owner and the interacting entity. It may also involve warnings as a precursor of legal action and public legislative protection

SIMULATION FRAMEWORK

To evaluate security techniques, a prototype IoMT network was set up comprising simulated medical devices (e.g., heart rate monitors, insulin pumps) and a healthcare cloud platform. Devices equipped with lightweight communication modules (e.g., LoRa, Bluetooth Low Energy). Simulated typical patient monitoring scenarios, such as data collection during remote monitoring.

- Security Tests
- Encryption Performance: Compared traditional methods (e.g., RSA) against lightweight alternatives like AES-256 and Elliptic Curve Cryptography (ECC).
- Blockchain Integration: Tested blockchain with decentralized authentication for access control and immutable logging of patient records.
- Anomaly Detection

- Developed AI-based models using supervised and unsupervised learning techniques for real-time intrusion detection.

Table 4.
IoMT security Model Comparison [43]

Year	Network model	Methods	Security models	Pros (+)	Cons (−)
2023	Internet of Things Smart Healthcare Financial System	Blockchain-based solution	Data privacy	+ The proposed system uses a blockchain-based zero-knowledge proof mechanism, which preserves the privacy of the users while sharing information between devices	− The scalability of the system may be limited due to the inherent characteristics of blockchain technology
2023	Healthcare Internet of Things network	Data aggregation	Privacy-preserving	+ Reduces the communication and computational cost compared to conventional methods	− The lack of real-world implementation
2023	Internet of Things-based smart healthcare	lightweight cryptographic primitives	Privacy-preserving	+ The security and performance analysis of the proposed authentication technique assesses its effectiveness over existing well-known schemes	− Reliability issues, limited accessibility, and high-cost communication
2023	Smart healthcare systems	Federated Learning	Privacy-preserving	+ FRESH effectively resists Source Inference Attacks (SIAs) by using certificates ring signature defense	− The proposed system is vulnerable to adversarial machine learning attacks
2022	Remote patient monitoring using IoT network	Elliptic Curve Cryptography-based solution	Privacy preserving	+ The proposed RPM system provides secure RFID based authentication, end-to-end secure communications, and privacy protection	− Reliability issues, limited accessibility, and high cost communication
2022	IoT-based healthcare	Homomorphic Encryption	Privacy-preserving	+ The proposed EPPADA scheme reduces energy consumption by eliminating redundant data through data aggregation	− The scheme involves the use of complex encryption and decryption methods

Experimental Setup and Metrics

The experimental phase evaluated three main areas: Ensured encrypted medical data could not be intercepted or decoded by unauthorized entities. Evaluated AI algorithms based on the detection of known and unknown threats, generating benchmarks for IoMT systems is presented in Table 5:

Table 5.
Benchmarks for IoMT systems [45]

Experiment	Metric	Outcome
AES-256 Encryption	Encryption Latency (ms)	3.5 ms (average)
Blockchain Authentication	Time to Authenticate (ms)	10 ms
AI Model Threat Detection	Detection Rate	92% (Average)

Below section presents the findings of this review (reporting the review). The outcomes of the selection process are first presented in their entirety, followed by individual reports of each research question's findings amount of sensors in our system, big data problem solving will be put into practice. Patients' medical records will be stored on a private blockchain.

Overview of the selected studies

This work addresses the issue of IOMST security by presenting a real-time security model with an authenticated encoded encryption technique. The two main concerns

facing the IOMST are real-time security and privacy. To encrypt a patient system using a rotational key, we first introduced a run-length encoding technique in this research used a rotating key to decrypt the data and a run-length decoding approach in the physician system. The patient's digital signature guarantees the accuracy of his medical record. Future research will amount of sensors in our system, big data problem solving will be put into practice. Patients' medical records will be stored on a private blockchain. The research paper on the role of IOMT ensures the safety and security of such systems. The development of new procedures, rules, and standards to guarantee the security of this new generation of medical technologies requires strong cooperation between the academic community, industry, and standard organizations due to growing research efforts in the security and privacy of IoMT devices.

The paper discusses the methods that give the system session-key agreement, forward/backward secrecy, authentication, authorization, confidentiality, integrity, and key-escrow resilience. By ensuring that these conditions are met, the system can withstand attacks such as physical security tokens, impersonation, manipulation, side channel, sniffer, MITM, relay, brute force, concurrent sessions, clock synchronization, and replay. The following issues could arise, nevertheless, because the methods in this section rely on pre-shared keys or starting arguments.

The paper also emphasizes the IOMT devices' network connectivity makes controlling and monitoring them easier, but it also often creates weaknesses in the network and the devices. IOMT devices may be subject to the same security risks and vulnerabilities as other IOT systems and devices. Because IOMT devices manage extremely private health data and some of them have life-sustaining actuation capabilities, security breaches on linked health equipment could directly and potentially kill users.

CONCLUSION

As the Internet of Medical Things (IoMT) gains ground, the integration with Circular Economy (CE) becomes popular. New business models and services are modeled, materializing, among others, remote sensing, assistance of elder people, and bioinformatics with crowdsourcing and Big Data. In conclusion, numerous software programs and medical gadgets are used to produce vast volumes of data and enhance the quality of medical services. Future related research will focus heavily on how to effectively protect data security and privacy at every stage of data flow. This study addresses the security and privacy concerns from five technological perspectives and outlines the obstacles to further research, beginning with the security and privacy requirements of MIOT. Although MIOT has received a lot of attention, more fruitful research is required since the associated standards and technical specifications particularly those pertaining to the unique application requirements of health care are constantly evolving.

DECLARATIONS

Acknowledgement: We appreciate the generous support from all the supervisors and their different affiliations.
Funding: No funding body in the public, private, or nonprofit sectors provided a particular grant for this research.
Availability of data and material: In the approach, the data sources for the variables are

stated.

Authors' contributions: Each author participated equally to the creation of this work.

Conflicts of Interests: The author declares that there is no conflict of interest related to this study. All research activities, data collection, and analysis were conducted with full transparency and impartiality. No financial or personal relationships that could influence the research outcomes exist. The findings and conclusions presented in this work are solely based on the data collected and the academic analysis carried out throughout the study.

Consent to Participate: Yes

Consent for publication and Ethical approval: Because this study does not include human or animal data, ethical approval is not required for publication. All authors have given their consent.

REFERENCES

[1] Reddy, B. I., & Srikanth, V. (2019). Review on wireless security protocols (WEP, WPA, WPA2 & WPA3). International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 5(4), 28-35.

[2] Halbouni, A., Ong, L. Y., & Leow, M. C. (2023). Wireless Security Protocols WPA3: A Systematic Literature Review. IEEE Access.

[3] Ambavkar, P. S., Patil, P. U., Meshram, B. B., & Swamy, P. K. (2012). Wpa exploitation in the world of wireless network. Int J Adv Res Comput Eng Technol, 1(4), 609-618.

[4] Cahyadi, D., Astuti, I. F., & Nazaruddin, N. (2023, February). Comparison of throughput and CPU usage between WPA3 and WPA2 security methods on wireless networks 802.11 n. In AIP Conference Proceedings (Vol. 2482, No. 1). AIP Publishing.

[5] Baray, E., & Ojha, N. K. (2021, April). WLAN security protocols and WPA3 security approach measurement through aircrack-ng technique. In 2021 5th International conference on computing methodologies and communication (ICCMC) (pp. 23-30). IEEE.

[6] Y. A. Khan, U. Khalil, H. Khan, A. Uddin, S. Ahmed, "Power flow control by unified power flow controller",sss Engineering, Technology & Applied Science Research., vol. 9, no. 2, pp. 3900-3904, Feb. 2019

[7] H. Khan, I. Uddin, A. Ali, M. Husain, "An Optimal DPM Based Energy-Aware Task Scheduling for Performance Enhancement in Embedded MPSoC", Computers, Materials & Continua., vol. 74, no. 1, pp. 2097-2113, Sep. 2023

[8] Khan, S., Ullah, I., Khan, H., Rahman, F. U., Rahman, M. U., Saleem, M. A., ... & Ullah, A. (2024). Green synthesis of AgNPs from leaves extract of Saliva Sclarea, their characterization, antibacterial activity, and catalytic reduction ability. Zeitschrift für Physikalische Chemie, 238(5), 931-947.

[9] S. Khan, I. Ullah, H. Khan, F. U. Rahman, M. U. Rahman, M. A. Saleem, A. Ullah, "Green synthesis of AgNPs from leaves extract of Salvia Sclarea, their characterization, antibacterial activity, and catalytic reduction ability", Zeitschrift für Physikalische Chemie., vol. 238, no. 5, pp. 931-947, May. 2024

[10] H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Dec. 2018

[11] Waleed, A. Ali, S. Tariq, G. Mustafa, H. Sarwar, S. Saif, I. Uddin, "An Efficient Artificial Intelligence (AI) and Internet of Things (IoT's) Based MEAN Stack Technology Applications", Bulletin of Business and Economics (BBE)., vol. 13, no. 2, pp. 200-206, July. 2024

[12] Liang, Y., Ur Rahman, S., Shafaqat, A., Ali, A., Ali, M. S. E., & Khan, H. (2024). Assessing sustainable development in E-7 countries: technology innovation, and energy consumption drivers of green growth and environment. Scientific Reports, 14(1), 28636.

[13] Noor, A. Ilyas, Z. Javaid, H. Khan, "Framing a Knowledge Domain Visualization on Green Human Resource Management: A Bibliometric Analysis from 2008-2022", Pakistan Journal of Humanities and Social Sciences., vol. 11, no. 4, pp. 4200-4212, Aug. 2023

[14] M. Gondal, Z. Hameed, M. U. Shah, H. Khan, "Cavitation phenomenon and its effects in Francis turbines and amassed adeptness of hydel power plant", In 2019 2nd International

Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-9, Mar. 2019
[15] Liang, Y., Ur Rahman, S., Shafaqat, A., Ali, A., Ali, M. S. E., & Khan, H. (2024). Assessing sustainable development in E-7 countries: technology innovation, and energy consumption drivers of green growth and environment. Scientific Reports, 14(1), 28636.
[16] U. Hashmi, S. A. ZeeshanNajam, "Thermal-Aware Real-Time Task Schedulabilty test for Energy and Power System Optimization using Homogeneous Cache Hierarchy of Multi-core Systems", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 4, pp. 442-452, Mar. 2023
[17] Y. A. Khan, F. Khan, H. Khan, S. Ahmed, M. Ahmad, "Design and Analysis of Maximum Power Point Tracking (MPPT) Controller for PV System", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 1, pp. 276-288, May. 2019
[18] Ali, M., Khan, H., Rana, M. T. A., Ali, A., Baig, M. Z., Rehman, S. U., & Alsaawy, Y. (2024). A Machine Learning Approach to Reduce Latency in Edge Computing for IoT Devices. Engineering, Technology & Applied Science Research, 14(5), 16751-16756.
[19] Khan, A. Yasmeen, S. Jan, U. Hashmi, "Enhanced Resource Leveling Indynamic Power Management Techniqueof Improvement In Performance For Multi-Core Processors" ,Journal of Mechanics of Continua and Mathematical Sciences., vol. 6, no. 14, pp 956-972, Sep. 2019
[20] Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Oct. 2018
[21] Akmal, I., Khan, H., Khushnood, A., Zulfiqar, F., & Shahbaz, E. (2024). An Efficient Artificial Intelligence (AI) and Blockchain-Based Security Strategies for Enhancing the Protection of Low-Power IoT Devices in 5G Networks. Spectrum of engineering sciences, 2(3), 528-586.
[22] H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, A. Saleem, "Performance Evaluation for Secure DES-Algorithm Based Authentication & Counter Measures for Internet Mobile Host Protocol", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 181-185, July. 2018
[23] Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.
[24] Khan, A. Ali, S. Alshmrany, "Energy-Efficient Scheduling Based on Task Migration Policy Using DPM for Homogeneous MPSoCs", Computers, Materials & Continua., vol. 74, no. 1, pp. 965-981, Apr. 2023
[25] Fakhar, M. H., Baig, M. Z., Ali, A., Rana, M. T. A., Khan, H., Afzal, W., ... & Albouq, S. (2024). A Deep Learning-based Architecture for Diabetes Detection, Prediction, and Classification. Engineering, Technology & Applied Science Research, 14(5), 17501-17506.
[26] Shah, S. Ahmed, K. Saeed, M. Junaid, H. Khan, "Penetration testing active reconnaissance phase–optimized port scanning with nmap tool", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-6, Nov. 2019
[27] Y. A. Khan, "A GSM based Resource Allocation technique to control Autonomous Robotic Glove for Spinal Cord Implant paralysed Patients using Flex Sensors", Sukkur IBA Journal of Emerging Technologies., vol. 3, no. 2, pp. 13-23, Feb. 2020
[28] Y. A. Khan, "A high state of modular transistor on a 105 kW HVPS for X-rays tomography Applications", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 1-6, Jun. 2019
[29] Khan, S. Ahmad, N. Saleem, M. U. Hashmi, Q. Bashir, "Scheduling Based Dynamic Power Management Technique for offline Optimization of Energy in Multi Core Processors", Int. J. Sci. Eng. Res., vol. 9, no. 12, pp. 6-10, Dec. 2018
[30] Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.
[31] Y. A. Khan, "Enhancing Energy Efficiency in Temperature Controlled Dynamic Scheduling Technique for Multi Processing System on Chip", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 46-53, Jan. 2019
[32] Khan, K. Janjua, A. Sikandar, M. W. Qazi, Z. Hameed, "An Efficient Scheduling based cloud computing technique using virtual Machine Resource Allocation for efficient resource

utilization of Servers", In 2020 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-7, Apr. 2020
[33] Hassan, H. Khan, I. Uddin, A. Sajid, "Optimal Emerging trends of Deep Learning Technique for Detection based on Convolutional Neural Network", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 264-273, Nov. 2023
[34] Khan, Q. Bashir, M. U. Hashmi, "Scheduling based energy optimization technique in multiprocessor embedded systems", In 2018 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-8, Sep. 2018
[35] Javed, M. A., Anjum, M., Ahmed, H. A., Ali, A., Shahzad, H. M., Khan, H., & Alshahrani, A. M. (2024). Leveraging Convolutional Neural Network (CNN)-based Auto Encoders for Enhanced Anomaly Detection in High-Dimensional Datasets. Engineering, Technology & Applied Science Research, 14(6), 17894-17899.
[36] Y. A. Khan, M. Ibrahim, M. Ali, H. Khan, E. Mustafa, "Cost Benefit Based Analytical Study of Automatic Meter Reading (AMR) and Blind Meter Reading (BMR) used by PESCO (WAPDA)", In 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-7, Aug. 2020
[37] Rahman, M. U., Khan, S., Khan, H., Ali, A., & Sarwar, F. (2024). Computational chemistry unveiled: a critical analysis of theoretical coordination chemistry and nanostructured materials. Chemical Product and Process Modeling, 19(4), 473-515.
[38] Naz, H. Khan, I. Ud Din, A. Ali, and M. Husain, "An Efficient Optimization System for Early Breast Cancer Diagnosis based on Internet of Medical Things and Deep Learning", Eng. Technol. Appl. Sci. Res., vol. 14, no. 4, pp. 15957–15962, Aug. 2024
[39] Khan, I. Ullah, M. U. Rahman, H. Khan, A. B. Shah, R. H. Althomali, M. M. Rahman, "Inorganic-polymer composite electrolytes: basics, fabrications, challenges and future perspectives", Reviews in Inorganic Chemistry., vol. 44, no. 3, pp. 1-2, Jan. 2024
[40] Naveed, A., Khan, H., Imtiaz, Z., Hassan, W., & Fareed, U. (2024). Application and Ethical Aspects of Machine Learning Techniques in Networking: A Review. Spectrum of engineering sciences, 2(3), 455-501.
[41] Sarwar, H. Khan, I. Uddin, R. Waleed, S. Tariq, "An Efficient E-Commerce Web Platform Based on Deep Integration of MEAN Stack Technologies", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 447-453, Jun. 2023
[42] Sebbar, A., Boulahya, S. E., Mezzour, G., & Boulmalf, M. (2016, May). An empirical study of wifi security and performance in morocco-wardriving in rabat. In 2016 International Conference on Electrical and Information Technologies (ICEIT) (pp. 362-367). IEEE.
[43] Apthorpe, N., Reisman, D. and Feamster, N., 2016. A smart home is no castle: privacy vulnerabilities of encrypted IoT traffic, Workshop on Data and Algorithmic Transparency (DAT), New York, USA, 19 November.
[44] [48] Zhou, W. and Piramuthu, S., 2014. Security/privacy of wearable fitness tracking IoT devices, CISTI, IEEE, Barcelona, Spain, 18-21 June, pp. 1-6.
[45] [49] Perera, C., 2017. Privacy guidelines for Internet of Things: a cheat sheet, Technical report, New Castle University, UK, pp. 1-9.