SEUSL

Sri Lankan Journal of Technology
Research

SLJoT
2026 Issue 01 37-56
ISSN-2773-6970

Security Vulnerabilities and Resilience Strategies in Healthcare IoT Systems: A Comprehensive Review

M.R.M. Hanan[1] and M.J Ahamed Sabani[2*]

[1]Department of Computer Science and Informatics
[2*]Department of Information and Communication Technology

*Corresponding Author: mjasabani@seu.ac.lk || ORCID: 0000-0002-9583-9057

Received: 18-10-2025. * Accepted: 29-06-2026 * Published Online: 30-06-2026

Abstract- Internet of Things (IoT) technologies in the healthcare industry, also known as the Internet of Medical Things (IoMT), have proven to greatly improve patient monitoring, diagnostics, and clinical decision-making. The increasing prevalence of resource-challenged medical devices, wireless connectivity, and cloud services, however, has brought new risks around security and privacy concerns that can now directly impact patient safety and data integrity. In this paper, a thorough study of 41 peer-reviewed research papers from January 2018 through May 2025 revealed the current state of security vulnerabilities and resilience strategies in healthcare IoT systems. It provides a comprehensive analysis of security threats at the device, network, and application levels such as unauthorized access, malware and ransomware, data breaches, and denial-of-service attacks delivered in a systematic manner. This contrasts with existing surveys, which consider single security mechanisms and improve upon various multi-layered security means such as AI-enabled anomaly detection, blockchain-based authentication and auditability, low-compute cryptographic techniques, and privacy-preserving methods such as federated learning. The outcomes also show that although emerging technologies add a great deal of security and trust capabilities, issues on scalability, interoperability, deployment, and regulations are not yet fully addressed. This review highlights important knowledge gaps and offers structured knowledge and future directions for research to address the design of secure, resilient, and practically deployable IoMT architectures for real-world healthcare environments.

***Keywords*:** IoMT, IoT-based healthcare security, IoT security vulnerability, multi-layer defense, resilience in healthcare security

Recommended APA Citation

Hanan, M. R. M., & Sabani, M. J. A. (2026). Security vulnerabilities and resilience strategies in healthcare IoT systems: A comprehensive review. *Sri Lankan Journal of Technology, 7*(1), 37–56.

Introduction

The Internet of Things (IoT) is a revolutionary technology in the health field, where interconnected medical devices, wearables, and intelligent monitoring systems can facilitate real-time monitoring and diagnosis at a distance of patients' health (Mejía Granda et al., 2023). In healthcare, the Internet of Things (IoT) is known as the "Internet of Medical Things" (IoMT) and is more and more used in hospitals, healthcare centers, and home-based healthcare settings. By continuously observing vital signs, early identification of disease, and automated emergency alerts, IoMT systems have a much stronger impact on the quality, efficiency, and accessibility of healthcare services (Kateb, 2025).

However, the explosive growth of IoMT has posed significant security and privacy concerns that pose a direct threat to patient safety and the privacy of medical data. Yet, the rapid proliferation of IoMT has emerged as huge security and privacy challenges directly endangering patient safety and the confidentiality of sensitive medical information (Barrett et al., 2023). The healthcare Internet of Things is extremely susceptible to various factors such as semi-secure deployment, limited computational power, dependence on wireless communication protocols, and heterogeneous architectures (Javaid et al., 2018; Alzahrani & Asghar, 2024). Fraud and unsafe deployment practices, such as using obsolete or incompatible software and hardware, are common vulnerabilities, including weak authentication methods, firmware updating problems, unsafe communications encryption, ransomware, distributed denial of service (DDoS) attacks, installing and using malware, and physically tampering with the system unauthorized (Al-Otaibi et al., 2025; Khan et al., 2025). There have been multiple examples from the real world that indicate successful IoMT attacks can impact clinical operations, patient information, and even human life.

In recent studies, the focus has been on implementing advanced technologies to enhance the security and resilience of IoT systems in healthcare. Various recent research efforts have investigated ways to leverage advances in technology to achieve increased security and resilience of IoT systems in healthcare. Cloud and Edge Computing are used to process security information with a capability of scaling up and providing low latency, and Edge Computing is used for localized detection closer to the medical device resource constraints, which would not be possible in a traditional Secure Cloud Computing (Ksibi et al., 2023). Tech solutions based on blockchain have been advanced to support distributed authentication, secure data sharing, and tamper evidentations in decentralized health care environments. Conversely, the use of artificial intelligence (AI) and deep learning techniques is rapidly growing in the detection of anomalies, in predictive threat analysis, and in the automation of intrusion prevention in IoMT ecosystems (Alnaim & Alwakeel, 2023). However, lightweight cryptographic and privacy-preserving protocols were also developed to mitigate the cost of computing and energy of medical IoT. (Ksibi et al., 2023).

In addition to technical concerns, IoMT systems must also adhere to regulatory and privacy frameworks like the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR) to maintain strict standards for patient data collection, processing, and security (Hathaliya & Tanwar, 2020; Krishnamoorthy et al., 2023). Security under-situations in healthcare IoT put systems at risk of significant legal, financial and reputation penalties, aside from patient safety issues. Therefore, the findings from recent research underlines the cited shortcomings of the isolation of either a security solution or network-centric approach and recommends using integrated multi-layered defense solutions that will employ integrated device-level protection, secure communication, intelligent threat detection, and resilient data management (Babar et al., 2025).

The first goal of this paper is to systematically identify and classify security vulnerabilities in IoMT systems including device, network and application layers. Secondly, it

considers and evaluates strategies for resilience, including new technologies, like AI, blockchain, edge computing and lightweight cryptography. Third, it identifies limitations in terms of practical deployments, regulations and open research areas of concern when adopting IoMT in the real-world medical context. In this work, a new holistic, cross-layer review from a security perspective, through the lens of medical IoTs, is presented, aiming to offer structure, insights, and future directions for developing an IoT-based healthcare system, which is secure, resilient, and compliant with regulations (Zanbouri et al., 2024).

Methodology

The authors followed the guidelines in PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) for a systematic examination of a total of 41 peer-reviewed articles relevant to the issues of security vulnerabilities and methods to enhance the security in the context of IoT in the healthcare sector were considered. Recent and good-quality papers are more preferred, and to make sure that the experimentations and research that were picked won't be out of date, some papers in the initial list retrieved from the internet were removed because of their bad content or because they failed to be indexed in esteemed scientific databases like IEEE Xplore, Springer, ScienceDirect, and arXiv. The keywords used in the literature search were "IoT security vulnerabilities," "healthcare IoT," "medical device cybersecurity," and "blockchain in IoT and AI-driven IoT security." The selected studies were grouped into categories such as vulnerable point, vulnerable layer, and vulnerable application point through considering vulnerable points and suitable techniques for resilience in point of view level, communication point of view, and application point of view, respectively. Healthcare application areas like remote patient monitoring, medical networks of sensors, and telemedicine systems have been emphasized in particular. The articles were analyzed systematically, looking for recurring themes, emerging trends in research, and critical gaps, both theoretically and practically.

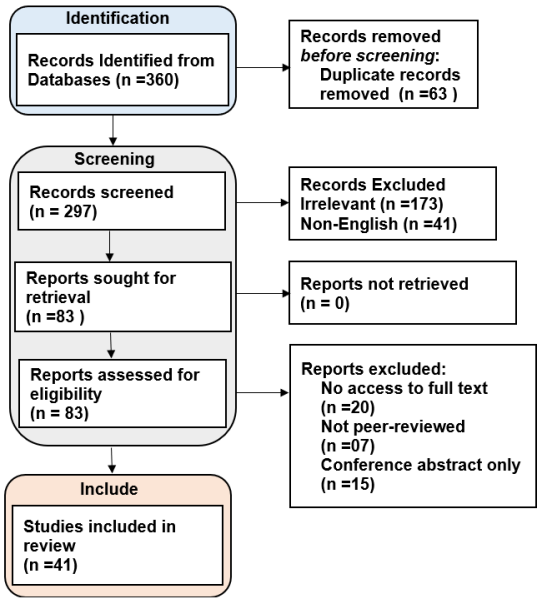

Figure 01. *Prisma Diagram to workflow*

Through an initial literature search using selected academic databases, 360 security and resilience-related records were found in healthcare IoT systems. 63 duplicate records were removed, leaving 297 studies for screening. A total of 214 records were excluded after title

and abstract screening 173 were either irrelevant or not in English. As a result, a total of 83 reports were requested for full-text retrieval, and those retrieved had been accessed. Of the retrieved reports, 42 studies were excluded because full text was not available (n = 20), the study was not peer-reviewed (n = 7), or the study was available only as an abstract from a conference presentation (n = 15). Lastly, 41 peer-reviewed studies, published from 2018 to 2025, were chosen and incorporated into the qualitative synthesis conducted for the current review.

Table 1
Summary of Literature Review Methodology for Healthcare IoT Security

Step	Description	Details / Criteria
1. Database Search	Identify relevant articles	IEEE Xplore, Springer, ScienceDirect, MDPI, arXiv, Scopus
2. Keywords Used	Define search terms	"Healthcare IoT", "IoMT security", "IoT vulnerabilities", "IoT resilience", "Blockchain in healthcare", "AI-based security IoT"
3. Inclusion Criteria	Decide which papers to include	Articles published 2018–2025, peer-reviewed journals or conferences, English language, relevance to security and resilience in healthcare IoT
4. Exclusion Criteria	Decide which papers to exclude	Non-English articles, duplicates, studies unrelated to healthcare or IoT security, non-peer-reviewed content
5. Screening	Initial assessment	Title and abstract screening to remove irrelevant articles
6. Eligibility Check	Full-text review	Evaluate methodology, findings, and relevance of selected studies
7. Data Extraction	Collect relevant information	Study type, IoT security threats, attack types, defense mechanisms, AI/Blockchain methods, performance metrics
8. Synthesis	Analyze and organize findings	Group vulnerabilities, security solutions, and resilience strategies into themes; highlight gaps and trends

Literature Review and Synthesis of Evidence

Security Vulnerabilities in Healthcare IoT Systems

Cyber-attacks on healthcare IoT systems are becoming significantly more targeted because of the sensitivity of patient information and the prevalence of the practice of combining medical technology with amenities. The presence of security vulnerabilities of medical devices, software, and network infrastructures has been extensively documented, and among such vulnerabilities, there exist weak authentication mechanisms, older firmware, inadequate encryption, and network-based vulnerabilities to attacks (Mejía Granda et al., 2023). These weaknesses may affect the security of patients, integrity of data and system availability; hence, the aspect of mitigating the overall situation requires holistic approaches. IoMT systems have also been suggested to use layered security frameworks combining device-level security with network-level security and application-level security in addition to intrusion detection systems, secure-data encryption, and blockchain-based verification (Almulla et al., 2025).

Deep-learning based anomaly detection and intrusion prevention have also been proven to boost security in a remote healthcare monitoring system. Algorithmically optimized models

like the Jellyfish Search Optimizer, enhance the identification of unusual network and device behavior as well as reduce false positives (Kateb, 2025). In developing virtual healthcare systems such as metaverse enabled services, there are threats of stealage, loss of identity, and loss of information through IoT data. To maintain privacy-sensitive and safe data processing in these conditions, the access control and AI-based surveillance models are suggested based on blockchain principles (Qureshi, 2025). Such malware attacks as Mirai or Bashlite use weak settings of devices and unapplied vulnerabilities to achieve distributed denial-of-service (DDoS) attacks to popular healthcare services and threaten the safety of patients (Barrett et al., 2023). Starting to counter the effects of such attacks, it has been suggested that blockchain-based decentralized authentication protocols should be introduced to improve communication resilience of IoT healthcare networks (Javaid et al., 2018). Medical sensor network security frameworks can also be AI-based by applying anomaly detection, encryption and blockchain verification to deliver privacy and trust as well as security in communication between parties (Al-Otaibi et al., 2025).

Edge computing approaches offer scalable, low-latency lightweight hybrid authentication frameworks based on a blockchain combined with edge computing, that ensure IoMT devices can securely obtain authentication without damaging computational efficiency (Khan et al., 2025). The potential dangers in the healthcare logistics IoT data flow, that may be detected using cyber vulnerability detection systems, include blind access, altered data and man-in-the-middle, all in real-time (Alzahrani & Asghar, 2024). Detailed research on the vulnerabilities of the IoT has divided the attack vectors, such as malware distribution, protocol-based, physical device manipulation, and unauthorized access, and the mitigation best practices (Coston et al., 2025). Privacy-Conservation Protecting sensitive patient information In the IoT of healthcare, privacy-stronger mechanisms concentrate on the safe circulation of data, encrypted data, delicate limited entry to data, and anonymization methods to handle sensitive patient data yet still to be interoperable (Amoo et al., 2024 and Nabha et al., 2023). Heterogeneity of mobile IoT devices creates challenges since it involves heterogeneous hardware, wireless communicative protocols and power limitation which require light weight and adaptive safety (Harkai, 2024).

Cryptography and Blockchain-Based Solutions

The limited resources of IoT devices require using vigorously small scale cryptographic systems that can regulate the degree of security and guarantee the effectiveness of the computation procedure . The approaches to emergency medical services based on blockchain have demonstrated that they are capable of taking key patient information securely and promptly within a smart city system because they can offer real capabilities to the decentralized IoT systems (Ksibi et al., 2023). The research in Healthcare 4.0 has revealed compliance, technical, and privacy issues that put into perspective the fact that there must be compliance mechanisms, proper encryption and standard communication protocols (Hathaliya & Tanwar, 2020).Machine learning coupled with edge computing allows the detection of anomalies, predictive data, and real time decision-making regarding IoT healthcare networks (Alnaim & Alwakeel, 2023), (Islam et al., 2023). Predictive diagnostics, anomaly detection, and secure data handling have been enhanced through AI applications and have brought an increase in the efficiency of operations, reliability of a system, or provide better patient outcomes (Ali et al., 2023), (Mao et al., 2023), and (Amiri et al., 2024).

Deep learning procedures designed by blockchain guarantee that data is confidential and intact through transmission meaning that third parties cannot access and corrupt data in the networked healthcare systems (Kumar et al., 2023), (Zanbouri et al., 2024). The use of continuous authentication method with deep learning enhances identity verification and insider

threat prevention which provides dynamic access control in the IoMT system (Singh et al., 2023). Machine learning-powered models allow identifying threats beforehand and monitoring the system and optimizing its performance (Babar et al., 2025). Heart disease and breast cancer are just two examples of the conditions, which have IoT-enabled predictive frameworks, where AI-driven analysis and secure remote monitoring are utilized to enhance patient outcomes and clinical decisions (Rajkumar et al., 2023), (Rani et al., 2025). The second type of cloud-federated IoT based on convolutional neural networks and blockchain-enforced federated learning do not compromise privacy but allow distributed analysis of electronic health records (Alzubi et al., 2022), (Ashraf et al., 2022). Investigations conducted on the topics of IoT security protocols indicate the absence of encryption, standardization, and anomaly detection capabilities, which suggests the need to conduct ongoing research in directing better protection of the IoMT security (Mishra, 2025).

Large-Scale Vulnerability Assessments

The practical application of an IoT system reveals weaknesses in the implementation, such as weak authentication system, outdated software, lack of updates to the software, and shows the urgency of implementing the strategies on security stringently (Selvaraj et al., 2025). Multilayer cryptography and artificial intelligence based monitor systems have been developed to secure transmission of information without interfering with the system performance (Rahim & Chishti, 2025), (Rasheed & Kumar, 2025). Multi-layers and high level multi-defense protocols have been enforced to safeguard healthcare IoT capabilities, so as to be resilient to new attack patterns (Panahi, 2025), (Ali et al., 2025). The response techniques have been streamlined using ProSRN and I COM approaches and other practices involving threat identification and mitigation to provide intensive supervision (Sowjanya et al., 2025), (Qi, 2025). The application of such technologies as AI, blockchain, and cryptography can be beneficial in order to minimize the points of vulnerability, making a system more resilient. Multi-layered, predictive AI surveillance, blockchain entitled access, and cryptography solutions all improve the achievement of security, continuity and reliability of activities (Ali et al., 2022), (Krishnamoorthy et al., 2023), (Rehman et al., 2025). IoT applications implemented in hospitals with multi-layer machine infrastructures hear more easy monitoring and system developers can identify threats at an early stage and ensure that sensitive healthcare data is safeguarded (Panahi, 2025), (Ali et al., 2025).

Cyber-Attacks and Threat Analysis

Cyber-attacks in healthcare IoT constitute of ransomware, DDoS, malware intrusion, as denoted by colossal reviews. The attacks disrupt the healthcare operations and compromise patient care and disclose confidential medical data. Studies are directed on the evolvement of the convergence of AI, blockchain, cryptography, constant checks and verification, layered-security systems to provide secure, resilient, dependable, and patient-centric healthcare IoT devices (Akram et al., 2025), (ElSayed et al., 2025). Such methodologies as statistical modeling, deep learning classifiers, and anomaly detection algorithms have been applied to prevent in order to ensure that the potential damages are minimized in time to detect attacks. The importance of strong IoT systems capable of identifying, isolating and fighting off threats in real-time situation has also been highlighted recently. They are decentralized access controls solutions, multi-level encryption and AI-based threat prediction systems to allow healthcare providers to proceed with activities upon computer attacks (Mejía Granda et al., 2023)-(ElSayed et al., 2025). It is also experimentally demonstrated that blockchain may be utilized to enhance inter-institutional health networks privacy and security in data analytics by

combining it with deep learning and federated learning (Kumar et al., 2023), (Zanbouri et al., 2024), (Alzubi et al., 2022), (Ashraf et al., 2022).

Summary of Trends and Research Gaps

According to the literature, there are a few crucial trends: (i) the employment of AI and machine learning in detection of threats and predictive analytics, (ii) using blockchain in secure and decentralized data management, (iii) using lightweight cryptography in low-resource IoT devices, and (iv) implementation of deploying multi-tier security schemes that integrate device-level, network-level, and application-level security. Regardless of these innovations, there are still flaws in the standardization of the security protocol of the IoMT, timely reaction to threat, and scalable application across heterogeneous gadgets (Almulla et al., 2025), (Mishra, 2025), (Selvaraj et al., 2025). Issues to be addressed regarding interoperability, energy efficiency and privacy preservation methods are to be addressed through further research in order to maintain high availability of critical healthcare services.

Table 02

Comparative Analysis of papers on Healthcare IoT

Theme	References	Method / Approach	Key Findings	Comparison / Observations	Research Gap
Layered Security & Defense-in-Depth	Almulla et al., 2025	Multi-layer security framework	Integrates device, network, and cloud layers; improves holistic security	Aligns with Babar et al., 2025 and Panahi, 2025 emphasizing multi-layered defenses	Limited real-world deployment studies
	Babar et al., 2025	Hybrid deep learning-driven IoT security	Enhances performance and detection accuracy	Adds AI component compared to Almulla et al.	Computational overhead for edge devices
	Panahi, 2025	Secure IoT framework for healthcare	Emphasizes practical implementation of layered security	Complements above studies	Needs empirical evaluation in hospital settings
AI / ML for Threat Detection	Al-Otaibi et al., 2025	AI-driven privacy/trust framework	Enhances security of medical sensor networks	Supports proactive threat detection trends	Scalability in real-time applications
	Kateb, 2025	Deep learning + Jellyfish Search Optimizer	High accuracy anomaly detection	Computationally intensive compared to Alnaim &	Lightweight models for resource-constrained

Theme	References	Method / Approach	Key Findings	Comparison / Observations	Research Gap
				Alwakeel, 2023	devices needed
	Alnaim & Alwakeel, 2023	Edge computing + ML	Efficient detection with lower latency	Slightly lower accuracy but suitable for IoT devices	Need hybrid solutions balancing accuracy and efficiency
	Islam et al., 2023	DL-based remote monitoring	Real-time detection of health issues	Confirms effectiveness of ML for IoT healthcare	Validation across diverse devices lacking
	Rani et al., 2025	Fractional dung beetle optimization + DL	High-precision cancer classification	Advanced optimization enhances ML performance	Computational cost in IoMT
IoT Device Vulnerabilities	Mejía Granda et al., 2023	Vulnerability analysis of medical devices/software	Weak authentication, outdated firmware, insecure settings	Confirms findings of Barrett et al., 2023	Need lightweight security for resource-constrained devices
	Barrett et al., 2023	Attack simulation (Mirai, Bashlite)	Demonstrates real attack vectors on IoT devices	Supports vulnerability findings	Real-world mitigation strategies required
	Akram et al., 2025	Survey on healthcare IoT device security	Highlights device-level challenges and solutions	Aligns with ElSayed et al., 2025	Deployment of proposed solutions not tested
	Coston et al., 2025	Comprehensive vulnerability study	Presents countermeasure strategies	Confirms trends across IoMT security literature	Real-world validation limited
	Harkai, 2024	IoT mobile device vulnerabilities	Device-specific weaknesses, mobility concerns	Adds mobility perspective to device vulnerability analysis	Practical security policies for mobile IoT missing
Blockchain & Decentralized Security	Kumar et al., 2023	Blockchain + DL for secure data transmission	Tamper-evident, decentralized authentication	Confirms federated control and auditability benefits	Latency and scalability concerns

Theme	References	Method / Approach	Key Findings	Comparison / Observations	Research Gap
	Khan et al., 2025	Lightweight blockchain + edge computing	Scalable hybrid authentication	More efficient than Kumar et al.	Hospital deployment validation needed
	Javaid et al., 2018	Blockchain for DDoS mitigation	Effective prevention of IoT device-based DDoS	Supports blockchain-based threat mitigation	Limited to specific attack types
	Ksibi et al., 2023	Blockchain for emergency healthcare	Fast, secure service in smart cities	Domain-specific application of blockchain	Wider adoption and evaluation needed
	Alzubi et al., 2022	Federated learning + blockchain + CNN	Privacy-preserving EHR processing	Complements Kumar et al., 2023; ensures privacy	Computational overhead in IoT devices
	Ashraf et al., 2022	Fidchain: Federated IDS + blockchain	Secures IoT healthcare applications	Confirms federated blockchain utility	Practical deployment studies limited
	Zanbouri et al., 2024	GSO-based blockchain optimization	Performance improvement in IIoT	Supports hybrid optimization approaches	Limited healthcare-specific validation
Privacy-Preserving Techniques	Nabha et al., 2025	IoT healthcare privacy mechanisms	Maintains data confidentiality	Aligns with Alzubi et al., 2022 and Ashraf et al., 2022	Regulatory and practical adoption frameworks missing
	Alzubi et al., 2022	Federated learning + CNN	Privacy-preserving EHR sharing	Edge-computation friendly approach	Need evaluation in large-scale IoT environments
	Ashraf et al., 2022	Blockchain-enabled federated IDS	Data privacy maintained	Confirms federated privacy preservation	Integration complexity remains high
Emerging Technologies & Metaverse	Qureshi, 2025	Metaverse + IoT healthcare	Adaptive security mechanism for immersive healthcare	Introduces novel security concerns beyond conventional IoMT	Solutions still conceptual; practical deployment lacking

Theme	References	Method / Approach	Key Findings	Comparison / Observations	Research Gap
	Rajkumar et al., 2023	IoT + DL for heart disease prediction	Accurate medical predictions	Confirms domain-specific utility of IoT + DL	Real-time testing and validation needed
	Mao et al., 2023	Triboelectric sensors + VR	Flexible, real-time monitoring	Novel interface for immersive healthcare	Security standards for VR healthcare needed
Operational, Compliance & Standards	Krishnamoorthy et al., 2023	Survey on IoT-driven Healthcare 4.0	Current challenges and future directions	Aligns with Selvaraj et al., 2025 emphasizing gaps	Standardized benchmarks missing
	Selvaraj et al., 2025	Large-scale IoT security weakness study	Identifies vulnerabilities in the wild	Confirms need for continuous monitoring	Real-time mitigation strategies not fully explored
	Rahim & Chishti, 2025	IoT security innovations	Comprehensive overview of threats and solutions	Supports trends from multiple AI/blockchain studies	Integration in healthcare operations needs testing
	Mishra, 2025	IoT security protocols	Current protocols and limitations	Provides foundation for protocol selection	Need for lightweight and scalable protocols
	Amoo et al., 2024	Review of protective measures	Evaluates IoT cybersecurity measures	Confirms device and network-level security importance	Empirical hospital implementation missing
	Ali et al., 2025	AI in healthcare: review	Benefits, challenges, methodologies	Confirms AI-based threat detection trends	Practical deployment frameworks needed
	Ali et al., 2022	DDoS recognition in IoT	Threat detection and mitigation	Supports vulnerability analysis studies	Deployment in heterogeneous IoT environments required
	Hathaliya & Tanwar, 2020	Survey on Healthcare 4.0 security	Exhaustive coverage of issues and solutions	Aligns with emerging IoT/AI security trends	Continuous updates needed due to

Theme	References	Method / Approach	Key Findings	Comparison / Observations	Research Gap
					technology evolution

Synthesis of findings

The findings of this study, which synthesizes insights from 41 studies, also show some overlap in the security threats that researchers are seeing with the Internet of Medical Things (IoMT). One of the common findings is vulnerabilities in devices and the firmware are still the biggest threat in healthcare IoT ecosystems. Common problems are weak authentication, out-of-date software, insecure default settings, and no encryption, allowing devices to be hijacked, have their data leaked, and have untrustworthy sensor readings manipulated. This confirms the importance of hardware and software-level security mechanisms and how it's crucial if there isn't enough lower-layer security. Many studies have been published to underscore the need for multiple layers of defense from device to network to cloud level to safeguard patient data and continue services in the face of a breach.

AI/Machine Learning (ML) is gaining traction for their usefulness in threat detection and IoMT system resilience. Image monitoring by prediction and outlier detection as well as continuous authentication through deep learning models are proposed approaches. These techniques illustrated here have reduced latency in detecting and lower false sign ups. But there are challenges about adversarial robustness, data availability, computational expense and implementation on resource limited devices. Moreover, the lack of explainability in most of the AI models hinders their direct use in clinical practice, which makes them not interpretable and having no rules.

Security solutions that rely on the blockchains also come to the fore in the literature. Blockchain can prevent data exchange tampering, maintain auditability and control by the authority, and provide decentralized authentication and federated access control. However, it has come with its own set of problems, namely the scalability and the significant amount of energy consumption that goes into it as well as the transaction latency, particularly in the life-critical environment in hospitals. Some studies suggest to use permissioned chains, light consensus mechanisms, or off-chain designs to solve these problems.

Another important aspect is the use of privacy-preserving architectures, which are crucial for meeting strict data protection requirements in the healthcare sector. Collaborative analytics without losing patient privacy is possible via techniques like federated learning, encrypted aggregation, and secure multiparty computation. These approaches enable organizations to share models, without having to share sensitive medical data, while maintaining ownership and oversight of their respective sources. Certain IoMT applications, like wearable or implantable sensors, devices in healthcare-related applications within the metaverse or emergency response and communication devices, have distinct security needs. Different applications present different requirements, such as energy-saving devices for wearables and data security concerns in immersive metaverse medical applications. This is a strong reminder that an overall approach to security is not effective and that there is no single solution that fits everyone.

This is to be expected because survey papers and systematic reviews have made up a considerable part of the literature; the growing research interest into IoMT security is evident from these as well. While these studies can provide a comprehensive view of the integration of knowledge between domains of AI, blockchain and Healthcare 4.0, there are gaps. The effects in real-world applications are rare and long-term evaluation even more so; there are also few real-world products that are examined under only simulated or small-scale cases. The

interoperability of the heterogeneous IoT domains and compliance with healthcare regulations are under-explored. The key to closing these gaps is to have both integrated defense in depth methods to save money and decrease the risk, as well as to use secure devices, encrypted communication, network segmentation, and continuous monitoring. Explainability/rules elements should be included in AI/ML solutions to reduce adversarial attacks and false positives. An important challenge with blockchain implementations is necessarily guaranteeing the accountability of these while also being efficient, not setting a design up the working system so that it takes up excessive latency and energy. Development of the system should adhere to privacy by design and should be mandatory to incorporate federated learning and uses of differential privacy when performing analytics across institutions.

There are still many important research gaps. There is a lack of benchmarking datasets and evaluation platforms for IoMT security. The lightweight cryptographic and ML models for resource constrained devices should be explored. These adversarial types of attacks and the comprehensibility of the detection systems for users must be addressed using AI. Testing of vendor/device compatibility and compliance with regulations is necessary. Moreover, integrating incidents as part of clinical operations has not been extensively researched, although it is an important aspect of patient safety.

Unified IoMT Security Resilience Model

First, to cope with the lack of uniformity in previous research, the study provides a Unified IoMT Security Resilience Model inspired by fusing together security mechanisms in various architectural levels. The end-to-end data lifecycle in healthcare IoT systems leads to three layers, namely the device layer, edge layer and cloud layer, of IoMT security solutions. The focus of the device layer is on resource-limited medical devices and sensors, with light-weight cryptographic operations, secure boot operations, firmware integrity, authentication and physical tamper resistance. The edge is intelligent via edge gateways, which would help detect anomaly, traffic indication and give real-time response with AI and machine learning techniques. The cloud environment provides the infrastructure for data analytics on a large scale, for secure data storage, access control and monitoring of the system across its entire operation, and frequently adds layers of auditability and trust management, usually implemented through a blockchain based system.

AI/ML modules and blocks as a crosscutting construct offer adaptive threat detection, predictive analytics, decentralized authentication, and tamper-evident rendering while logging. A policy and regulatory overlay is found throughout the layers, providing adherence to healthcare laws and regulations like HIPAA and GDPR, and compliance with private-by-design measures. All reviewed studies are illustrated on this shared model based on the security goal they focused on, which allows an analysis of existing approaches within the uniform context of this model. The mapping exercise indicates that although significant effort is being dedicated to network and cloud-based security solutions, the number of solutions dedicated to lightweight, explainable security solutions at the device and edge layer is relatively low. The model proposed therefore not only provides a taxonomy and analytical framework to identify the research gaps and suggest future designs of IoMT security but also includes metrics used to evaluate the performance of IoMT security.

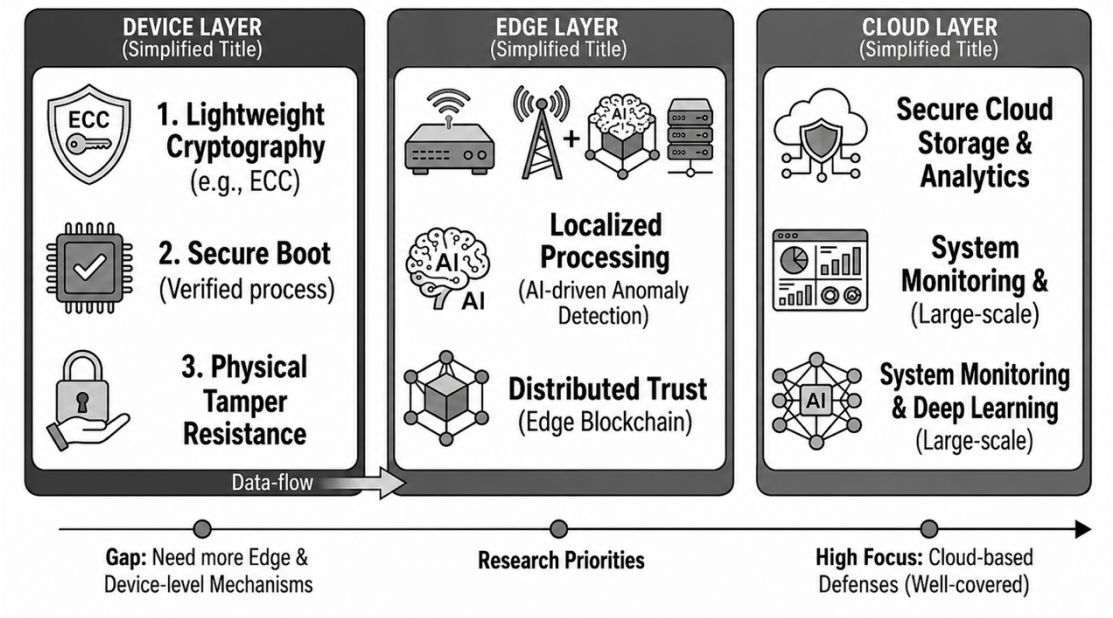

Figure 02. *Unified IoMT Security Resilience Model (guided by policy and regulatory overlay GDPR, HIPAA, Privacy by design)*

Discussion

Technical vulnerabilities are found as a primary security issue in health care IoT systems in the existing literature. Some of the most frequent problems with IoMT devices are weak authentication methods, lack of encryption, the use of outdated wireless communication protocols, out-of-date firmware, and the computational power of the devices themselves (Mejía Granda et al., 2023; Barrett et al., 2023; Selvaraj et al., 2025). These vulnerabilities allow cyberattacks like ransomware attacks, malware injection, distributed denial-of-service (DDoS) attacks and tampering with medical devices, which can severely disrupt healthcare operations and threaten patient safety (Ali et al., 2022; Khan et al., 2025). Recent studies also highlight the emerging use of Artificial Intelligence, Blockchain, and Edge Computing to enhance intrusion detection, data integrity, and secure communication in IoMT systems (Alnaim & Alwakeel, 2023; Kumar et al., 2023; Ksibi et al., 2023). By the way of the interpretation made by the authors, while a few technologies are advanced and can increase technical resilience, there are many candidate solutions that are mostly experimental and are not tested in deployments in the health field. The vast diversity of IoMT devices and their limited resources pose challenges in terms of scalability, interoperability, and maintenance. Future work on lightweight, energy efficient and interoperable security mechanisms to ensure seamless integration into different healthcare IoT architectures, that does not affect clinical performance or system reliability is merited.

The findings from this review can be interpreted through the proposed Unified IoMT Security Resilience Model. The model shows the imbalance of research investments currently carried out in the device, edge, and cloud layers as a result of mapping the existing research works. There is a degree of familiarity with cloud and network-centric security, but relatively little research has been done on lightweight and explainable security mechanisms at the device and edge layers. The imbalance is a volatile scenario especially considering the resource limitations and tight time constraints of medical IoT systems. The study also facilitates the identification of the lack of continuity in the use of AI and blockchain technologies, with many

AI tools used separately from blockchain as part of a disjointed, multi-layered defense approach.

There are many other challenges that are well documented in the literature, especially with regard to device management, system maintenance, and incident response capabilities. Harkai (2024), Alzahrani & Asghar (2024) and Rahim & Chishti (2025) state in several studies that there is a lack of awareness among the healthcare personnel, monitoring infrastructure is weak and there is a lack of integrated approach towards handling cybersecurity issues in the healthcare organizations which increases the operational exposure. Furthermore, as hospitals, clinics and home care settings adopt IoMT devices, the fragmented implementation makes it difficult to securely manage devices and to detect potential threats timely. Considering this, the authors conclude that operational resilience must not be attempted with only technical solutions. To ensure the safety of IoMT devices, coordinated solution and operation strategies are necessary: Continuous system monitoring, regular device patching, cybersecurity training for healthcare workers and establishing an incident response procedure. That it's critical to integrate security measures into clinical practices without disrupting the delivery of patient care or clinical decision making.

Additionally, regulatory and compliance issues are discussed in the reviewed literature, as they are essential for safeguarding patient information in IoT-based healthcare systems, such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR) (Hathaliya & Tanwar, 2020; Krishnamoorthy et al., 2023). Still, a few studies indicate that current rules can't keep up with the evolving technology of IoMT, leading to discrepancies in compliance and enforcement across healthcare institutions (Ali et al., 2025; Rehman et al., 2025). As the authors' films, complying with regulations is always a rule which is security-sustaining instead of a security afterthought. Implementing technical designs and operational practices that meet evolving regulatory requirements can help engender trust, provide legal accountability, and enhance the system-wide resilience. Regulatory models need to take adaptive, technology-centric ways to maintain effective regulation of future healthcare IoT ecosystems.

Table 3

Summary Table of IoMT Security Research Outcomes

Theme	Key Findings	Implications / Recommendations	Research Gaps
Device & Firmware Vulnerabilities	Weak authentication, outdated firmware, insecure default settings	Device hardening, secure provisioning, encryption	Need lightweight security for resource-constrained devices
Multi-layered Defense	Device, network, and cloud layers should work together	Defense-in-depth to prevent single point failures	Real-world deployment studies are limited
AI/ML for Threat Detection	Anomaly detection, predictive monitoring, continuous authentication	Use hybrid models; complement AI with rule-based or explainable methods	Adversarial robustness, interpretability, computational overhead

Theme	Key Findings	Implications / Recommendations	Research Gaps
Blockchain	Tamper-evident, decentralized authentication, auditability	Use selective blockchain solutions (permissioned/hybrid)	Scalability, latency, and energy consumption issues
Privacy-Preserving Techniques	Federated learning, secure multiparty computation	Embed privacy by design, enable collaborative analytics without sharing raw data	Regulatory alignment, practical deployment frameworks
Domain-Specific Applications	Wearables, implantable, metaverse healthcare	Tailor security measures per device/application	Specialized strategies for different domains
Operational & Regulatory Challenges	Incident response, compliance, interoperability	Integrate incident response into clinical workflow	Empirical validation needed, standardization lacking

Conclusion

The research reveals forty-first studies that IoMT systems have created significant enhancements in healthcare, but are faced with several security and privacy issues. The vulnerabilities are at the device, firmware, network, cloud, and application layer, and weak authentication, outdated firmware, and default settings are significant vulnerabilities. Employing multi-layered defense strategies including device hardening, network protections and cloud security will enhance patient protection, reduce single points of failure, and boost resiliency. Despite using great potential for real-time threat detection, predictive monitoring, and adaptive authentication, challenges like interpretability, adversarial resistance, and resource limitations need to be addressed within AI and machine learning contexts. Blockchain solutions offer benefits of tamper-proof auditing and decentralised authentication; however there are scalability, latency and green energy costs issues.

To carry out such defense, the literature ultimately points to four key priority areas: co-ordinated defenses at both the device and network level, combined with privacy and/or resource-efficient defenses; incorporating AI-based anomaly detection with explainable and resource-aware defenses; ensuring that the defenses are both privacy-preserving and data provenance-preserving via the use of blockchain and federated learning; and integrating privacy-by-design defenses to the device and/or application level. They are all the responses to bolster security measures and facilitate regulatory and operational needs in healthcare facilities. Although there has been some progress, there are still gaps that need to be filled that would benefit from more empirical research. They involve the deployment of IoMT solutions in the real world, interoperability of dealing with heterogeneous device systems, lightweight cryptographic techniques, explainable AI for resource-constrained devices, and incorporating incident response mechanisms into clinical workflows. The next steps towards making IoMT systems resilient, practical, and compliant with security concepts involve overcoming these gaps.

One of the main contributions of this study is the Unified IoMT Security Resilience Model that adds together security approaches and create a combined, cross-layer taxonomy. This model not only brings together disparate studies, but also reveals key areas of security threats on the device, edge intelligence, and explainable AI implementation. This offers a

structured reference framework that will facilitate future research and implementation of resilient, compliant IoMT-based systems. While IoMT offers significant opportunities for transformation in healthcare services, realising these benefits in a safe manner requires a multi-layered approach that includes advanced device security, AI-driven monitoring, blockchain-auditing systems, industry-specific security measures, and compliance with regulatory and operational standards. To realize secure and stable IoMT ecosystems, future research is needed around energy-efficient and privacy-enhancing mechanisms, highly accessible and interoperable ecosystems, and interpretable mechanisms validated in the clinical world.

Reference

Almulla, Z., Almajed, H., & Rahman, M. M. H. (2025). A layered security perspective on Internet of Medical Things: Challenges, risks, and technological solutions. *International Journal of Advanced Computer Science and Applications, 16*(5). https://doi.org/10.14569/IJACSA.2025.0160576

Al-Otaibi, S., Ayouni, S., Sarwar, N., et al. (2025). AI-driven security framework for medical sensor networks: Enhancing privacy and trust in smart healthcare systems. *Cluster Computing, 28*, 408. https://doi.org/10.1007/s10586-024-05049-3

Alzahrani, A., & Asghar, M. Z. (2024). *Cyber vulnerabilities detection system in logistics-based IoT data exchange*. *Egyptian Informatics Journal, 25*, Article 100448. https://doi.org/10.1016/j.eij.2024.100448

Alnaim, A. K., & Alwakeel, A. M. (2023). Machine-learning-based IoT–edge computing healthcare solutions. *Electronics, 12*(4), 1027. https://doi.org/10.3390/electronics12041027

Ashraf, E., Areed, N. F., Salem, H., Abdelhay, E. H., & Farouk, A. (2022). Fidchain: Federated intrusion detection system for blockchain-enabled IoT healthcare applications. *Healthcare, 10*(6), 1110. https://doi.org/10.3390/healthcare10061110

Ali, O., et al. (2023). A systematic literature review of artificial intelligence in the healthcare sector: Benefits, challenges, methodologies, and functionalities. *Journal of Innovation & Knowledge, 8*(1), 100333. https://doi.org/10.1016/j.jik.2023.100333

Ali, M. H., et al. (2022). Threat analysis and distributed denial of service (DDoS) attack recognition in the Internet of Things (IoT). *Electronics, 11*(3), 494. https://doi.org/10.3390/electronics11030494

Amiri, Z., Heidari, A., Navimipour, N. J., Esmaeilpour, M., & Yazdani, Y. (2024). The deep learning applications in IoT-based bio- and medical informatics: A systematic literature review. *Neural Computing and Applications, 36*(11), 5757–5797. https://doi.org/10.1007/s00521-023-09366-3

Akram, A., Ismail, M., Hussan, S. T., Arshad, A., Qureshi, S. I., & Iqbal, J. (2025). Securing IoT devices in healthcare: Challenges and solutions. *Spectrum of Engineering Sciences, 3*(5), 133–142. https://sesjournal.org/index.php/1/article/view/341

Alzubi, J. A., Alzubi, O. A., Singh, A., & Ramachandran, M. (2022). Cloud-IIoT-based electronic health record privacy-preserving by CNN and blockchain-enabled federated learning. *IEEE Transactions on Industrial Informatics, 19*(1), 1080–1087. https://doi.org/10.1109/TII.2022.3189170

Ali, T. E., Ali, F. I., Dakić, P., & Zoltan, A. D. (2025). Trends, prospects, challenges, and security in the healthcare internet of things. *Computing, 107*(1), Article 28. https://doi.org/10.1007/s00607-024-01352-4

Babar, M., Tariq, M. U., Qureshi, B., Ullah, Z., Arif, F., & Khan, Z. (2025). An efficient and hybrid deep learning-driven model to enhance security and performance of healthcare Internet of Things. *IEEE Access, 13*, 22931–22945. https://doi.org/10.1109/ACCESS.2025.3536638

Barrett, S., Boswell, B., & Dorai, G. (2023). Exploring the vulnerabilities of IoT devices: A comprehensive analysis of Mirai and Bashlite attack vectors. In *10th International Conference on Internet of Things Systems, Management, and Security* (pp. 125–132). IEEE. https://doi.org/10.1109/IOTSMS59855.2023.10325725

ElSayed, Z., Abdelgawad, A., & Elsayed, N. (2025). Cybersecurity and frequent cyber-attacks on IoT devices in healthcare: Issues and solutions. *arXiv Preprint*. https://doi.org/10.48550/arXiv.2501.11250

Harkai, A. (2024). Main characteristics and cybersecurity vulnerabilities of IoT mobile devices. In *Smart Innovation, Systems and Technologies, 367*, 219–230. https://doi.org/10.1007/978-981-99-6529-8_19

Hathaliya, J. J., & Tanwar, S. (2020). An exhaustive survey on security and privacy issues in Healthcare 4.0. *Computer Communications, 153*, 311–335. https://doi.org/10.1016/j.comcom.2020.02.018

Islam, M. R., Kabir, M. M., Mridha, M. F., Alfarhood, S., Safran, M., & Che, D. (2023). Deep learning-based IoT system for remote monitoring and early detection of health issues in real-time. *Sensors, 23*(11), 5204. https://doi.org/10.3390/s23115204

Coston, I., Plotnizky, E., & Nojoumian, M. (2025). Comprehensive study of IoT vulnerabilities and countermeasures. *Applied Sciences, 15*(6), 3036. https://doi.org/10.3390/app15063036

Kateb, F. (2025). Improved security for IoT-based remote healthcare systems using deep learning with jellyfish search optimizer. *Scientific Reports*. https://doi.org/10.1038/s41598-025-97065-5

Khan, A. A., et al. (2025). A lightweight scalable hybrid authentication framework for IoMT using blockchain and edge computing. *Scientific Reports*. https://doi.org/10.1038/s41598-025-05130-w

Ksibi, A., et al. (2023). Secure and fast emergency road healthcare service based on blockchain technology for smart cities. *Sustainability, 15*(7), 5748. https://doi.org/10.3390/su15075748

Krishnamoorthy, S., Dua, A., & Gupta, S. (2023). Role of emerging technologies in future IoT-driven Healthcare 4.0 technologies: A survey, current challenges and future directions. *Journal of Ambient Intelligence and Humanized Computing, 14*(1), 361–407. https://doi.org/10.1007/s12652-021-03302-w

Kumar, P., Kumar, R., Gupta, G. P., Tripathi, R., Jolfaei, A., & Islam, A. K. M. (2023). A blockchain-orchestrated deep learning approach for secure data transmission in IoT-enabled healthcare system. *Journal of Parallel and Distributed Computing, 172*, 69–83. https://doi.org/10.1016/j.jpdc.2022.10.002

Mejía Granda, C. M., Fernández Alemán, J. L., Carrillo de Gea, J. M., & García Berná, J. A. (2023). Security vulnerabilities in healthcare: An analysis of medical devices and software. *Medical & Biological Engineering & Computing, 62*(1), 257–273. https://doi.org/10.1007/s11517-023-02912-0

Mishra, R. (2025). Current research on Internet of Things (IoT) security protocols. *Computers & Security, 115*, 102557. https://doi.org/10.1016/j.cose.2024.104310

Mao, J., et al. (2023). A health monitoring system based on flexible triboelectric sensors for intelligent medical IoT and its applications in virtual reality. *Nano Energy, 18*, 108984. https://doi.org/10.1016/j.nanoen.2023.108984

Amoo, O. O., Osasona, F., Atadoga, A., Ayinla, B. S., Farayola, O. A., & Abrahams, T. O. (2024). Cybersecurity threats in the age of IoT: A review of protective measures. *International Journal of Scientific Research in Advances, 11*(1), 217. https://doi.org/10.30574/ijsra.2024.11.1.0217

Panahi, O. (2025). Secure IoT for healthcare. *European Journal of Innovative Studies and Sustainability, 1*(1), Article 3. https://doi.org/10.59324/ejiss.2025.1(1).03

Qi, K. (2025). Advancing hospital healthcare: Achieving IoT-based secure health monitoring through multilayer machine learning. *Journal of Big Data, 12*(1), 1. https://doi.org/10.1186/s40537-024-01038-w

Qureshi, S. S. (2025). Enhancing IoT security and healthcare data protection in the metaverse: A dynamic adaptive security mechanism. *Egyptian Informatics Journal, 30*, 100670. https://doi.org/10.1016/j.eij.2025.100670

Nabha, R., Laouiti, A., & Samhat, A. E. (2025). Internet of Things-based healthcare systems: An overview of privacy-preserving mechanisms. *Applied Sciences, 15*(7), 3629. https://doi.org/10.3390/app15073629

Rajkumar, G., Devi, T. G., & Srinivasan, A. (2023). Heart disease prediction using IoT-based framework and improved deep learning approach: Medical application. *Medical*

Engineering & Physics, 111, 103937. https://doi.org/10.1016/j.medengphy.2022.103937

Rani, V. V., Vasavi, G., Paul, P. M., & Rani, K. S. (2025). IoT-based healthcare system using fractional dung beetle optimization-enabled deep learning for breast cancer classification. *Computational Biology and Chemistry, 114*, 108277. https://doi.org/10.1016/j.compbiolchem.2024.108277

Rahim, R., & Chishti, M. A. (2025). IoT security innovations: Recent technologies, threats, and solutions. *SN Computer Science, 6*(1), 593. https://doi.org/10.1007/s42979-025-04106-x

Rehman, A. U., Lu, S., Bin Heyat, M. B., Iqbal, M. S., Parveen, S., Bin Hayat, M. A., Akhtar, F., Ashraf, M. A., Khan, O., Pomary, D., & Sawan, M. (2025). Internet of Things in healthcare research: Trends, innovations, security considerations, challenges and future strategy. *International Journal of Intelligent Systems, 2025*(1), Article 8546245. https://doi.org/10.1155/int/8546245

Rasheed, A. M., & Kumar, R. M. S. (2025). Efficient lightweight cryptographic solutions for enhancing data security in healthcare systems based on IoT. *Frontiers in Computer Science, 7*, 1522184. https://doi.org/10.3389/fcomp.2025.1522184

Singh, N. P., Chaku, S., & Singh, J. (2023). Enhancing healthcare security using IoT-enabled continuous authentication with deep learning. In *Proceedings of the International Conference on Electrical and Electronics Engineering* (pp. 275–289). Springer Nature Singapore.

Selvaraj, M., Uddin, G., & Mazloomzadeh, I. (2025). A large-scale study of IoT security weaknesses and vulnerabilities in the wild. *ACM Transactions on Software Engineering and Methodology, 34*(2), Article 10.1145/3691628. https://doi.org/10.1145/3691628

Sowjanya, Y., Gopalakrishnan, S., & Kumar, R. D. (2025). Elevating IoT healthcare security using ProSRN and ICOM methodologies for effective threat management. *International Journal of Information Technology, 17*(1), 1–14. https://doi.org/10.1007/s41870-024-02395-8

Javaid, U., Siang, A. K., Aman, M. N., & Biplab. (2018). Mitigating IoT device-based DDoS attacks using blockchain. In *Proceedings of the 2018 Workshop on Security in Software Defined Networks & Network Function Virtualization* (pp. 25–30). Association for Computing Machinery. https://doi.org/10.1145/3211933.3211946

Zanbouri, K., Darbandi, M., Nassr, M., Heidari, A., Jafari Navimipour, N., & Yalcın, S. (2024). A GSO-based multi-objective technique for performance optimization of blockchain-based industrial Internet of Things. *International Journal of Communication Systems, 37*(15), e5886. https://doi.org/10.1002/dac.5886