Track 1: Sustainable Communication Technologies

A Systematic Literature Review on the Privacy and Security of Cloud-Integrated AI-Enabled Internet of Medical Things (IoMT)

Sabarna Sarkar[1], Saptarshi Roychowdhury[2,*], Binod Kumar Singh[3]
National Institute of Technology Jamshedpur, Adityapur, Jamshedpur, Jharkhand 831014, India
[1] 2023pgcscs003@nitjsr.ac.in, [2] 2020rscs001@nitjsr.ac.in,
[3] bksingh.cse@nitjsr.ac.in
* Corresponding author: Saptarshi Roychowdhury, 2020rscs001@nitjsr.ac.in

Abstract. The continuous development of Cloud computing and the Internet of Things accelerates the development of the revolutionary Internet of Medical Things. The seamless integration of cloud platforms into the Internet of Medical Things framework has structured the healthcare data management, processing, and real-time analytics. Cloud services provide a scalable, secure, and cost-effective infrastructure for storing, processing, and analyzing the vast volumes of data generated by Internet of Medical Things devices. However, this integration also introduces privacy and security concerns, as data becomes increasingly intertwined with cloud-based system integration. This systematic review meticulously examines the challenges and enhancements of privacy and security in a Cloud-Integrated Internet of Medical Things system. It identifies and analyzes, through four research questions, a wide spectrum of potential threats like unauthorized access to sensitive data, data breaches, device manipulation, and privacy violations and provides some enhancement on existing systems to tackle those issues efficiently.

Keywords: Internet of Things, Internet of Medical Things, Cloud Computing, Privacy, Security, Attacks

1 Introduction

Modern society has opted for the digital way [1] of well-being by using significant technologies. As part of the digitized society, healthcare is developing faster than ever. Cloud technology streamlines data administration, processing, and real-time analytics. To maximize cloud-based medical technology utilization, IoMT is an advanced medical system that integrates IoT with medical equipment. This system changes patient care and healthcare delivery. Cloud and AI platforms' easy integration with the IoMT framework allows for scalable, secure, and cost-effective infrastructure for managing high amount of healthcare data generated by the various operations of IoMT devices. However, health data contains personal information, medical history, etc., raising privacy and security concerns. Any unwanted access to these critical data

could lead to harm the user identity by data theft, extortion, or affecting patient health directly.

Cloud-based IoMT architecture privacy and security are examined in this systematic review. Cloud technologies and healthcare data privacy and security issues are examined here. Exploitable threats and vulnerabilities are investigated here. These problems were identified and analyzed to provide a full understanding of crucial features of medical data protection in a Cloud-based IoMT system. This review also examines novel Cloud-Integrated IoMT architecture privacy and security solutions. These solutions include access control, data encryption, device authentication, network security, and vulnerability management. As AI-enabled IoMT is evolving quickly and will continue to do so, future research areas and enhancements like homomorphic encryption, distributed machine learning models, and blockchain were identified to improve the system's sensitive data security.

2 Research Question

This study investigates the privacy and security challenges of Cloud-Integrated AI-Enabled Internet of Medical Things (IoMT) systems, with a focus on identifying threats and proposing advanced solutions. The following research questions guide the investigation:

RQ1: How can privacy challenges in IoMT systems be effectively addressed to ensure data confidentiality and compliance with regulations?

RQ2: What are the most critical security threats in IoMT systems, and how can emerging technologies mitigate these risks?

RQ3: How can privacy and security be balanced in AI-enabled IoMT systems without compromising efficiency?

RQ4: What future technologies can revolutionize privacy and security in IoMT systems?

These questions provide a foundation for systematically analysing the current challenges, emerging threats, and potential solutions to safeguard sensitive healthcare data in IoMT ecosystems.

3 Background

3.1 Internet of Things

The IoT allows connection and data exchange between physical devices like sensors and actuators with embedded systems. A smarter environment can be delivered, and better productivity can be achieved by using physical systems to connect with computer systems. Wi-Fi, Bluetooth, and Zigbee data-sending methods are used in IoT Systems. This data can measure and show performance or trigger inaction. Things like a smart thermostat can track parameters such as temperature and humidity of the room and adjust air conditioner temperatures. The potential of IoT is enormous,

although it's still at a nascent stage. For example, IoT devices can monitor some physical parameters of the health-oriented objects in healthcare so that doctors can follow patients and preliminary data before they diagnose a disease.

3.2 Application of Internet of Things

The IoT can be found in various types of industries, including Manufacturing, Transport, Retail, Agriculture, Healthcare, etc. Some significant IoT applications are discussed briefly here. IoT devices can monitor machine performance and productivity in manufacturing. They can also warn of imminent machine failure so it can be replaced. For example, machine temperature can be measured with LM35 [2] or comparable sensors. If a machine's temperature exceeds a specified level, it might alert and shut down. Integration of IoT in Transportation [3] improves traffic flow, reduces accidents, and optimizes routes. Sensors can monitor traffic data in real-time in a selected area, enabling traffic lights to be adjusted to move traffic based on this data efficiently.

IoT applications in retail [4] include smart shipment, inventory tracking, improved customer service, and personalized marketing campaigns, as seen in Flipkart's smart shipping. IoT is also applied in Agriculture [5], where it can optimize irrigation systems and monitor crop health. For instance, DHT11 can assess soil moisture [6]. Such data can automate irrigation systems, preventing crop overwatering or underwatering. In Healthcare [7], IoT devices can remotely monitor patients' health attributes, improving outcomes and reducing costs while maximizing efficiency. Wearable gadgets can monitor heartbeat, blood pressure, and activity, with the data used to predict health issues and deliver individualized therapy. This system is often referred to as the IoMT.

There are many examples of IoT; these are just a few. As technology continues to develop, even more, innovative ideas are expected in the coming years.

3.3 Internet of Medical Things

The industry which is dedicated to the healthcare services today is having rapid growth, in turn, calling for security-apprentice sectors such as IoMT. In terms of Health, IoMT is a type of embedded system that can collect and transmit data about health. This data can help track patients' vitals. It can help in seeing the progress of treatment, as well as finding out a possible problem at its earlier stage.

The marketable devices are deployed in a number of healthcare environments like hospitals, medical centres and home care. IoMT devices, for example, can monitor patients' vital signs, follow up on the physical conditions of a patient in treatment, and detect health problems early [8].

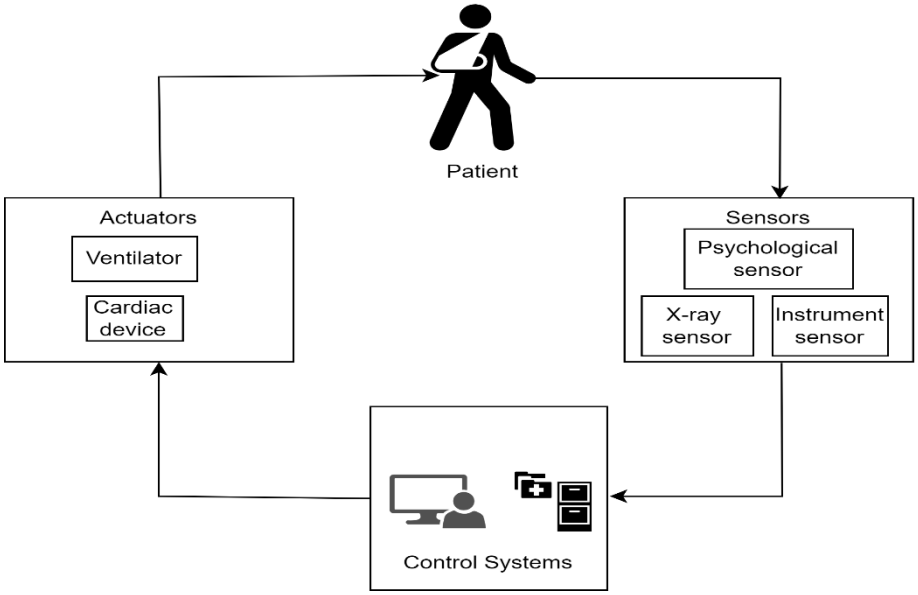

Fig. 1. Cloud Integrated Modern Healthcare System

As they streamline patient care, IoMT devices can support better outcomes for patients and lower healthcare costs overall, resulting in a higher quality of life. Moreover, IoMT devices are able to empower patients with their health. Some examples of IoMT devices are smart insulin pumps, which are used to monitor glucose levels for diabetic patients. Cardiac Monitor is an embedded IoT use case example for Wearable Devices. The adoption of IoMT devices is forecast to skyrocket in the years ahead. The key reason is massive growth among aging population, who are then requiring more medical services. Furthermore, improvements in technology make IoMT devices more reliable, efficient, and cheap, which makes them convenient to use.

3.4 Cloud Integration in IoT

This one is a bit more general, as it refers to the fact that cloud computing platforms are always used in tandem with IoT devices. IoT devices can collect, store and analyse huge amounts of data for instantaneous results through cloud technology. IoT solutions are made scalable and flexible through cloud integration, which allows organizations and consumers to control connected devices across the globe [9]. It also supports predictive analytics and smart decision-making using complex machine-learning algorithms and artificial intelligence. The link enhances IoT application performance and sparks applications for smart homes, healthcare, industrial automation, etc. It transforms raw data to actionable insights that modifies the way of our connected environment interact globally by means IoT cloud integration.

3.5 Cloud Integration in IoMT

Cloud integration in the Internet of IoMT, as shown in Fig. 1, connects medical equipment and systems to cloud platforms, changing Healthcare. Healthcare practitioners may safely collect, store, and analyze patient data with IoMT devices and cloud computing. This integration allows real-time patient monitoring, remote diagnostics, and predictive analytics, improving patient outcomes and personalizing Healthcare. Cloud-based IoMT solutions improve cooperation and decision-making by enabling healthcare professionals and patients to share medical data. The cloud also scales and stores medical device data, making it ideal for data management. IoMT uses cloud integration to make healthcare [10] more responsive, cost-effective, and patient-centered, changing the healthcare business.

3.6 AI Integration in IoMT

So, Artificial Intelligence leveraged across IoMT, as shown in Fig. 2, can be a game changer for the healthcare industry by making smarter and connected medical devices capable of collecting data more match data analysis in the same manner they distribute. Through the use of AI algorithms (commonly machine learning and deep learning) on huge volumes of data created by IoMT devices, healthcare providers are able to collect real-time information about a patient's state(s), forecast future health conditions, and customize treatment strategies. Remote patient monitoring and telemedicine.

AI technology primarily helps improve diagnostics, resulting in faster diagnoses, which means a lesser number of hospital visits and reduced operational costs. It also provides improved patient outcomes and engagement, data-drive decision-making as well as security & privacy for handling sensitive health information.

4 Privacy in IoMT

Privacy in IoMT is a critical concern as the data collected and transmitted by IoMT devices are sensitive. These data contain a variety of personal health information like heart rate, blood pressure, etc., which are sensitive critically. These data must be protected from unauthorized access, disclosure or modification.

4.1 Privacy Challenges in IoMT

Privacy challenges in IoMT [11] emulate significant concerns for patients and healthcare providers. The IoMT devices are very much vulnerable to various cyberattacks like malware infections, data breaches, etc. and it is a major issue. From another point of view, there lies a high need to protect the data because of the risk of unauthorized access and misuse of data, as the data sharing is done among healthcare providers, researchers, and different vendors. The lack of transparency of data flow in an IoMT system emphasizes the urgent need for privacy policies and transparent

practices in the IoMT system. This section attempts to address some significant factors behind privacy issues in the IoMT ecosystem.

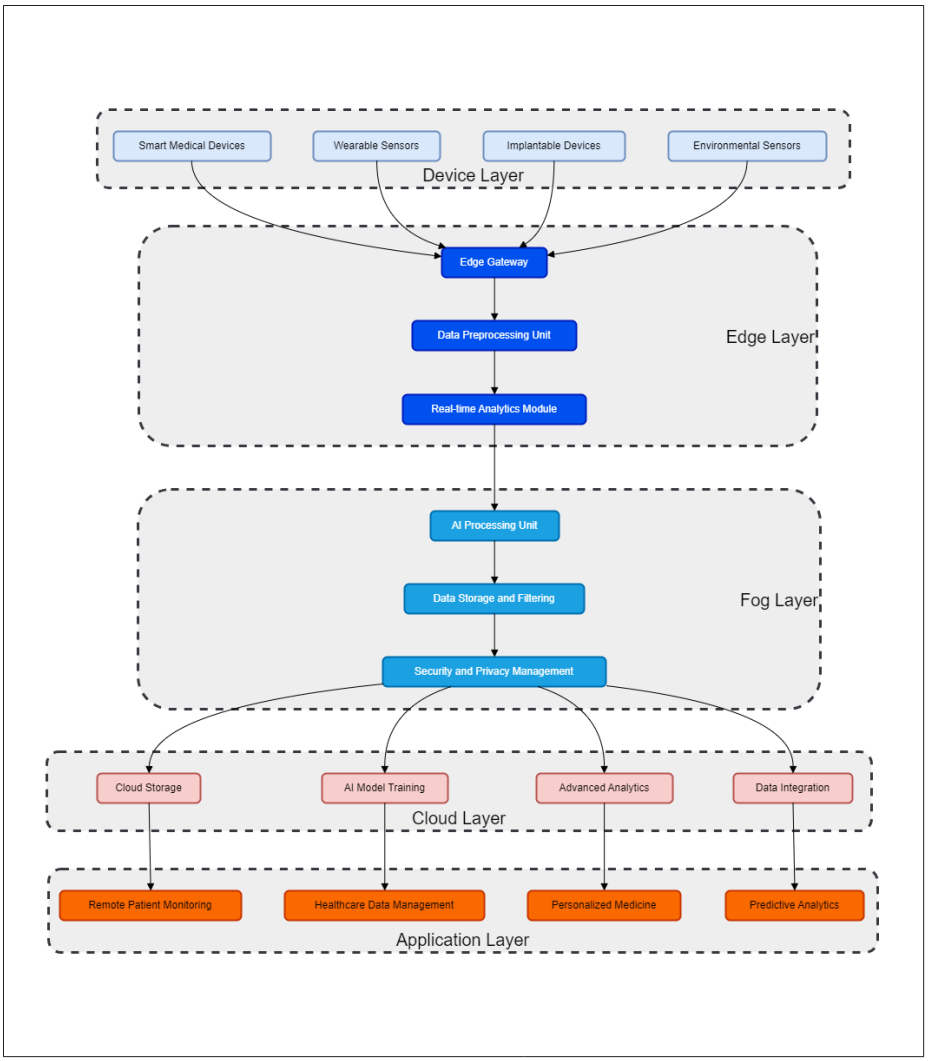

Fig. 2. Architecture of AI-Enabled IoMT

While considering Data Security, IoMT devices are very susceptible to malware infections and can be prone to cyberattacks in which patient reports, charts, or other critical information may become available for unauthorized users. This type of attack shows that businesses must ensure having strong cybersecurity measures in place to

shield them from range of threats regardless of the name or classification, and protect their data integrity and confidentiality.

In case of Data Sharing, IoMT data are often shared with healthcare providers, researchers and third-party vendors. The more data shared, the chances of unauthorized access to and misuse of patient information are increased. There is a need for efficient protocols and provenance of data flow, as well as secured channels in place to control them from sharing the confidential information of patients or using the crowd resources with unauthorized access.

Data de-identification and anonymization, while the removal of personally identifiable information (PII) from IoMT data, is a privacy safeguard that denies linking data to individual patients for research or care purposes. This means protecting the privacy of patients is important in choosing an appropriate method to ensure that data remains usable for insights. However, it can be challenging as some advanced techniques used to maintain data utility are nearly unbreakable in terms of anonymizing patient identifiers.

Lack of Transparency and control, often patients do not have transparency (which means visibility) into how their IoMT data is being collected used or shared. Without administration or preservation authorities, internet patients lose trust and cannot properly determine the level of privacy regarding their data. Transparent data practices that provide control mechanisms to patients will help build trust in a gateway application and increase the likelihood of engaging consumers with their healthcare privacy.

4.2 Privacy Enhancement in IoMT

IoMT privacy improvement involves multiple solutions. First, IoMT devices and networks must be protected from cyberattacks via strong passwords, encryption, and firewalls. Data optimization reduces sensitive data kept and transmitted by gathering just what is needed. User authentication and role-based access control (RBAC) restrict patient data access to authorized workers [12]. Encrypting IoMT data at rest and in transit with strong algorithms and protocols adds security. Data deidentification and anonymization eliminate personally identifiable information (PII) with keeping data useful for analytics and healthcare. Patient consent is required before data collection and clear privacy policies alert patients about various usage of data like collection, utilization, and sharing. Patient education and empowerment programs emphasize data protection and give patients options to control their data-sharing preferences, encouraging confidence. Complying with privacy laws like HIPAA [13] in the US and GDPR [14] in the EU promotes a secure and privacy-conscious IoMT environment. The following section briefly discusses significant privacy measures for IoMT.

Cybersecurity Measures: There is need for strong Passwords & Encryption-Firewalls should be established to protect IoMT devices as well as networks from cyber threats and attacks.

Data Minimization: This is the approach of collecting as little data as needed. This enables of storing and transmitting less sensitive information which lead to being only minimally harmed by breaches.

Access Control to Data: It is always important to implement RBAC and user authentication by having strong policies that allow access by only authorized users. This helps to protect patient data and reduces the chance of occurrence of data breaches.

Data Encryption: Encrypt IoMT data at rest and in transit with strong encryption algorithms & secure protocols, adding a layer of security against unauthorized access.

Data De-identification and Anonymization: Use automated techniques to remove personally identifiable information (PII) from data that will still be useful for research, healthcare delivery or other purposes. Balancing privacy with utility in generating deidentified health data is never easy.

Data Transparency: Clearly written privacy policies that state explicitly to patients how data is collected, used and shared. Get prior approval of patient data using it based on the given advice, transparency, and true decision-making.

Empowering the Patient: Teach patients that data privacy is important and provide on-ramps to adjusting their data-sharing settings. Creating the trust that patients need to stay in control over their personal health data, and thus engaging with the IoMT ecosystem.

Compliance with Privacy Regulations: Adhering to privacy laws such as the Health Insurance Portability and Accountability Act (HIPAA) in the case of the United States or the General Data Protection Regulation (GDPR) in the case of the EU, ensuring legal compliance providing the required safeguarding for data communications over this vast landscape governed under IoMT.

RQ1: How can privacy challenges in IoMT systems be effectively addressed to ensure data confidentiality and compliance with regulations? Privacy challenges in IoMT systems arise from vulnerabilities in data security, sharing protocols, and transparency issues. Measures like encryption, anonymization, and compliance with GDPR or HIPAA are essential for safeguarding sensitive patient data. Innovative solutions, such as federated learning and privacy-preserving AI models, can further enhance data protection by reducing reliance on centralized data processing.

5 Security in IoMT

The amount of sensitive data collected by health trackers and other IoMT devices means that the security requirement in this domain is paramount. The diversity of devices, limited resources and legacy systems are all challenges to IoT equipment integration. Malware, Data breaches, and DoS are just a few information security risks associated with exposed vulnerabilities on an IoMT device. Mitigation strategies with robust device security measures, network security, data encryption and watermarking, vulnerability management, employee training are some standard processes to minimize the risk [15][16].

5.1 Security Challenges in IoMT

Advancements in technology have made the IoMT a discipline that is now being developed at an increasingly fast pace. Nevertheless, there is a need to appreciate and

mitigate the challenges associated with it. The challenge in dealing with IoMT devices lies in their sophistication and reliability. The problems with IoMT systems are many and include old software hardware, compatibility issues, security flaws, cloud intrusions [17], password difficulties, low-end worms, etc.

Moreover, IoMT discrepancies can arise from untrustworthy communication, difficulties in determining device effectiveness, automation systems for data management, limited IoMT device management, lack of support for low-power networks, IoMT operating systems, and processor-related issues.

5.2 Different Types of Security Threats in IoMT

The IoMT security concerns (Fig. 3) can endanger patient data, device operation, and healthcare infrastructure. Malware infections are frequent and can compromise IoMT devices and steal patient data. Hackers exploit IoMT devices or network weaknesses to steal patient data, jeopardizing privacy and confidentiality. Traffic flooding from DoS attacks can affect IoMT devices and networks. MitM attacks can intercept and manipulate data communications between IoMT devices and other systems. Physical hazards like theft or tampering might impair device and data security. Insider threats, inadequate authentication, lack of encryption, software vulnerabilities, supply chain assaults, and regulatory compliance risks exacerbate IoMT security issues. To protect the IoMT devices and security-privacy sensitive data, strong security mechanisms and best suited practices are needed. The following section discuss significant attacks in brief.

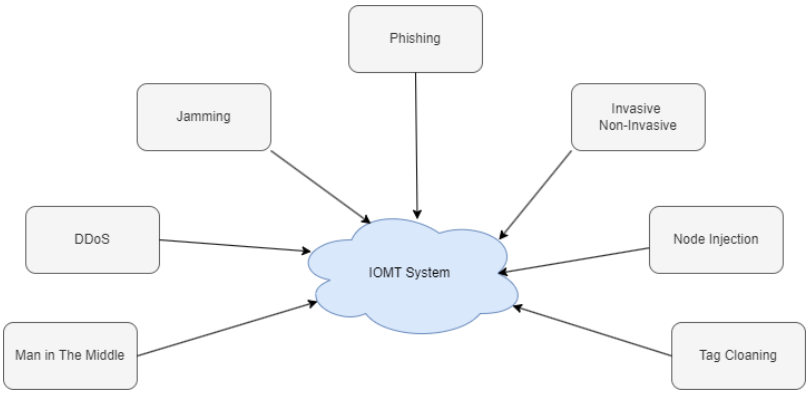

Fig.3. Threats in the IoMT System

Invasive attacks require physical access or intrusion into targeted devices and demand high skills along with the help of specialized tools. These attacks are executed by approaching the hardware of the devices directly. In the other hand, the non-invasive attacks harm IoMT devices through their input interfaces without physically disturbing the hardware setup.

The Jamming attacks aim to harm the wireless communication of IoMT devices by using malicious nodes in attempt to generate noise signals. Reactive jamming attacks produce noise signals only when the transmission channels are actively used for communication.

The Node Injection attacks aim to disrupt IoMT network wireless communication by using malicious nodes to generate noise signals. Instead of using original nodes, this attack uses the malicious nodes to hamper the normal workings of IoMT network.

The Sleep Denial attack disrupts the sleep mode of IoMT devices, keeping them awake to increase battery consumption. By transferring unauthenticated packets, these attacks drain the device's battery and potentially compromise its security as well as the performance capability. Intruders inspect the IoMT networks to determine when to inject these packets, causing more battery wastage with potential security vulnerabilities. This disrupts the system working along with the lesser data privacy and security.

The Denial of Service (DoS) attacks in the IoMT network can compromise patient safety and critical healthcare services by flooding the devices and systems with traffic. Multiple-source Distributed Denial of Service (DDoS) attacks can affect badly the patient care and therapies. Permanent Denial of Service (PDoS) attacks which is often known as "Brick Attacks," damage systems permanently and require repair or replacement of hardware. To mitigate these attacks, the healthcare staff must be educated about cybersecurity best practices, network segments, access controls, and regular updates. Various technology education programs aid towards this.

The traffic analysis attack on IoMT network involves monitoring network traffic to extract sensitive information without accessing the actual data directly. To mitigate these attacks, the professionals use encryption with anonymization and traffic inspection techniques.

The Man-in-the-middle (MitM) attack in the IoMT, attacker intercepts and alters communication between two devices or systems without their knowledge. This assault can arise in IoMT when medical devices, wearables, and patient monitoring systems exchange data. MitM attacks in healthcare could manipulate patient data, access confidential data, or interrupt crucial medical equipment functions.

Sinkhole and wormhole attacks threaten IoMT cybersecurity. Sinkhole attacks allow malicious actors to intercept, change, or block data by redirecting network traffic from legitimate devices to their own, and this can provide illegal access to medical data or device modification. However, wormhole attacks allow malevolent nodes to communicate covertly, bypassing routing systems and potentially compromising data integrity and confidentiality. Strong security mechanisms like encryption, authentication, access control, intrusion detection systems, and frequent security audits and vulnerability fixes can reduce these dangers.

Table 1. Significant research findings on the Security and Privacy of IoMT

Article Reference	Main Findings
George et. al. [18]	This paper focuses on the healthcare domain's Connected Environment (CE). It covers protection mechanisms throughout the data lifecycle, from device to cloud (E2E)
S. M. Riazul et. al. [19]	This paper introduces the Internet IoT as a transformative trend connecting smart devices across various sectors.
Dimitris et. al. [20]	The study delves into the inherent security traits and constraints of IoMT-specific communication protocols by analyzing practical attacks.
Ioannis et al. [21]	This paper focuses on categorizing IoT communication protocols in the context of their application in the IoMT.
Kuan Zhang et. al. [22]	This paper focuses on a survey on Sybil's attacks and their defense.
Da Yin et. al. [23]	This paper focused on detecting and mitigating DDoS attacks using the SD-IoT framework.
Noshina et. al. [24]	The paper proposes MCTM for IoT SN trust assessment. MCTM uses mobile code to visit SNs and gather trust-related information. It improves over SDN-based management.
Liang Liu et. al. [25]	This work proposes Perceptron Detection (PD) and Perceptron Detection with enhancement (PDE) models for improving IoT network security against insider attacks.
William J. et. al. [26]	This paper examines current methods aimed at minimizing the privacy implications of location tracking. It introduces a new encryption technique to safeguard user location and trajectory information using Privacy-Enhancing Technologies.
Chakib Bekara [27]	This paper discusses about different security challenges in IoT based Smart grid.
Miguel López et. al. [28]	It provides a description of an epidemic method being used to analyse the working conditions of jamming attacks, which tends to impact across all communication layers in all nodes, independent of the device complexity and computing power, in diverse IoT wireless networks.
Haibo Yi et. al. [29]	This paper discusses about vulnerability of RSA and ECC signatures to quantum attacks.
Samuel et al. [30]	This paper explores IoT application domains and cybersecurity challenges, focusing on firmware, hardware, and software infrastructure setups.
Mikko et. al. [31]	The paper focusses on the latter by proposing a way to find tags with identical identifiers. This fixed code is fine for cheap tags, since it always writes a new random number to the tag's memory each time it is scanned.

In the IoMT, Phishing attacks use electronic communication to mislead healthcare workers or patients into supplying sensitive information or access credentials. In IoMT, phishing attempts might use emails, texts, or bogus websites to get recipients to click on dangerous links or attachments.

Virus and Worm attacks in the IoMT can harm crucial healthcare infrastructure and sensitive data. Viruses attach to legal programs or files and spread when they are

executed. A virus could infect infusion pumps or patient monitors in IoMT, threatening their operation and patient safety. However, a worm is a self-replicating malware that spreads across networks without a host program. Worms can easily infect many devices and cause widespread damage in IoMT networks. They can disrupt Healthcare, steal patient data, or disable medical devices.

Table 2. Significant research findings on the Security and Privacy of IoMT

Attacks Vs Issues	Service Unavail-ability	Data Interc-eption	Unaut-horized Access	Data Manip-ulation	Data Corru-ption	Data Theft	Privacy Violat-ion	Service Disrup-tion	Device Malfn-ction
DoS/DDoS	✓							✓	
MitM		✓	✓	✓					
Malware	✓		✓	✓	✓			✓	✓
Ransom-ware	✓					✓	✓		
Phishing		✓	✓						
Replay			✓	✓					
SQL Injection			✓	✓					
Insider Attack			✓	✓		✓			
Firmware			✓						✓
Side Channel						✓	✓		

Firmware attacks target software-controlled medical devices, potentially compromising their functionality, stealing data, or rendering them unusable. To prevent such attacks, secure firmware update mechanisms, encryption, authentication, and regular security audits are crucial.

A Side-channel attack targets the physical implementation of a device to extract sensitive data, such as encryption keys. To prevent such attacks, devices should use strong physical security measures and robust cryptographic algorithms and undergo regular security audits.

Malware and spyware attacks involve malicious software that can infect devices, steal data, or disrupt functionality. These threats can be mitigated by using antivirus software, firewalls, and regular updates, as well as training users to recognize and avoid suspicious activities.

Table 1 and Table 2 state in brief the significant research findings on security, privacy and effects of attacks on the IoMT ecosystem.

RQ2: What are the most critical security threats in IoMT systems, and how can emerging technologies mitigate these risks? IoMT security threats include malware, DoS attacks, and MitM attacks, which compromise patient safety and device functionality. Emerging solutions such as blockchain for immutable audit trails, multi-factor authentication, and AI-based intrusion detection systems are being explored to address these threats effectively. These technologies ensure secure communication, real-time threat detection, and proactive responses to attacks.

6 Privacy and Security in AI Enable IoMT

The collected health data that is much sensitive in nature, processed and transferred across different devices and networks in an AI-enabled IoMT ecosystem, privacy & security are paramount concerns. AI constitutes a much-needed addition to IoMT systems. However, it raises new patient data security challenges whilst boosting real-time monitoring capabilities, predictive analytics and personalized treatment possibilities in healthcare delivery [32][33].

6.1 Privacy in AI-enabled IoMT

Privacy protection of patient data from unauthorized access or release and safekeeping it in the hands of its intended recipient. The range of devices in an AI-enable IoMT (Wearables, Remote monitors and medical imaging-based scans), which all collect & sending personal health data endlessly. Often, this data includes personally identifiable information (PII) such as names of individuals, health records like diagnoses or personal medical history, and genetic details, which is why preserving privacy at all times from beginning to end in terms of data access management within healthcare services cannot be overstated [34].

In the effort to maintain the integrity of patient's data and their privacy, IoMT systems with AI capabilities need a strong method for encrypting data which mainly includes encryption during transit (along the sender side) as well as at rest [35]. Distributed AI systems can leverage the privacy-preserving benefits of federated learning, where data is processed on devices locally instead of sending raw data to a central server and running code in an isolated environment [36].

6.2 Security in AI-enabled IoMT

AI-enabled IoMT security means protecting the whole system from hacking, malware, or ransomware attacks. Since IoMT devices are interconnected, the attack surface is expanded providing more ways in for a malicious actor to take advantage of vulnerabilities. Also, artificial intelligence algorithms can be manipulated through previous adverse attacks that used bad data to create desired outputs of the models [37].

In addition, the security of the system needs to be enforced, and IoMT systems are required to provide strong authentication protocols, such as multi-factor authentication, in order to limit access [38]. It will also require continued vigilance against suspicious activity, AI-fed threat detection systems and frequent refreshes of software required to fend off the new adversities. In addition, following the best secure coding practices and regular security assessments would be an excellent solution that can be used to find some of these unknowns [39].

6.3 Balancing Privacy and Security

Balancing privacy and security in AI-enriched IoMT systems requires a multi-faceted approach comprised of technological defences, from encryption to advanced threat detection capabilities powered by artificial intelligence (AI) - alongside data governance policies that limit access while ensuring compliance with standards like GDPR or HIPAA [40]. In this way, healthcare providers gain the most from AI-enabled IoMT while reducing patient data privacy risks and systems security.

RQ3: How can privacy and security be balanced in AI-enabled IoMT systems without compromising efficiency? AI-enabled IoMT introduces advanced capabilities like real-time analytics and predictive diagnostics but increases the attack surface. Balancing privacy and security involve adopting federated learning, secure AI algorithms, and encryption technologies for data in transit and at rest. Advanced threat detection mechanisms powered by AI can simultaneously ensure efficiency and robust protection.

7 Future Directions and Emerging Technologies

The cloud-integrated IoMT landscape is quickly maturing, rising from the ashes of technical development and improved privacy and security. There are several promising new technologies that can be used to address the challenges and release this full utilization potential of IoMT in Healthcare.

7.1 Homomorphic Encryption

As discussed earlier, homomorphic encryption allows computation on encrypted data without decrypting it first. This approach could significantly improve data analytics in cloud-linked IoMT systems, providing secure analysis of MHDs containing personal information while ensuring patient privacy [41].

7.2 Federated Learning

Federated learning is a type of distributed machine learning technique that allows system nodes to jointly train a model without having to share the sensitive data of each party. This is especially important in the case of IoMT, where data privacy is being discussed against all. Federated learning approach where essentially the training of machine-learning models are done by mutual model updating on edge-devices based on locally processed data but preserving patients' privacy [42].

7.3 Blockchain Integration

IoMT architectures can use this immutable and transparent blockchain technology to maintain the quality of data, in terms of both reliabilities as well integrity. This makes it possible to create tamper-proof audit trails for healthcare data, providing traceability and provenance of the data from when it is first uploaded. Moreover, the blockchain helps to share and combine importantly secure information between physicians and healthcare providers that support care for not only current patients [43] [44].

RQ4: What future technologies can revolutionize privacy and security in IoMT systems? Emerging technologies such as homomorphic encryption, blockchain, and quantum cryptography have the potential to redefine privacy and security in IoMT. Homomorphic encryption enables computations on encrypted data, preserving confidentiality. Blockchain ensures tamper-proof data sharing, and quantum cryptography offers unparalleled security against modern computational threats. These advancements pave the way for a more resilient IoMT ecosystem.

8 Conclusion

The marriage of cloud computing and the Internet of IoMT together changed Healthcare, enabling data-driven decision-making and individualized care. But, of course, this advancement depends on protecting patient data. So, this paper reviews various privacy and security challenges in cloud-integrated IoMT, which highlight the need to ensure strong data protection from important health-related information. It is essential to have encryption in place, secure protocols and data anonymization done properly. Policy frameworks and international standards are needed to protect data privacy. By combining innovation with collaboration, emerging areas of privacy (within the realm of homomorphic encryption) and, security, technology, and smart contracts, methodological advances can be applied to tackle everything from fundamental questions about transition principles to compliance challenges. This way, patient privacy should include protecting patients and data security is required to achieve the full power of IoMT in healthcare.

References

[1] Choudhury, A., Roychowdhury, S., Singh, B. K., & Singh, T. P. Introduction to Digital Society: An Overview. Evolution of Digitized Societies Through Advanced Technologies, 1–6, (2022).

[2] Soni, G. Implementation of LM35 interfacing of temperature sensor with Arduino using LabVIEW 2015. 2022 IEEE Delhi Section Conference (DELCON), 1–3. IEEE, (2022).

[3] Singh, P., Elmi, Z., Meriga, V. K., Pasha, J., & Dulebenets, M. A. (2022). RThings for sustainable railway transportation: Past, present, and future. Cleaner Logistics and Supply Chain, 4, 100065, (2022).

[4] Kaur, J., Santhoshkumar, N., Nomani, M. Z. M., Sharma, D. K., Maroor, J. P., & Dhiman, V. Impact of Internets of Things (IOT) in retail sector. Materials Today: Proceedings, 51, 26–30, (2022).
[5] Kim, W.-S., Lee, W.-S., & Kim, Y.-J. A review of the applications of the internet of things (IoT) for agricultural automation. Journal of Biosystems Engineering, 45, 385–400, (2020).
[6] Melo, D., Silva, P., Costa, A., Delmond, J., Ferreira, A., Souza, J., Oliveira-Júnior, J., Silva, J., Rosa Ferraz Jardim, A., Giongo, P., Ferreira, M., Assunção Montenegro, A., Oliveira, H., Silva, T., & Silva, M. Development and Automation of a Photovoltaic-Powered Soil Moisture Sensor for Water Management. Hydrology, 10(8), (2023).
[7] Almotairi, K. H. Application of internet of things in healthcare domain. Journal of Umm Al-Qura University for Engineering and Architecture, 14(1), 1–12, (2023).
[8] Razdan, S., & Sharma, S. Internet of medical things (IoMT): Overview, emerging technologies, and case studies. IETE Technical Review, 39(4), 775–788, (2022).
[9] Javed, A., Malhi, A., Kinnunen, T., & Främling, K. Scalable IoT platform for heterogeneous devices in smart environments. IEEe Access, 8, 211973–211985, (2020).
[10] Roy, T., & Nahid, M. M. The IoMT and cloud in Healthcare: Use, impact and efficiency of contemporary sensor devices used by patients and clinicians. Proceedings of the 2nd International Conference on Computing Advancements, 426–434, (2022).
[11] López Martínez, A., Gil Pérez, M., & Ruiz-Martínez, A. A comprehensive review of the state-of-the-art on security and privacy issues in Healthcare. ACM Computing Surveys, 55(12), 1–38, (2023).
[12] Butt, A. U. R., Mahmood, T., Saba, T., Bahaj, S. O., Alamri, F. S., Iqbal, M. W., & Khan, A. R. An Optimized Role-Based Access Control Using Trust Mechanism in E-Health Cloud Environment. IEEE Access, (2023).
[13] Nosowsky, R., & Giordano, T. J. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) privacy rule: implications for clinical research. Annu. Rev. Med., 57(1), 575–590, (2006).
[14] Voigt, P., & Von dem Bussche, A. The eu general data protection regulation (gdpr). A Practical Guide, 1st Ed. , Cham: Springer International Publishing, 10(3152676), 10–5555, (2017).
[15] Roychowdhury, S., & Singh, B. K. A Hybrid and Multi-objective Approach for Data Leak and Tamper Detection in Healthcare Cloud Data. In Machine Vision and Augmented Intelligence: Select Proceedings of MAI 2022 (pp. 275–285). Springer (2023).
[16] Mandal, B. K., Roychowdhury, S., Majumder, P., & Das, A. Securing the Information Using Combined Method. In Advances in Data Science and Computing Technology (pp. 305–317). Apple Academic Press (2022).
[17] Das, A., Choudhury, S. R., Negi, A., & Choudhury, A. Security and Challenges in Cloud Computing. ICET 3, (2017).
[18] Hatzivasilis, G., Soultatos, O., Ioannidis, S., Verikoukis, C., Demetriou, G., & Tsatsoulis, C. Privacy for the Review of security and Internet of Medical Things (IoMT). 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), 457–464. IEEE, (2019).
[19] Islam, S. M. R., Kwak, D., Kabir, M. D. H., Hossain, M., & Kwak, K.-S. The internet of things for health care: a comprehensive survey. IEEE Access, 3, 678–708, (2015).
[20] Koutras, D., Stergiopoulos, G., Dasaklis, T., Kotzanikolaou, P., Glynos, D., & Douligeris, C. Security in IoMT communications: A survey. Sensors, 20(17), 4828, (2020).
[21Stellios, I., Kotzanikolaou, P., Psarakis, M., Alcaraz, C., & Lopez, J. A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. IEEE Communications Surveys & Tutorials, 20(4), 3453–3495, (2018).
[22] Zhang, K., Liang, X., Lu, R., & Shen, X. Sybil attacks and their defenses in the internet of things. IEEE Internet of Things Journal, 1(5), 372–383, (2014).

[23] Yin, D., Zhang, L., & Yang, K. A DDoS attack detection and mitigation with software-defined Internet of Things framework. IEEE Access, 6, 24694–24705, (2018).
[24] Tariq, N., Asim, M., Maamar, Z., Farooqi, M. Z., Faci, N., & Baker, T. A mobile code-driven trust mechanism for detecting internal attacks in sensor node-powered IoT. Journal of Parallel and Distributed Computing, 134, 198–206, (2019).
[25] Liu, L., Ma, Z., & Meng, W. Detection of multiple-mix-attack malicious nodes using perceptron-based trust in IoT networks. Future Generation Computer Systems, 101, 865–879, (2019).
[26] Buchanan, W. J., Kwecka, Z., & Ekonomou, E. A privacy preserving method using privacy enhancing techniques for location-based services. Mobile Networks and Applications, 18, 728–737, (2013).
[27] Bekara, C. Security issues and challenges for the IoT-based smart grid. Procedia Computer Science, 34, 532–537, (2014).
[28] López, M., Peinado, A., & Ortiz, A. An extensive validation of a SIR epidemic model to study the propagation of jamming attacks against IoT wireless networks. Computer Networks, 165, 106945, (2019).
[29] Yi, H., & Nie, Z. Side-channel security analysis of UOV signature for cloud-based Internet of Things. Future Generation Computer Systems, 86, 704–708, (2018).
[30] Tweneboah-Koduah, S., Skouby, K. E., & Tadayoni, R. Cyber security threats to IoT applications and service domains. Wireless Personal Communications, 95, 169–185, (2017).
[31] Lehtonen, M., Ostojic, D., Ilic, A., & Michahelles, F. Securing RFID systems by detecting tag cloning. Pervasive Computing: 7th International Conference, Pervasive 2009, Nara, Japan, May 11-14, 2009. Proceedings 7, 291–308. Springer (2009).
[32] Manickam, P., Mariappan, S. A., Murugesan, S. M., Hansda, S., Kaushik, A., Shinde, R., & Thipperudraswamy, S. P. Artificial intelligence (AI) and internet of medical things (IoMT) assisted biomedical systems for intelligent Healthcare. *Biosensors*, *12*(8), 562, (2022).
[33] Syed, F. M., & Es, F. K. AI-Powered Security for Internet of Medical Things (IoMT) Devices. *Revista de Inteligencia Artificial En Medicina*, *15*(1), 556–582, (2024).
[34] Paavola, J., & Ekqvist, J. Privacy preserving and resilient cloudified IoT architecture to support eHealth systems. *Interoperability, Safety and Security in IoT: Third International Conference, InterIoT 2017, and Fourth International Conference, SaSeIot 2017, Valencia, Spain, November 6-7, 2017, Proceedings 3*, 134–143. Springer (2018).
[35] Ahmed, S. F., Alam, M. S. B., Afrin, S., Rafa, S. J., Rafa, N., & Gandomi, A. H. Insights into Internet of Medical Things (IoMT): Data fusion, security issues and potential solutions. *Information Fusion*, *102*, 102060, (2024).
[36] Lakhan, A., Mohammed, M. A., Nedoma, J., Martinek, R., Tiwari, P., Vidyarthi, A., … Wang, W. Federated-learning based privacy preservation and fraud-enabled blockchain IoMT system for healthcare. *IEEE Journal of Biomedical and Health Informatics*, *27*(2), 664–672, (2022).
[37] Ibitoye, O., Shafiq, O., & Matrawy, A. Analyzing adversarial attacks against deep learning for intrusion detection in IoT networks. *2019 IEEE Global Communications Conference (GLOBECOM)*, 1–6. IEEE, (2019).
[38] Mahmood, K., Akram, W., Shafiq, A., Altaf, I., Lodhi, M. A., & Islam, S. K. H. An enhanced and provably secure multi-factor authentication scheme for Internet-of-Multimedia-Things environments. *Computers & Electrical Engineering*, *88*, 106888, (2020).
[39] Al Ali, A., Al-Blooshi, O., Al Ali, R., & Al Hamadi, H. Securing the Internet of Things (IoT) Application: Best Practices and Challenges in IoT Software. *2024 Advances in Science and Engineering Technology International Conferences (ASET)*, 1–7. IEEE, (2024).
[40] Arigbabu, A. T., Olaniyi, O. O., Adigwe, C. S., Adebiyi, O. O., & Ajayi, S. A. Data governance in AI-enabled healthcare systems: A case of the project nightingale. *Asian Journal of Research in Computer Science*, *17*(5), 85–107, (2024).

[41] Gentry, C., & Halevi, S. Implementing gentry's fully-homomorphic encryption scheme. *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, 129–148. Springer, (2011).
[42] Yang, Q., Liu, Y., Chen, T., & Tong, Y. Federated machine learning: Concept and applications. *ACM Transactions on Intelligent Systems and Technology (TIST)*, *10*(2), 1–19.
[43] Kuo, T.-T., Kim, H.-E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association*, *24*(6), 1211–1220, (2019).
[44] Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. Medrec: Using blockchain for medical data access and permission management. *2016 2nd International Conference on Open and Big Data (OBD)*, 25–30. IEEE, (2016).