A Layered Security Perspective on Internet of Medical Things: Challenges, Risks, and Technological Solutions

Ziad Almulla, Hussain Almajed, M M Hafizur Rahman
Department of Computer Networks and Communications-College of Computer Sciences and Information Technology,
King Faisal University, Al-Ahsa, 31982 Saudi Arabia

***Abstract*—The Internet of Medical Things (IoMT) refers to smart devices that are used in their transformation of the healthcare sector with continuous monitoring in real time, remote diagnostics as well as real time data exchange. nevertheless such systems are being targeted by a number of challenges like data breaches, unauthorized users and service interruptions. The study uses the PRISMA 2020 method and analyzes 25 peer-reviewed articles that were published between 2020 and 2025. Security risks are identified and mapped on the IoMT architecture's perception, network, application and cloud layers. One of the key findings was confirming the fact that blockchain based identity management, algorithmic lightweight cryptographic protocol, and Artificial Intelligence(AI) driven intrusion detection systems can potentially address these risks. However, these areas are still limited in terms of interoperability, resource efficiency, and there are no solutions against the emerging quantum threats. A number of countermeasures achieved almost perfect detection accuracy over 98%, leading to increased security for IoMT systems. In order to solve the above issues, the framework, TrustMed-IoMT, is introduced to integrate blockchain-based identity management, intelligent intrusion detection and encryption that is safe against quantum attacks.**

***Keywords*—IoMT; security risks; challenges; healthcare IoT; countermeasures; TrustMed-IoMT**

I. Introduction

IoMT is fast becoming the next big thing in the healthcare industry due to which provision of smart, connected devices is allowing the real time patient monitoring, remote diagnostics, and the efficient clinical workflows [1]. According to a report conducted in 2017, there were already $28 billion in revenue from IoMT based systems, and the projection is that the revenue will grow to $135 billion in coming years, which favors in reducing the healthcare costs worldwide by $300 billion. While such advantages existing, security and privacy are serious problems that prevent IoMT from being widely adopted. The environment in which IoMT systems operate is highly heterogeneous consisting of many different devices, protocols, and operating system, which makes such systems particularly vulnerable to cyberattacks. Additionally, the value of medical data (50 times higher than the value of data in another sector) makes IoMT a lucrative target to adversaries. These factors point out the necessity of understanding the motivation for adoption of IoMT and to provide solutions for the associated cybersecurity risks to enable resilient and sustainable healthcare infrastructures.

A. Motivation

IoMT has become part of the healthcare industry reducing healthcare costs, providing real time patient monitoring, remote diagnostics, communication between different devices and overall experience [2], [3], [4]. The components that form IoMT are wearable health trackers, smart medical devices and cloud based healthcare systems that permits continuous collection and transmission of health data over the internet. All these advancements have made great impacts in healthcare and even improved the efficiency and accessibility of patients among other outcomes.

IoMT devices process and generate huge quantities of sensitive patient data and so require strong security measures to prevent cyber threats. However, the increasing dependence on IoMT poses some critical security challenges, hence the systems are likely to be targeted by a potential cyber attack [5].

B. Problem Statement

A cyberattack on a global healthcare network via ransomware exploited vulnerabilities in more than 6.2 percent of IoMT devices in 2024, and impacted 53 percent of the critical healthcare systems eventually resulting in loss of more than a million patient records, and costs exceeding $22 million [6]. The attack took advantage of security flaws on medical device that were unpatched, disrupting operations and in some cases causing data breaches. This incident illustrates the necessity of stronger security interventions for the safeguarding of IoMT systems from attackers.

In the context of healthcare, the Medical Internet of Things or IoMT has changed the direction in which healthcare is headed towards today. However, these advancements have provoked crucial security challenges that have transformed the IoMT into a susceptible environment for attacks such as Distributed Denial of Service (DDoS) attack, malware infiltration, data breaches and unauthorized access. In addition, the disparate nature of IoMT Networks adds to security risks given that there exist devices with different communication protocols and security capabilities communicating across several layers among themselves. Moreover, the growing use of cloud based healthcare systems has extended the threat surface, rendering the intervention of data tampering, credential theft, and the blow of healthcare systems [7].

Signature based Intrusion Detection Systems(IDS) and static cryptography, which represent the traditional approaches

to security, have failed to detect new attacks and to prevent the current evolving cyber attacks. Almost 50% of IoMT devices remain open for exploits, risking serious operational and financial operations for the healthcare systems. To overcome these problems, the use of the forced AI and Machine Learning (ML) based security frameworks have been investigated to address these concerns. Using these techniques, anomaly can be detected in real time, known threats can be identified proactively and the automated security response mechanisms [8]. AI driven security solutions have shown better detection accuracy, adaptability to the new attack patterns as well as system resilience, which make them a key part of the security of the IoMT infrastructure.

C. Research Objectives

This research intends to address the above issue by exploring current state of IoMT security and categorizing security challenges, countermeasures and research gaps. The study gives a structured analysis of threats and mitigation procedures based on AI driven security mechanisms, blockchain based authentication, cryptographic protocols and IDS.

This study is structured to answer the following key Research Questions (RQs):

- RQ1: What are the major security challenges in IoMT?
- RQ2: What proposed countermeasures are there to address the security risks mentioned?
- RQ3: What are these security mechanisms mapped to different IoMT communication layers?
- RQ4: Which research gaps exist on the IoMT security field, and in what directions it should be further researched?

Through answering these research questions, this study will explore the existing studies, trend, and be the foundation for further research in IoMT security. This study follows a systematic methodology for study selection, data extraction and analysis in order to ensure rigor and transparency as per PRISMA 2020 guidelines.

The paper outlines different IoMT threats and security measures in relation to how the system is structured (perception, network, application, cloud). In contrast to other reviews, the conceptual framework, TrustMed-IoMT, which integrates key security controls to guide the development of secure IoMT systems.

In Section II, an in depth overview of IoMT security is provided starting with an analysis of IoMT architecture, a security risk analysis followed by a classification of countermeasures. After that, Section III conducting the security challenges across IoMT layers. Section IV starts with a PRISMA 2020 compliant research methodology that describes the study selection process, inclusion criteria and synthesis methods applied in this study. Section V will represent the existing studies in the area of IoMT. After that, Section VI discusses the findings of the methodology. Section VII concludes the discussion by identifying the current research gaps and points out possible ways to improve IoMT security frameworks. In Section VIII, finally, the key insights are summarized and final thoughts on how IoMT security can progress and what challenges it will face are expressed.

II. Background

A. Overview of IoMT and its Security Importance

The IoMT is a sub specialization of the Internet of Things (IoT) which is used in the sector of healthcare utilizing wearable devices, smart medical sensors and even cloud based health system to monitor patients in real time, get remote diagnostics and other actions within healthcare services [9]. Fig. 1 shows that IoMT systems comprise of wearable health devices, smart monitoring systems, diagnostic centers and electronic medical records that work towards an effective and safe data collection, processing and healthcare management.

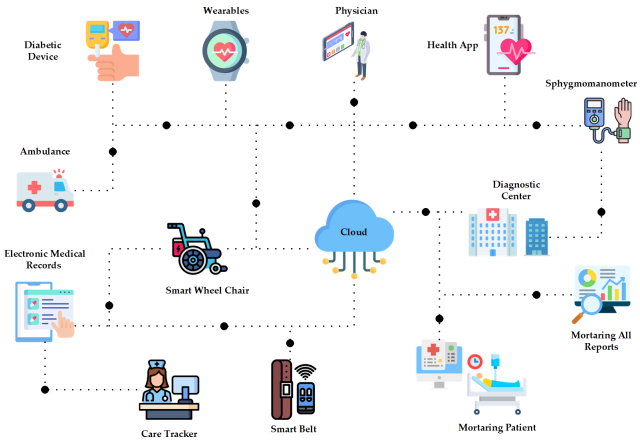

Fig. 1. Architecture of IoMT.

1) The Growth and adoption of IoMT: In recent years, there is a surge of adoption of IoMT a number of steps forward for AI, cloud computing and edge technology [10]. In 2017, the market was around $41 billion and it grew to become $158 billion in 2022 on account of demand for remote healthcare and AI diagnostic platforms. IoMT has also facilitated the Healthcare Industry 5.0's integration with patient monitoring and personalized treatment by smart devices and real time data processing. Although it has grown very fast, IoMT suffers from constraints related to security, interoperability and regulatory issues. Cyber threats to medical devices are also on the rise due to the increased connectivity, while inconsistency in the standards needed for seamless integration prevents it.

2) Importance of security in IoMT: The IoMT devices process, collect, and transmit a huge amount of sensitive patient data that is used for future treatment, specifying huge risks from cyber threats [8]. IoMT systems security breach can result in unauthorized access to Electronic Health Records (EHRs), medical devices manipulation, and even dangerous interruption of healthcare services. According to studies, almost half of the IoMT devices are exposed to certain exploits that could lead to ransomware attacks, malware and unauthorized intrusions to hospitals and patients.

In order, to ensure IoMT security, strong authentication techniques, encrypted data transmission, and always watching the network to prevent unauthorised access is required[10].

TABLE I. LIST OF CHALLENGES AND POTENTIAL THREATS ON EACH LAYER OF IOMT

IoMT Layer	Security Challenges	Potential Threats
Perception Layer	Device vulnerabilities due to limited resources (low power, weak encryption).	Sensor tampering, unauthorized access, data spoofing.
Network Layer	Communication security risks, Man-In-The-Middle (MITM) attacks, and data interception.	Eavesdropping, jamming attacks, DDoS.
Application Layer	Software vulnerabilities in healthcare platforms, unauthorized Application Programming Interface(API) access.	Malware, phishing, ransomware attacks.
Cloud and Edge Layer	Privacy risks due to cloud-based storage, risk of data breaches and leaks.	Insider threats, cloud hacking, unauthorized access.

However, IoMT network security is made even more challenging by the interoperability challenges and the absence of security protocols that are standardized. The adoption of diverse medical devices without a unified security framework means routine data leaks, device hijacking, and in turn regulatory non-compliance risk is increased much higher.

B. IoMT Architecture and Security Layers

IoMT architecture has different layers of interconnected architectural components that allow for data collection, transmission, and processing, which brings distinct security risks. Knowing these layers is very important when designing security strategies as these layers are interconnected and one can be subjected to any other [11]. There are the perception layer which call device layer where used for collecting physiological and environmental data. In addition, network layer where It enables the data transmission over IoMT devices and the cloud with the help of wireless communication technologies like Wi-Fi, Bluetooth, Zigbee. Moreover, application layer where It consists of the user interfaces and the healthcare services. Finally, cloud and Edge Computing infrastructure where where the storage and data analytics are facilitated at the cloud level, and real time processing is facilitated using the edge level.

III. SECURITY CHALLENGES ACROSS IOMT LAYERS

The IoMT ecosystem faces several security vulnerabilities across different layers, posing risks to data integrity, privacy, and device reliability [11], [9]. Table I will list the challenges that may affect each layer along with potential threats.

A. Major Security Challenges in IoMT

The IoMT is improving health care efficiency, but it also brings great security risks that can be analyzed using the CIA (Confidentiality, Integrity, and Availability) triad. The following section analyzes the security challenges of IoMT based on these three fundamental security principles.

1) Confidentiality risks (Data privacy and unauthorized access): The confidentiality helps to maintain the patient data confidential and can be accessed only by authorized persons. However, most of the IoMT devices do not protect sensitive information, which exposes them to attacks [9], [11], [12], [10]. First, the unauthorized access and data breaches which it the attacks on weak authentication mechanisms, it enable attackers to access patient data and patient's medical identity data for medical identity theft and financial fraud [12]. Also, lack of encryption in data transmission on IoMT devices. They are transmitting unencrypted packets which would enable attackers to intercept and manipulate the packets in other word (MITM Attacks) [9]. Additionally, the Insider Threats consider as a challange in IoMT where patient records are exposed either intentionally or unintentionally by employees or compromised accounts [10]. Lastly, the regulatory and non-compliance where many devices fail to meet Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR) and other data protection laws; therefore, IoMT systems must comply with such laws [11].

In order to mitigate, you could implement certain controls such as Endto End encryption using Advanced Encryption Standard (AES)-256 for sending out data securely [10]. Moreover, Multi-Factor Authentication (MFA) that may strengthen access control mechanisms. Also, Role Based Access Control (RBAC) that allowing only access of data on the basis of user role, and blockchain for secure medical records that will ensure tamper-proof and auditable patient data storage.

2) Integrity risks (Data manipulation and device security): Medical data accuracy and untouched status depend on the concept of integrity. Medical data inaccuracies which arise from unauthorized changes result in diagnostic errors along with improper treatments and device malfunction. First risk faced is malware and ransomware Attacks. These kinds of attacks involving malware and ransomware grant attackers the ability to modify medical data that exists on or passes through IoMT devices [10]. Also, data tampering via network attacks where the attackers can modify medical reports through unsecured network transmissions which results in incorrect medical diagnosis [9].Moreover, The outdated firmware and patch management which is the use of legacy software by many IoMT devices exposes them to attack because it contains well-documented security weaknesses that hackers can exploit[11]. Lastly, lack of audit trails which is the lack of proper logging systems prevents healthcare staff from noticing when unauthorized data changes occur in patient records [12].

In order to mitigate, digital signatures and hashing (Secure Hash Algorithm(SHA)-256) that will ensure authenticity and resolve if any data tampering, and digital signatures and hashing (SHA-256) [10]. Also, AI-powered anomaly detection that could identify and flag suspicious modifications. As well as firmware Updates and patch management need to be regularly update device software to fix vulnerabilities. Lastly, immutable logs and blockchain integration could maintain a secure, unchangeable history of medical data.

3) System downtime and network attacks: The availability dictates that IoMT services and data remain accessible whenever they are needed. Availability cyber threats may disrupt patient monitoring, delay treatments and cause the loss of life. Such of availability risk Denial-of-Service (DoS) Attacks which is the exploitation of excessive network traffic by attackers disrupts the ability to monitor patients in real-time [9]. Also, device failures due to malware where hospital patient care becomes endangered when malware infects IoMT devices which results in device failure or produces incorrect results [10]. Moreover, cloud and Edge Computing security risks where the healthcare cloud platforms experience three main

security threats which include data center failures plus insider dangers and cyberattacks [12]. Lastly, lack of redundancy and backup Plans where A lack of fail-over protocols in IoMT systems creates complete system downtime during cyber incidents [11].

In order to mitigate you could applied network segmentation where the IoMT devices need to be physically cut off from public networks as a prevention strategy against large-scale attacks [10]. Also, Intrusion Detection and Prevention Systems (IDPS) which is can monitor anomalous activities and block malicious traffic. In addition, cloud-based disaster recovery that can Implement backup systems to recovery systems for attack response. Lastly Edge Computing for localized processing in order to keep devices functioning the company should reduce their dependence on cloud networks.

IV. Research Methodology

The study adopts PRISMA 2020 guidelines to organize a transparent research process which can be reproduced. The research method includes four essential steps which are eligibility criteria, information sources, search strategy, and selection process and data collection and synthesis methods.

A. Inclusion and Exclusion Criteria

The inclusion and exclusion criteria were selected for the studies to ensure that only relevant and high quality research was included.

1) Inclusion criteria: Paper selection was based on the following inclusion criteria: the paper must address security concerns in the IoMT, cover security challenges and risks, discuss mitigation strategies, be peer-reviewed, and have been published between 2020 and 2025.

2) Exclusion criteria: Papers were excluded if they were not focused on Medical IoT, did not address security risks or solutions, were not peer-reviewed, or were published before 2020.

B. Information Sources

A systematic search was conducted on several databases of academic publication as well as digital libraries whose purpose was to ensure that the studies selected are complete and unbiased. The relevant publications on Medical IoT (IoMT) Security Risks: Challenges and Countermeasures were retrieved from IEEE Xplore, ScienceDirect (Elsevier), MDPI, Google Scholar, and the Saudi Digital Library.

C. Search Strategy

The studies relating to security risks, challenges and countermeasures in IoMT were identified using a structured search strategy. The search for relevant literature was performed systematically over information sources. In order to achieve that the most relevant papers were retrieved using structured search query using Boolean operators (AND, OR, NOT). The primary search string was: "Medical IoT" OR "IoMT" AND "security risks" OR vulnerabilities OR threats AND (challenges OR countermeasures).

To ensure a comprehensive search, variations of keywords were used such as: IoMT security, medical IoT security, healthcare IoT threats; IoMT risk assessment, IoMT attack detection, IoMT authentication solutions; IoMT encryption, IoMT privacy challenges, and AI for IoMT security.

The main search string was slightly modified to match the search engine syntax and the database indexing system and each database was queried.

1) Search filters applied: The search was filtered using the following conditions: publication date between 2020 and 2025; publication type limited to peer-reviewed journal and conference papers; and the subject area focused on cybersecurity, IoT security, and AI-driven security.

D. Selection Process

The flow diagram in Fig. 2 indicates how the study selection was carried out following the PRISMA 2020 guidelines. This comprised of three main phases including identification, screening and inclusion.

The selection process involved the following steps: Identification – studies were retrieved from IEEE, MDPI, Saudi Digital Library, and Google Scholar. Screening – an initial filtering was conducted based on title and abstract relevance. Eligibility Assessment – a full-text review was carried out based on the inclusion and exclusion criteria.

The flow of number of studies at each stage was tracked using a PRISMA 2020 Flow Diagram.

1) Identification phase: A total of 365 records were found in major academic databases including IEEE Xplore, Saudi Digital Library, MDPI and Google Scholar. Duplicate (100 studies) and ineligible records (20 studies) were removed. Additionally, 30 records were excluded for other reasons, and 215 records were retained for further screening.

2) Screening phase: The remaining 215 records were subjected to title and abstract screening in order to assess their relevancy to the objectives of the review. Out of this stage, 135 records were discarded as irrelevant to the inclusion criteria. This process yielded 80 records for retrieval and full text review.

3) Eligibility and inclusion phase: Of the 80 records retrieved, 5 were not retrieved due to the unavailability of the studies. A full-text review of the remaining 75 records was performed, and 50 records were excluded. A total of 25 studies were included in the final review after inclusion criteria were met. These studies form a complete and high quality subset which covers the main targets of highlighting the Medical IoT Security challenges and remedies.

The purpose for studying IoMT security from 2020-2025 was to consider the most recent advances in telehealth, blockchain and AI use following the pandemic. Only 25 studies were selected that followed strict criteria and focused on matters of threats, how to address them and how to design systems.

The distribution for the selected papers per year included in this research is shown in the Fig. 3. Of the 25 studies chosen, the most studies were published in 2024 (12 studies)

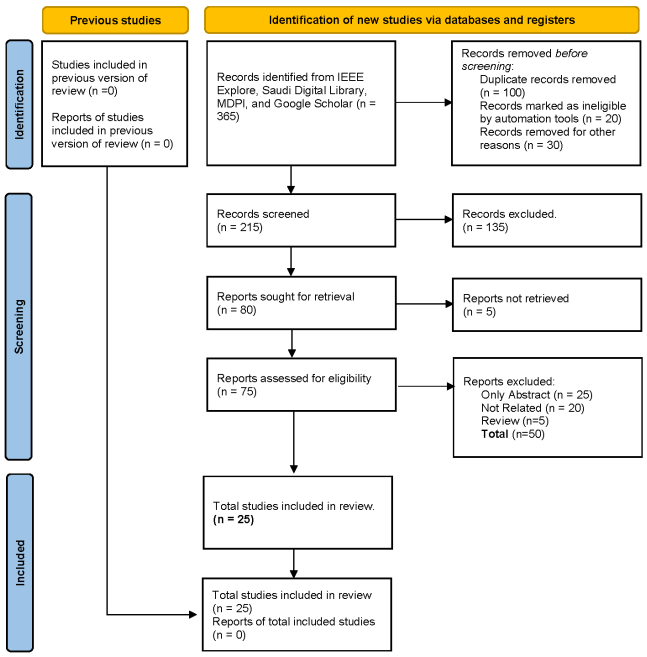

Fig. 2. Selection of papers for research.

with their interest in this area growing. While only 6 studies, the year 2023 continues to pay attention to the IoT security challenges. There are only 3 studies in 2022, 1 in 2021, and 2 in 2020, which significantly decreases the research activity in prior years. However, One study, which contributes to the early year of 2025, is notably included in 2025. As shown by this trend, IoMT security has gained higher importance and significance in recent years and, especially in 2024, it can be considered a newly emerging research domain.

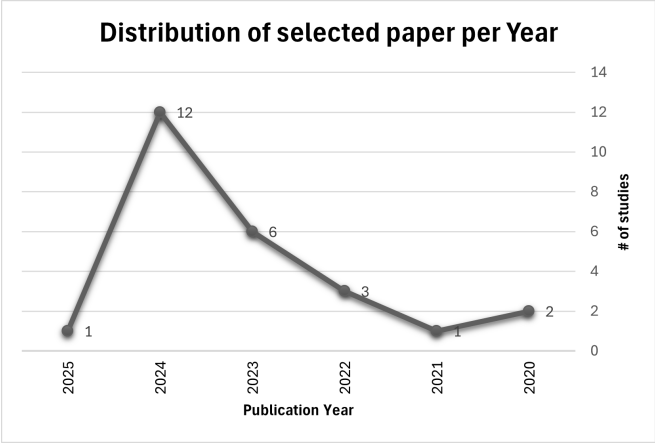

Fig. 3. Distribution of selected paper per year.

V. Existing Studies on IoMT

A. Challenges of IoMT

Yaacoub et al. [13] assess security challenges in the IoMT, particularly from the standpoint of authentication vulnerabilities, privacy risks, malware threats, and network vulnerabilities. They include unauthorized access, ransomware, botnet infection, eavesdropping, DDoS attacks, and pose a major threat to the perception, network, application, and cloud layers. For example, malware injection is a threat to the perception layer, as are eavesdropping and data interception to the network layer. Besides this, the risk of ransomware and privilege escalation is at the application layer whereas the cloud layer is at a risk of data breaches and weak encryption. Additionally, these threats are serious and real world attacks, such as the Mirai botnet, prove so. As a result, problems arising from these issues affect patient safety, data integrity and regulatory compliance. Though such countermeasures and protocols exist for use, there are still limitations including insufficient standard security protocols and weak cryptographic implementations. Hence, the paper asks for lightweight cryptographic mechanisms, AI driven intrusion detection and increased privacy preserving techniques.

According to Bajpayi et al. [14], the security risks of IoMT include authentication flaws, malware attacks, privacy issues, and network vulnerabilities. As a result, these vulnerabilities render critical medical systems susceptible to several attack vectors such as unauthorized access, ransomware, DDoS, eavesdropping, and data breach that consequently affect the perception, network, application, and cloud layers. For example, malware injection is a huge threat for perception layer devices and weak encryption for cloud layer makes it highly vulnerable to data breach. In addition, real world cyber attack cases, like botnet from Mirai also confirm the severity of these risks as impacting patient safety, data integrity, and compliance to regulations in the industry. Similarly, the paper also mentions several drawbacks, which include outdated security patches, weak encryption and insecure device configurations. However, it emphasizes the required security automation improvement, such as employing AI based intrusion detection, lightweight cryptographic models and privacy preserving models to improve the IoMT resilience.

Waqdan et al. [15] evaluate the security risks of IoMT and highlights the problems that are faced with the unauthorized data access, system vulnerabilities, and network security threats. Risk assessment is studied in healthcare settings like emergency rooms with concern in network and application layers. The primary attack vectors that covers are DDoS, data breaches and protocol based exploits. Discussion is also included on real world cyberattacks, such as unauthorized access of patient data. Such security issues impact patient safety, data integrity, system performance, and are also regulatory compliance issues. The concerns that remain unresolved for the IoT devices are accompanied by heterogeneity in devices, limited security updates, as well as high risks of interconnectivity. Therefore, future research on adaptive security frameworks and secure encryption mechanisms to increase IoMT resilience is also suggested by the paper.

Czekster et al. [16] explain the security challenges in IoMT and identify Dynamic Risk Assessment (DRA) risks. The question examined in this study is the cybersecurity concerns in healthcare environment, such as unauthorized intrusions, data breaches, and device malfunction. Security threats significantly affect the perception, network and application layers, with the key attack vectors being unauthorized access, malware

and DoS attacks. Discussions of real world cyber attacks like a ransomware attack on a hospital are also provided. Such threats adversely affect patient safety, data integrity, system reliability and raise regulatory compliance issues. The paper addresses the unresolved security concerns, such as real time risk assessment and improvement of IoT security frameworks. Finally, future research is suggested in developing adaptive security models which can provide security on evolving IoMT threats.

Jayaraj et al. [17] discuss security risks in the IoMT, with an emphasis on wireless spoofing attacks. The study identifies the major threats of spectrum security vulnerabilities, unauthorized access and data breach. In the research, perception and network layers are found to be most affected by the attack and the primary attack vectors being sniffing, spoofing, and protocol based attacks. Cyberattacks on IoMT in the real world are described in relation to patient safety, data integrity, and regulatory compliance risks. Although cryptography and Deep Learning(DL) has improved, security problems are not solved yet. The paper identifies some gaps in recognizing legitimate from rogue transmissions and hence advocates for future work in hybrid security frameworks to enhance IoMT resilience.

The work of Sankepally et al. [18] emphasise critical security challenges in the IoMT and in particular, compromising of the data integrity in the form of false data injection attacks that lead to incorrect diagnosis and jeopardise patient safety. Specifically, the study focuses on vulnerabilities in data transmission and storage, and the network and the application layers are the most affected. Since false data injection attack is the primary attack vector, it can reveal side effects such as increasing system performance along with regulatory infractions. According to this study, the real world cyber threats are referenced and 35% of IoMT using firms suffered breaches in 2016. In proposing a ML based mitigation technique, there are limitations such as data loss, low detection accuracy and propose that there is a need for further research in Explainable AI for more trust and security.

Madanian et al. [19] discuss the critical security challenges in the IoMT where they highlight vulnerabilities across the layers of perception, network, and application. In particular, insecure device authentication, weak cryptography algorithms, and phishing of healthcare institutions are pointed out. Additionally, DDoS, ransomware and data breach comprise the main attack vectors, that affect patient safety, operational capacity and compliance issues. Furthermore, the real world cyberattacks on hospitals emphasize the need for protection of IoMT. Although the paper identifies existent security gaps, in conclusion, the paper also recommends further research on AI based anomaly detection and blockchain technology as a purposed form of increasing data security.

Study by Sasaki [20] deals with security challenges in IoMT paying special attention to security risks related to Remote Maintenance (RM). It points out the threats of unauthorized intrusions that could interfere with operations of IoT devices, compromise patient safety, and misuse of private hospital data by maintenance personnel. The study problem focuses on balancing Maintainability, Safety, Security, and Privacy (MSSP) in IoMT systems. Network and application are the most impacted layers, as these are the layers which get affected with unauthorized access, impersonation attacks and data leakage. Cyberattack on RM channels is discussed as a real world risk. Most of these security challenges relate to patient safety, data integrity and regulatory compliance. It indicates the remaining issues in optimizing security mechanisms without affecting usability and hence recommends further research in security enhanced RM solutions for IoMT.

Table II shows the summary of security challenges addressed in each IoMT layer and possible attacks.

1) Taxonomy of security challenges of IoMT: Fig. 4 provides a layer wise taxonomy of security challenges involved in the IoMT. The challenges are grouped based on perception, network and application layers and are synthesized based on the reviewed studies in Table II.

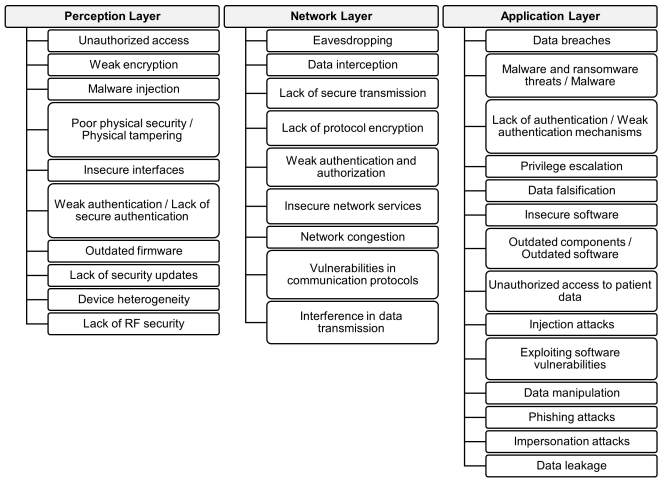

Fig. 4. Layer-based taxonomy of security challenges in IoMT.

B. Countermeasures of IoMT

Xie et al. [21] propose to combat sensor node capture attacks, impersonation threats, moreover non authorized information access, they introduces a lightweight and privacy preserved authentication protocol for Medical IoT. That dual purpose is what the study aims to achieve when it comes to ensuring user anonymity and data security when it comes to using IoT-based healthcare systems. The proposed solution combines the inclusion of Physical Unclonable Function (PUF) and Elliptic Curve Cryptography (ECC) to increase the security notion of the three-factor authentication, and achieves perfect forward secrecy. Securing the user authentication and preventing unauthorized device access is what these countermeasures protect, in the layers of the perception and network. On the other hand, it is low computational cost, improved privacy, and resistant to major cyber threats. There still exist limitations to potential biometric vulnerabilities. Resilience to new IoMT cyber threats and advancement of biometric security are shown in the future research.

Sabrina et al. [22] propose the post quantum privacy preservation technique based on blockchain for solving this issue. This work is motivated by the fact that although healthcare has been an active target of resource constrained data privacy and integrity, the proposed work improves on that by providing privacy and integrity. Based cryptography, Quantum Key Distribution (QKD) and hybrid cryptographic models are

TABLE II. SUMMARY OF CHALLENGES IN IOMT

Author	Security Challenges	IoMT Layer Affected	Attack
Yaacoub et al.[13], 2020	Unauthorized access, weak encryption, malware injection	Perception Layer	Device hijacking, unauthorized access, malware (botnets, ransomware)
	Eavesdropping, data interception, lack of secure transmission	Network Layer	Traffic interception, DDoS, unauthorized access.
	Data breaches, ransomware, lack of authentication	Application Layer	Malware, phishing, privilege escalation, data falsification
Bajpayi et al.[14], 2024	Poor physical security, insecure interfaces, lack of proper encryption, weak authentication, outdated firmware.	Perception Layer	Tampering, jamming, eavesdropping, DoS.
	Lack of protocol encryption, weak authentication and authorization, insecure network services.	Network Layer	MITM, spoofing, wormhole, Sybil attacks, flooding.
	Insecure software, lack of proper encryption, weak authentication, outdated components	Application Layer	Phishing attacks, viruses, worms, Trojans, spyware, DoS.
Waqdan et al.[15], 2023	Lack of security updates, device heterogeneity, physical tampering risks	Perception Layer	Unauthorized access and device manipulation.
	Network congestion, vulnerabilities in communication protocols, and interference in data transmission	Network Layer	DDoS attacks, MITM attacks, and packet sniffing
	Unauthorized access to patient data, weak authentication mechanisms, malware and ransomware threats.	Application Layer	Data breaches, injection attacks, exploiting software vulnerabilities
Czekster et al.[16], 2023	Unauthorized access, lack of secure authentication	Perception Layer	Physical tampering, unauthorized access
	Insecure communication, data interception	Network Layer	MITM attacks, DoS
	Data breaches, malware infections, ransomware	Application Layer	Malware, ransomware, data integrity breaches
Jayaraj et al.[17], 2024	Unauthorized access, lack of RF security	Perception Layer	Physical attacks, Sniffing
	Spectrum security vulnerabilities, unauthorized transmissions	Network Layer	Spoofing
	Data integrity risks, unauthorized control	Application Layer	Exploiting software vulnerabilities
Sankepally et al.[18], 2022	Data manipulation	Perception Layer	False Data Injection
	Data transmission vulnerabilities	Network Layer	MITM Attacks, False Data Injection
	Compromised patient data, incorrect diagnosis	Application Layer	False Data Injection
Madanian et al.[19], 2024	Insecure device authentication, physical tampering, data breaches	Perception Layer	MITM, Replay Attacks, Physical Tampering.
	Weak cryptographic algorithms, lack of encryption, eavesdropping, DDoS	Network Layer	DDoS, IP Spoofing, Eavesdropping, Packet Injection.
	Phishing attacks, malware, ransomware, outdated software, weak authentication	Application Layer	Ransomware, Phishing, Malware, Structured query language(SQL) Injection
Sasaki [20], 2020	IoT device disruption, patient safety risk	Perception Layer	Unauthorized access, device tampering
	Data leakage, remote intrusion	Network Layer	Man-in-the-middle, unencrypted communication
	Unauthorized hospital data access, impersonation	Application layer	Social engineering, weak authentication

some of the proposed countermeasures. By providing secured perception, network and application layers, the secure medical data transaction from quantum threats. The advantages are decentralization, on the fact that is immutable and the chain is to be resistant to future post quantum cryptographic vulnerabilities. There is, however, still computational overhead and complexity of integration. This paper inspires further research on how to encourage development of the optimal quantum resistant blockchain framework and to develop the energy efficient cryptographic algorithms for IoMT applications.

Mavhemwa et al. [23] propose an adaptive user authentication model for elderly IoMT users in an effort to address the authentication usability and security challenges. The aim of the study is to improve authentication accuracy by not degrading usability for the elderly. A naive bayes risk aware authentication model is proposed that uses health condition and risk scores to assign authenticators. In this approach, the trust score of the user can be used to alter the difficulty at which authentication should take place such that the perception, network and application layers are protected. The resulting benefits are also the reduction of authentication fatigue or the improvement of usability and, finally, dynamic security. These do come at the cost of overfitting and reduced usability. Future research recommends fortifying biometric security, extending the dataset for the purpose of validation and indicating the optimal authentication procedure for a wide range of IoMT applications.

To address the above stated security risks like unauthorized access to personal information of the patient, data breach and privacy issues in smart health care systems, Kumar et al. [24] propose A Novel Architectural Framework (ANAF)-IoMT. It aims at providing advanced authentication, enhanced data privacy and secure storage for IoMT environments. Include Rooted Elliptic Curve Cryptography with Vigenère Cipher (RECC-VC), Exponential K-Anonymity (EKA) for preserving privacy and blockchain as secure data storage. These protect against this at perception, network and applications layers by securing data transmission, user authentication and cloud storage. The advantages are that of higher security 98%, better privacy and resistance against the cyber threats. A challenge still remains however, of computational overhead. In future research, it will be more worthwhile to optimize the encryption efficiency and incorporate quantum resistant security measures.methods.

Laabab et al. [25] Propose to combat identity theft, data breaches and invalid access, offers an integration of biometric systems and blockchain in IoMT. The aim of the study is to improve the tasks of authentication, access control and data integrity in the environment of healthcare. Biometric based authentication with blockchain smart contracts are the proposed counter measures for the secure and decentralized identity verification. These solutions protect all the perception, network, and application layers via encrypted tamper proof identity verification and logging transactions. This also provides for enhanced security, transparency and privacy. With Challenges in computational complexity and integration issues. Optimizing biometric encryption methods and working for blockchain scalability to utilize in real time IoMT applications is suggested to be conducted in future research.

Alsadhan et al. [26] Propose to overcome unauthorized

access, data breaches as well as the lack of patients control in the IoMT. The intention of the study is to protect the patient's data from being lost by using decentralized identity management and access control. It suggests permissioned and permissionless blockchain models, cryptographic methods, and smart contracts as the proposed countermeasures. These solutions secure the storage layer, encrypted transactions, and fine grained access control for the perception, network and application layer. Its advantages include greater transparency, immutability as well as reduced (or even no) single points of failure. However, the energy consumption and integration complexity as well as scalability are challenges. Research for the future can concentrate on enhancing scalability of blockchain, enhancing the efficiency of encryption, and implementing a private preserving consensus.

Mahmood et al. [27] discuss critical security challenges in the IoMT like unauthorized access of data, malware attack and privacy breach. The study is centered around security issues in IoMT stakeholders, architecture and solutions. In order to meet these threats, the authors suggest a security framework consisting of the access control, encryption, threat detection, and incident response protocols. The countermeasures protect all layers of IoMT (perception—device security, network—secure transmission, and application—data privacy). However, the proposed solutions improve patient data confidentiality and the redundancy of the system but have the limitation of implementation complexity and resource constraints. Therefore, future research is suggested to enhance IoMT security without performance trade-off via lightweight security mechanisms and AI-driven threat detection.

Sandulescu et al. [28] explore the security issues such as data privacy, unauthorized access and device interoperability in IoMT. Specifically, it integrates IoMT with AI driven healthcare solutions, and specifically discusses the security concerns in this data transmission and storage. Encryption protocols, secure data transmission and access controls in the ICIPRO cloud infrastructure are proposed countermeasures. These solutions ensure confidentiality and integrity of the perception, network, and application layers of IoMT. It guarantees better patient data compliance and security. However, high implementation costs and data privacy concern still exist. Future research might include improving protocols of interoperability between IoMT devices to further enhance security frameworks, as well as improvement of AI driven anomaly detection.

Subramaniam et al. [29] propose an interoperable privacy enhanced framework to address the security risks in IoMT. This study will work on overcoming problems of data privacy, authentication vulnerabilities, and secure data transmission. In order to achieve this, the proposed security solutions are device authentication with Secure Credentials (SCs), data encryption with Twine-LiteNet, and data integrity verification with Ten Fold Cross Entropy Verification (TCEV). These countermeasures protect the IoMT from the perception, network, and application layers. The method increases throughput, lowers the latency and extends the network's longevity. However, computational overhead and suitability to various IoMT environments are the limitations.

Su and Xu [30] discuss critical security issues in the IoMT that cover vulnerabilities of user authentication, privilege escalation attacks and resource limitations in IoMT devices. The study proposes a Three-factor Cluster-based user Authentication Protocol(3ECAP), a Secure and lightweight cluster based User authentication protocol, which supports fine grained access control using Merkle trees, multi factor authentication as well as efficient session key establishment. These countermeasures protect against IoMT attacks that work through any of the layers of perception, IoMT and application by securing communication, blocking unauthorized access and avoiding privilege escalation. It has advantages such as low computational cost and high resistance to cyber threats of common type. However, there are limitations as it increases overhead associated with access control. Further research lies in scaling up the environment scalability and integrating the AI based anomaly detection for real time security in IoMT scenarios.

Alsolami et al. [31] discusse some of the critical security challenges in the IoMT such as data breaches, malware, device hijack and insider threats. The research is aimed at intrusion detection using ensemble learning, such as Stacking, Bagging and Boosting to improve cybersecurity in medical networks. Moreover, the main goal of these countermeasures is to protect the network and application layers of the cyberspace against cyberattacks in real time. The proposed models achieve 98.88% accuracy and are more accurate, scalable and adaptable than the current models. However, they come with limitations; one of them being the risk of overfitting and the other being the computational complexity. Future research would include making improvements to the Boosting techniques and increase the diversity in dataset as Boosting techniques are subject to applicability in real world. The contribution of this study is towards securing healthcare environments by progressing intelligent detection systems against evolving IoMT threatening.

Krishna M et al. [32] address the significant challenge of DoS attacks in the IoMT. The aim of the research is to improve the security of IoMT through an IDS using ML algorithms including Support Vector Machine (SVM), Random Forest(RF), Linear Discriminant Analysis (LDA), and K-Nearest Neighbors (K-NN). These countermeasures analyze network traffic and detect countermeasures by attacking patterns to mitigate DoS threats. The IDS protects the network layer primarily, and it guarantees the safe data transmission. The advantage of the proposed approach is the high detection accuracy and adaptability, while the disadvantage is the lack of dataset and real-time implementation. Future improvement includes optimizing IDS to be deployed in a realworld environment as well as contribute to increasing the diversity of the dataset to generate more resilient IoMT security.

Balhareth and Ilyas [33] propose an IDS to reduce security threats in the Internet of Medical IoMT. The study is on detection of cyber threats in IoMT networks using ML based IDS. It is proposed that the use of tree based classifiers (Decision Tree (DT), RF, eXtreme Gradient Boosting (XGBoost), and CatBoost) with a filter based feature selection method (Mutual Information (MI) and XGBoost) increases the detection accuracy. The main objective of these countermeasures is to protect the network and application layers from real time threat detection. The benefits include a 98.79% accuracy rate and a 0.007 false alarm rate. However, it focuses on binary classification. Future work is to implement multi class classification to detect the attack type and to evaluate the

performance of such detection capabilities in real world IoMT domain.

Alalwany et al. [34] propose a real time IDS for critical security risks in the IoMT by means of Stacking ensemble DL approach. The goal of the study is to protect IoMT from cyber threats including ARP spoofing, DoS, Smurf and Port Scan attacks. This security solution uses an ensemble stacking method of integrating ML and DL models to increase the accuracy and the time detection speed. The IDS is implemented using Kappa Architecture to minimize latency and speed up threat response. Continuously monitoring data streams to detect anomalies in all IoMT layers (perception, network and application) provide the countermeasures that safeguard all the layers. However, it has advantages such as high accuracy, adaptability and low false positive rates. However, there is an overhead associated with computation and also dependency on the dataset. Future research on the model includes making it more efficient, and scaling up the amounts of data it collects for better generalization.

Bodapati and Raj [35] present security challenges in IoMT regarding data confidentiality and authentication against cyber–physical attacks. The study focuses mainly on lightweight encryption solutions for resource constrained medical devices. An FPGA based implementation of the ASCON-128 encryption algorithm is proposed to be used as a secure data transmission countermeasure. This solution improves security by being Authenticated Encryption with Associated Data (AEAD) which limits interception and tampering of data. The main aim of IoMT is to secure the perception and network layers. It also requires 35% less LUTs and increases the encryption throughput by 45%. However, there is still some room for optimization of the approach for real time medical applications. Further future research indicates that increasing rounds per cycle can improve encryption efficiency further.

Arpaia et al. [36] study security vulnerabilities of IoT medical transducers, and proposes methods to mitigate side-channel attacks such as Differential Power Analysis (DPA) and Correlation Power Analysis (CPA). Also, cryptographic countermeasures are evaluated, such as random delay insertion, random SBox, and masking to enhance AES encryption. The protection of the perception and network layers of IoMT is achieved by disrupting power consumption patterns and increasing the difficulty of the attack. The most effective one was masking, increasing security by a factor of 318. However, there are still limitations with regard to computational overhead. The future research concludes on optimizing the attack detection mechanism as well as power countermeasures for resource constrained devices. It is also recommended to strengthen the security regulations for the IoMT devices in order to provide robust protection against the existing and emerging cyber threats.

Patni and Lee [37] present EdgeGuard, which is a decentralized security framework for IoMT, dealing with data privacy, malicious attacks and service inefficiency. The primary contribution of this study is to leverage blockchain secured federated learning for secure medical resource orchestration. To ensure security, it comes with a lightweight blockchain consensus mechanism, adaptive federated learning with differential privacy, and access control based on smart contract. The countermeasures ensure data integrity, confidentiality and resource efficiency for IoMT's perception, network and application layers. However, although the approach improves in security, scalability, and real time responsiveness, it suffers for computational overhead as well as for energy consumption. Improvements in the future are to optimize blockchain efficiency and quantum train cryptographic methods that are better protected in healthcare IoT environments.

Table III shows the summary of security Countermeasures proposed to address the security challenge in IoMT layers.

Table IV shows the performance comparison of security countermeasures proposed to address the security challenge in IoMT layers along with strengths and weaknesses of the countermeasures.

VI. Existing Findings of the Studies

In this study, we analyze existing 25 studies in the IoMT and clarify the nature of the problems of security risks in IoMT and discuss the recommended countermeasures for those risks at various architectural layers in IoMT applications. It accomplished this by analysing the posed RQs methodically.

A. RQ1: Major Security Challenges in IoMT

The eight of studies revealed several critical IoMT device security threats that are significant including data breach, unauthorized access, malware infection, system downtime from DDoS like cyberattacks, and more. Different vulnerabilities were involved with each architectural layer of IoMT [13], [14], [15]:

1) Perception layer: Because IoMT devices have limited device resources, vulnerabilities of IoMT devices come from the IoMT devices such as they are vulnerable to physical tampering, unauthorized access, and spoofing attacks.

2) Network layer: MITM attacks and the eaves dropping attacks were almost based on the weak and insecure communication protocols and encryption standards that were used.

3) Application layer: Malware existent on software vulnerabilities and lax authorization mechanism were risky and had resulted to malware infections, ransomware attacks, unauthorized API access.

4) Cloud and Edge computing layer: The majority of risks were in the privacy breach, data leak, and cloud infrastructure vulnerability categories, involving health-sensitive data.

B. RQ2: Proposed Countermeasures to Address IoMT Security Risks

To mitigate identified risks, 17 of existing studies suggest several proactive and reactive countermeasures [27], [21], [22]:

1) Cryptographic solutions: Some of the recommendations were regarding the use of lightweight cryptographic models (ECC and AES-256), blockchain based encryption and quantum resistant methods to ensure secure storage and transmission of data.

2) Authentication and access control: Improve authentication mechanisms, such as biometric integration, blockchain-based identity management, and MFA, were suggested to mitigate unauthorized access

TABLE III. SUMMARY OF SECURITY COUNTERMEASURES IN IOMT

Author	Year	Security Challenge Addressed	Proposed Countermeasure	Technology Used	Layer Targeted
Xie et al. [21]	2023	Sensor node capture, impersonation, unauthorized access	Lightweight authentication with ECC and PUF	ECC, PUF	Perception, Network
Sabrina et al. [22]	2024	Quantum attacks on cryptographic security in IoMT	Post-quantum privacy preservation using blockchain	Lattice-based cryptography, QKD, hybrid cryptographic models	Perception, Network, Application.
Mavhemwa et al. [23]	2024	Authentication usability and security for elderly IoMT users	Adaptive authentication using risk-based Naive Bayes model	ML, Android-based authentication, MFA	Perception, Network, Application.
Kumar et al. [24]	2022	Unauthorized access, data breaches, privacy concerns in IoMT	ANAF-IoMT framework using RECC-VC, EKA, and blockchain	RECC-VC, EKA, Blockchain	Perception, Network, Application.
Laabab et al. [25]	2024	Identity theft, unauthorized access, data breaches in IoMT	Blockchain-integrated biometric authentication	Smart contracts, fingerprint recognition, decentralized identity management	Perception, Network, Application.
Alsadhan et al. [26],	2024	Unauthorized access, data breaches, lack of patient control	Blockchain-based privacy preservation with smart contracts	Permissioned and permissionless blockchain, cryptographic techniques	Perception, Network, Application.
Mahmood et al.[27]	2023	Unauthorized access, malware attacks, privacy breaches	Access control, encryption, threat detection, incident response	Cryptography, AI-driven threat detection, lightweight security models	All layers.
Sandulescu et al.[28]	2024	Data privacy, secure transmission, and unauthorized access	Encryption, access control, and secure cloud storage	ICIPRO cloud security, secure data transmission protocols	Network, Application.
Subramaniam et al.[29]	2023	Data privacy, authentication vulnerabilities, secure data transmission	Device authentication (SCs), encryption (Twine-LiteNet), integrity verification (TCEV)	SCs, Twine-LiteNet encryption, TCEV verification	All layers.
Su and Xu [30]	2024	Authentication vulnerabilities, privilege escalation, and resource constraints in IoMT	3ECAP: Secure and Lightweight Cluster-Based User Authentication Protocol	Merkle trees,MFA, session key establishment	All layers.
Alsolami et al.[31]	2024	Data breaches, malware, device hijacking, insider threats	IDS using ensemble learning	Stacking, Bagging, Boosting with Radio Frequency (RF) and SVM	Network, Application.
Krishna M et al.[32]	2023	DoS attacks in IoMT	IDS	ML (SVM, RF, LDA, K-NN)	Network Layer.
Balhareth and Ilyas [33]	2024	Intrusion detection in IoMT networks	ML-based IDS with feature selection	Tree-based ML (DT, RF, XGBoost, CatBoost), MI-XGBoost	Network, Application.
Alalwany et al.[34]	2025	ARP spoofing, DoS, Smurf, Port Scan attacks	Stacking ensemble DL-based IDS	ML, DL, Kappa Architecture	All layers.
Bodapati and Raj [35]	2022	Data confidentiality, authentication, and cyber-physical attacks	FPGA-based ASCON-128 encryption	FPGA, ASCON-128 (lightweight AEAD cipher)	Perception, Network.
Arpaia et al. [36]	2021	Side-channel attacks (DPA and CPA) on AES encryption in IoT medical transducers	Random delay, Random SBox, Masking	AES Encryption	Perception, Network.
Patni and Lee [37]	2024	Data privacy, malicious attacks, service inefficiencies	Blockchain-secured federated learning (EdgeGuard)	Blockchain, Federated Learning, Edge Computing, Smart Contracts	All layers.

3) AI and ML: Anomaly detection or intrusion detection and systems strategies that incorporated AI-based tools along with ML tools and DL systems such as RF, SVM and others were found to be highly efficient in real-time threat detection and response.

4) Cloud security measures: Use of blockchain and encryption methods in handling, storing and retrieving information sought to enhance security of cloud and Edge Computing systems against internal and external attacks.

C. RQ3: Security Mechanisms Mapped to IoMT Communication Layers

The reviewed studies presented security mechanisms explicitly mapped to the IoMT communication layers [21], [25], [33]:

1) Perception layer: Aimed at lightweight encryption (e.g., ECC, PUF), biometric authentication, and secure device hardware (i.e., preventing physical attacks, unauthorized access).

2) Network layer: Secure communication protocols such as blockchain and transaction security using the power of AI for IDS came into the picture as the first line of defense against interception and spoofing of data transmission.

3) Application layer: New layers of authentication were considered as well as encryption for API's and the use of artificial intelligence based threat detection systems were also recommended.

4) Cloud and Edge computing layer: For better confidentiality, integrity and availability of data, blockchain based secure storage and quantum resistant cryptographic models were significant.

TABLE IV. SUMMARY AND PERFORMANCE COMPARISON OF SECURITY COUNTERMEASURES IN IOMT

Author	Strengths	Weaknesses	Performance
Xie et al. [21]	Enhanced privacy, low computational cost.	Potential biometric vulnerabilities	11.296 ms, Low CPU with high security.
Sabrina et al. [22]	Decentralization, immutability, resistance to post-quantum attacks.	Computational overhead, integration complexity	Not implemented.
Mavhemwa et al. [23]	Improved usability, dynamic authentication, risk-aware security.	Potential overfitting, usability challenges for some users	Accuracy: 98.6%, AUC: 1.0, FRR & FAR: 0.0.
Kumar et al. [24]	High security (98%), improved privacy, blockchain integrity.	Computational overhead, integration complexity	Security: 98%, Accuracy: 96%.
Laabab et al. [25]	Enhanced authentication, tamper-proof identity verification, improved privacy.	Computational complexity, biometric spoofing risks, integration challenges	Not implemented.
Alsadhan et al. [26]	Increased transparency, immutability, reduced single points of failure.	Scalability issues, high energy consumption, integration complexity	Not implemented.
Mahmood et al.[27]	Enhances data security and system resilience.	Implementation complexity, resource constraints.	Performance not quantitatively measured.
Sandulescu et al.[28]	Ensures data confidentiality and integrity.	High implementation cost and privacy concerns	Accuracy up to 97.1%
Subramaniam et al.[29]	Improves throughput, reduces latency, enhances security.	limited adaptability, computational overhead.	+20% throughput, -10% energy use/delay, +35% network lifetime.
Su and Xu [30]	Strong security, low computational cost.	Overhead in access control management	24.14 ms total cost; 1696-bit communication
Alsolami et al.[31]	High accuracy (98.88%), real-time detection, scalable.	potential overfitting, high computational cost.	Accuracy: 98.88% (Stacking); AUC: 1.0; real-time detection with low latency.
Krishna M et al.[32]	High accuracy, adaptive detection.	limited dataset availability, real-time implementation challenges.	Highest SVM: Receiver Operating Characteristic 99.97%, Sensitivity 99.27%.
Balhareth and Ilyas [33]	High accuracy 98.79%, low false alarm (0.007).	limited to binary classification.	Accuracy: 98.79%, FAR: 0.007 (CatBoost).
Alalwany et al.[34]	High accuracy, real-time detection, low false positives.	computational overhead, dataset dependency.	Accuracy: 99.13% (binary), 99.3% (multi-class); detection time: 0.888 ms.
Bodapati and Raj [35]	35% less LUT usage, 45% higher throughput.	Needs further optimization for real-time medical applications.	1330 LUTs, and 457 Mbps throughput; 56% higher throughput/area compared to baseline.
Arpaia et al. [36]	Masking is most effective (318x protection)	increases computational overhead	Masking: 318× AES protection; Random SBox: 208×; Random delay: 1.3×.
Patni and Lee [37]	High security, scalability, real-time responsiveness.	Computational overhead, energy consumption.	Accuracy: 94.34%; –30.67% communication overhead; robust to 40% malicious nodes.

D. RQ4: Research Gaps and Future Directions

Several research gaps were identified through this SLR, highlighting areas requiring further exploration [21], [18], [35]:

1) Adaptive security frameworks: Need to do more research on the design of Adaptive Security Frameworks, that is Scalable and Real Time Responsive security mechanisms, which can dynamically handle future IoMT threat.

2) Resource efficiency: Future studies should consider the cost of computational overheads and resource in current security measures with such aim of enhancing efficiency without compromising performance.

3) Interoperability standards: Interoperability standards to reduce system complexities and improve security comprehensively among IoMT network of heterogeneous devices.

4) Quantum-resistant solutions: Since the advent of quantum computing is closer now than ever, quantum resistant blockchain solutions as well as crypto techniques need to be researched to ensure that the IoMT is securely resilient for a long term.

VII. CONCEPT DEVELOPMENT

Based the outlined literature analysis suggests this study proposes a security framework called **TrustMed-IoMT** which seeks to address various security issues in IoMT areas. Instead of focusing on the technical side, TrustMed-IoMT serves as a plan for integrating blockchain, AI and cryptography that boosts the safety of all the layers in IoMT.

The framework is structured provide three core components:

1) Blockchain-based identity and access control: Make sure data and authentication cannot be modified at the perception and cloud layers.

2) AI-driven intrusion detection systems: Detecting and responding to threats in the network and application areas.

3) Quantum-resistant encryption: Using techniques such as lattice-based cryptography and QKD, security in the long run is assured while dealing with the cloud.

All these components are assigned to the perception, network, application and cloud/edge layers to build the defense-in-depth strategy. IoMT systems must be improved to make them ready for any future attacks such as ones caused by quantum technology.

TrustMed-IoMT is built on research in the field and can guide research to develop more reliable, wide-ranging, intelligent and secured healthcare IoT systems.

VIII. Conclusion

This study analyzed security risks across the IoMT and covered all major types of security vulnerabilities along with countermeasures. The findings from the study showed that IoMT systems are susceptible to many security challenges spanning from various layers ranging from unauthorized access, malware infections, and data breaches to service disruptions. A key finding is that advanced and integrated security frameworks are an essential feature in today's world and includes lightweight cryptographic techniques with use of blockchain solution, biometrics, and AI enabled IDSs. The strategic approach to enhancing overall system resilience was applied security mechanisms to various IoMT layers were clearly depicted.Adaptive security frameworks, efficient resource utilization with implementation of standards, and adoption of quantum-resistant technologies significant areas for improving IoMT security. Moreover, Solutions such as IDS using ensembles and identity management using blockchain achieved over 98% accuracy. Still, obstacles exist in connecting different systems, using them efficiently and testing them in real situations. These points should be addressed to create systems in IoMT that are both scalable and secure. In addition, Further research should, therefore, target the closing of these gaps by means of scalable and standardized solutions that satisfy the latest cybersecurity threats, and the continuously growing complexity of IoMT infrastructures. In short, further development and cooperation will be necessary to retain safe health care technology, protect important patient data, and continue to provide a stable and safe health care system in an ever more digitalized health care network.

The study is limited by the fact that it uses information from previous research that may use different conditions and testing methods. In addition, several solutions were evaluated in controlled situations which makes it hard to apply them in the real world. Researchers should focus more on putting their systems into practical use and analyzing their performance.

Funding

This work was funded by King Faisal University, Saudi Arabia. [Project No. GRANT KFU251862].

Acknowledgment

This work was supported through the Annual Funding track by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia [Project No. GRANT KFU251862].

Conflicts of Interest

All authors declare no conflict of interest.

Author's Contributions

All authors equally contributed.

References

[1] B. Bhushan, A. Kumar, A. K. Agarwal, A. Kumar, P. Bhattacharya, and A. Kumar, "Towards a secure and sustainable internet of medical things (iomt): Requirements, design challenges, security techniques, and future trends," *Sustainability*, vol. 15, no. 7, p. 6177, 2023.

[2] S. Vishnu, S. J. Ramson, and R. Jegan, "Internet of medical things (iomt)-an overview," in *2020 5th international conference on devices, circuits and systems (ICDCS)*. IEEE, 2020, pp. 101–104.

[3] K. T. Putra, A. Z. Arrayyan, N. Hayati, C. Damarjati, A. Bakar, H.-C. Chen *et al.*, "A review on the application of internet of medical things in wearable personal health monitoring: A cloud-edge artificial intelligence approach," *IEEE Access*, 2024.

[4] M. W. Bhatt and S. Sharma, "An iomt-based approach for real-time monitoring using wearable neuro-sensors," *Journal of Healthcare Engineering*, vol. 2023, no. 1, p. 1066547, 2023.

[5] P. Kumar, G. P. Gupta, and R. Tripathi, "An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for iomt networks," *Computer Communications*, vol. 166, pp. 110–124, 2021.

[6] F. Sajjad, "Safeguarding healthcare organizations from iomt risks," November 2024, url:https://levelblue.com/blogs/security-essentials/safeguarding-healthcare-organizations-from-iomt-risks Accessed: February 12, 2025. [Online]. Available: https://levelblue.com/blogs/security-essentials/safeguarding-healthcare-organizations-from-iomt-risks

[7] D. R. Ibrahim and M. Y. Thanoun, "Iomt availability threats attacks and solution," in *2024 1st International Conference on Emerging Technologies for Dependable Internet of Things (ICETI)*. IEEE, 2024, pp. 1–8.

[8] A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali, and R. Jain, "Recent advances in the internet-of-medical-things (iomt) systems security," *IEEE Internet of Things Journal*, vol. 8, no. 11, pp. 8707–8718, 2020.

[9] P. K. Sadhu, V. P. Yanambaka, A. Abdelgawad, and K. Yelamarthi, "Prospect of internet of medical things: A review on security requirements and solutions," *Sensors*, vol. 22, no. 15, p. 5517, 2022.

[10] T. Abbas, A. H. Khan, K. Kanwal, A. Daud, M. Irfan, A. Bukhari, and R. Alharbey, "Iomt-based healthcare systems: A review." *Computer Systems Science & Engineering*, vol. 48, no. 4, 2024.

[11] N. A. Askar, A. Habbal, A. H. Mohammed, M. S. Sajat, Z. Yusupov, and D. Kodirov, "Architecture, protocols, and applications of the internet of medical things (iomt)." *J. Commun.*, vol. 17, no. 11, pp. 900–918, 2022.

[12] R. Hireche, H. Mansouri, and A.-S. K. Pathan, "Security and privacy management in internet of medical things (iomt): A synthesis," *Journal of cybersecurity and privacy*, vol. 2, no. 3, pp. 640–661, 2022.

[13] J.-P. A. Yaacoub, M. Noura, H. N. Noura, O. Salman, E. Yaacoub, R. Couturier, and A. Chehab, "Securing internet of medical things systems: Limitations, issues and recommendations," *Future Generation Computer Systems*, vol. 105, pp. 581–606, 2020.

[14] P. Bajpayi, S. Sharma, and M. S. Gaur, "Ai driven iot healthcare devices security vulnerability management," in *2024 2nd International Conference on Disruptive Technologies (ICDT)*. IEEE, 2024, pp. 366–373.

[15] M. Waqdan, H. Louafi, and M. Mouhoub, "An iot security risk assessment framework for healthcare environment," in *2023 International Symposium on Networks, Computers and Communications (ISNCC)*. IEEE, 2023, pp. 01–08.

[16] R. M. Czekster, P. Grace, C. Marcon, F. Hessel, and S. C. Cazella, "Challenges and opportunities for conducting dynamic risk assessments in medical iot," *Applied Sciences*, vol. 13, no. 13, p. 7406, 2023.

[17] I. A. Jayaraj, B. Shanmugam, S. Azam, and S. Thennadil, "Detecting and localizing wireless spoofing attacks on the internet of medical things," *Journal of Sensor and Actuator Networks*, vol. 13, no. 6, p. 72, 2024.

[18] S. R. Sankepally, N. Kosaraju, V. Reddy, and U. Venkanna, "Edge intelligence based mitigation of false data injection attack in iomt framework," in *2022 OITS International Conference on Information Technology (OCIT)*. IEEE, 2022, pp. 422–427.

[19] S. Madanian, T. Chinbat, M. Subasinghage, D. Airehrour, F. Hassandoust, and S. Yongchareon, "Health iot threats: Survey of risks and vulnerabilities," *Future Internet*, vol. 16, no. 11, p. 389, 2024.

[20] R. Sasaki, "Risk assessment method for balancing safety, security, and privacy in medical iot systems with remote maintenance function," in *2020 IEEE 20th International Conference on Software Quality, Reliability and Security Companion (QRS-C)*. IEEE, 2020, pp. 190–197.

[21] Q. Xie, Z. Ding, and Q. Xie, "A lightweight and privacy-preserving authentication protocol for healthcare in an iot environment," *Mathematics*, vol. 11, no. 18, p. 3857, 2023.

[22] F. Sabrina, S. Sohail, and U. U. Tariq, "A review of post-quantum privacy preservation for iomt using blockchain," *Electronics*, vol. 13, no. 15, 2024. [Online]. Available: https://www.mdpi.com/2079-9292/13/15/2962

[23] P. M. Mavhemwa, M. Zennaro, P. Nsengiyumva, and F. Nzanywayingoma, "An android-based internet of medical things adaptive user authentication and authorization model for the elderly," *Journal of Cybersecurity and Privacy*, vol. 4, no. 4, pp. 993–1017, 2024.

[24] M. Kumar, S. Verma, A. Kumar, M. F. Ijaz, D. B. Rawat *et al.*, "Anaf-iomt: A novel architectural framework for iomt-enabled smart healthcare system by enhancing security based on recc-vc," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 12, pp. 8936–8943, 2022.

[25] I. Laabab, A. Ezzouhairi, N. El Madhoun, and M. H. Khan, "Blockchain and biometric systems integration for iomt security," in *2024 8th Cyber Security in Networking Conference (CSNet)*. IEEE, 2024, pp. 259–262.

[26] A. Alsadhan, A. Alhogail, and H. Alsalamah, "Blockchain-based privacy preservation for the internet of medical things: A literature review," *Electronics*, vol. 13, no. 19, p. 3832, 2024.

[27] M. Mahmood, M. I. Khan, H. Hussain, I. Khan, S. Rahman, M. Shabir, B. Niazi *et al.*, "Improving security architecture of internet of medical things: A systematic literature review," *IEEE Access*, vol. 11, pp. 107 725–107 753, 2023.

[28] V. Sandulescu, M. Ianculescu, L. Valeanu, and A. Alexandru, "Integrating iomt and ai for proactive healthcare: Predictive models and emotion detection in neurodegenerative diseases," *Algorithms*, vol. 17, no. 9, p. 376, 2024.

[29] E. V. D. Subramaniam, K. Srinivasan, S. M. Qaisar, and P. Pławiak, "Interoperable iomt approach for remote diagnosis with privacy-preservation perspective in edge systems," *Sensors*, vol. 23, no. 17, p. 7474, 2023.

[30] X. Su and Y. Xu, "Secure and lightweight cluster-based user authentication protocol for iomt deployment," *Sensors*, vol. 24, no. 22, 2024. [Online]. Available: https://www.mdpi.com/1424-8220/24/22/7119

[31] T. Alsolami, B. Alsharif, and M. Ilyas, "Enhancing cybersecurity in healthcare: Evaluating ensemble learning models for intrusion detection in the internet of medical things," *Sensors*, vol. 24, no. 18, p. 5937, 2024.

[32] S. R. Kumar *et al.*, "Intrusion detection system for defending against dos attacks in the iomt ecosystem," in *2023 4th International Conference on Communication, Computing and Industry 6.0 (C216)*. IEEE, 2023, pp. 1–5.

[33] G. Balhareth and M. Ilyas, "Optimized intrusion detection for iomt networks with tree-based machine learning and filter-based feature selection," *Sensors*, vol. 24, no. 17, p. 5712, 2024.

[34] E. Alalwany, B. Alsharif, Y. Alotaibi, A. Alfahaid, I. Mahgoub, and M. Ilyas, "Stacking ensemble deep learning for real-time intrusion detection in iomt environments," *Sensors*, vol. 25, no. 3, p. 624, 2025.

[35] K. Raj and S. Bodapati, "Fpga based light weight encryption of medical data for iomt devices using ascon cipher," in *2022 IEEE International Symposium on Smart Electronic Systems (iSES)*. IEEE, 2022, pp. 196–201.

[36] P. Arpaia, F. Bonavolontà, A. Cioffi, and N. Moccaldi, "Power measurement-based vulnerability assessment of iot medical devices at varying countermeasures for cybersecurity," *IEEE Transactions on Instrumentation and Measurement*, vol. 70, pp. 1–9, 2021.

[37] S. Patni and J. Lee, "Edgeguard: Decentralized medical resource orchestration via blockchain-secured federated learning in iomt networks," *Future Internet*, vol. 17, no. 1, p. 2, 2024.