International Journal of Emerging Engineering and Technology (IJEET)
ISSN (e): 2958-3764
Volume: 4, Number: 2, Pages: 88- 96, Year: 2025

Analyze the Critical Factors of Security and Privacy Issues in IoT Domains

Hamza Azeem*, Irshad Ahmed Sumra, Syeda Shan e Zahra , and Malik Adnan

Department of Informatics and Systems, School of Systems and Technology, University of Management and Technology, Lahore, 54000, Pakistan
* Corresponding author: Hamza Azeem (Email: Hamzaazeem024@gmail.com)

Received: 02/02/2025, Revised: 21/04/2025, Accepted: 23/05/2025

***Abstract*—The Internet of Things is all around us, influencing our personal as well as business lives. IoT devices communicate personal data to provide some modern luxuries, raising privacy questions that affect almost every aspect of modern life. This survey will examine the security of IoT, particularly in Smart Homes, Industrial Internet of Things, and Internet of Medical Things, and will propose that solutions to some challenges in one area could be applicable to solving challenges in other areas due to the heterogeneity of IoT. The challenges IoT devices present in terms of privacy and security have a specific relevance in a variety of industries: they could make our households insecure (smart homes), they could disrupt a whole industry (industrial IoT), or they could be physically damaging to us in a medical context (internet of medical things). In general, the rush to put IoT hardware, software, and devices into use is prioritised over consideration of whether they are actually secure. The development of IoT is so fast-paced that it sometimes creates security vulnerabilities, which may in turn compromise personal information or information held by an organisation or business. If IoT is used in a medical context, these vulnerabilities could be detrimental, resulting in injury/physical harm to people who were expecting services, rather than disruptions.**

***Index Terms*—Internet of Things Security, Connected Device Security, Cyber-Physical System Security, Embedded Device Security, Smart Device Security, IoT Protection, IoT Network Security.**

I. INTRODUCTION

The Internet of Things has become deeply integrated into the modern world. Nobody is now away from it, and it is difficult to imagine that someone does not use the IoT for their personal and professional work purposes, and the IoT collects their information. IoT devices are sensors that are connected to or communicate with each other over the internet to provide services to humans or to other devices for further processing [1]. As IoT devices encroach on all aspects of contemporary life, farmers may use a smartwatch to share his Protected Health Information (PHI), tractor using IoT sensor for saving fuels, home using smart tv monitoring activities on his farm. All of the above data were from IoT devices and they need to be sent out for processing. This huge amount of data raises concerns about data privacy during processing. Figure 1 shows the standard research process for this study.

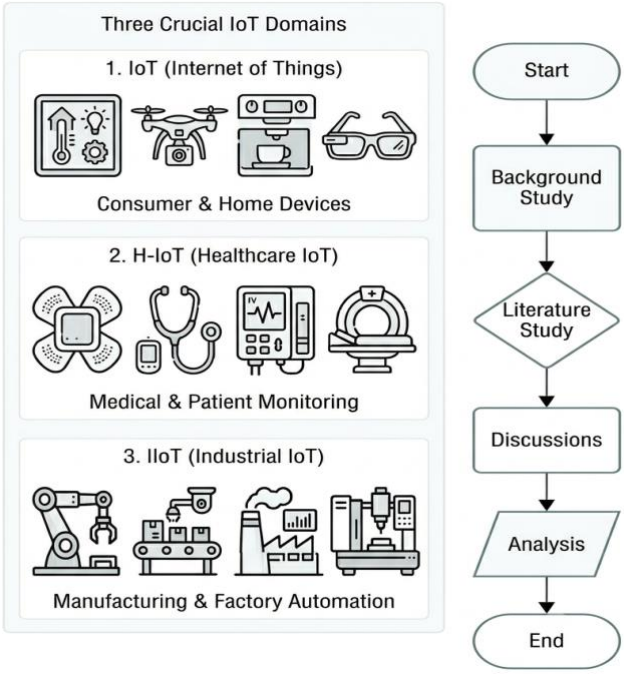

Fig. 1: Visualizing step-by-step research procedure.

This survey has reviewed the literature from IEEE Xplore, Google Scholar, and Scopus, primarily from 2016 to 2024, with a focus on publications after 2019 that depict recent advancements in IoT security. Smart homes, IIoT, and IoMT are important IoT domains to cover in a survey, as they are the most widely adopted Internet of Things applications and present interesting, distinct threat scenarios. Furthermore, the

level of danger and impact posed by a security breach across the three IoT application domains is of varying severity; smart home breaches may lead to breach of personal privacy, breaches in IIoT are more likely to result in disruption of operations, whereas breaches to Internet of Medical Things (IoMT) applications may even put human lives in direct danger. In all cases, we have chosen those that address security or privacy challenges for one or more of the specified types of IoT. In section II, the goal is to further analyze three domains from IoT devices including Smart Homes, the Industrial IoT (IIoT) and IoMT respectively. Each domain has been studied largely with independent research. IoT is heterogeneous, so the solution found for IoMT could move to IIoT. In Section III analysis and discussion, we will cover the common vulnerabilities in IoT Smart Homes, IIoT and IoMT and the level of risk in a high, medium and low format, respectively, for IoT Smart Homes, IIoT, and IoMT. In section IV, possible solutions are discussed to increase IoT security to some extent. In section V, we will conclude the study results.

II. BACKGROUND AND RELATED WORK

A. Privacy in Smart Homes Internet of things

An Analytic Hierarchy Process (AHP), proposed by Allifah and Zualkernan [2], offers consumers an effective way to assess the security risks of smart home devices prior to purchase. Their method assigns a quantifiable risk rating to everyday IoT devices using clear, non-technical language. The effectiveness of this approach was demonstrated through a case study of common household smart products - specifically home theaters, security cameras, smart lights, speakers, video cameras, smart plugs, home control hubs, home security networks, smart WiFi units, doorbell cams, home stereos - using an AHP model. Ironically, several smart home devices designed for security often end up creating vulnerabilities such as loss of private information, compromised personal data and even takeover of control over home devices. By leveraging the AHP rating system, consumers can make more informed decisions to safeguard their privacy when buying smart homes and IoT gadgets.

George et al. [3] emphasize the vast amount of personal data that smart home device users are willingly or unknowingly divulging. IoT devices collect data that advertisers use for targeted marketing campaigns or that companies sell to various entities for legitimate or malicious purposes. At present, there's no accurate way to quantify the exact volume of data that smart home devices collect during usage. According to the research, a proposed solution using a packet tracer aims to gradually counteract the collection of sensitive information by raising public awareness. The developers envision this packet tracer as a tool to provide consumers with a visual representation of the quantity and nature of the data being collected.

Emami-Naeini et al. [4] worked with professionals from NGOs, government agencies, and schools, who were interviewed by the researchers to determine which information from the labels on IoT devices consumers would consider most important when deciding whether to buy certain products. These security and privacy experts agreed that information such as the risk of a privacy violation should be presented on product information labels for consumers. To achieve this goal, the experts divided the risk factors into two levels: primary risks that should be displayed on the packaging and secondary risks that consumers would access via online links or QR codes. The study concluded by highlighting the need for further research on these improved labels (Fig. 2).

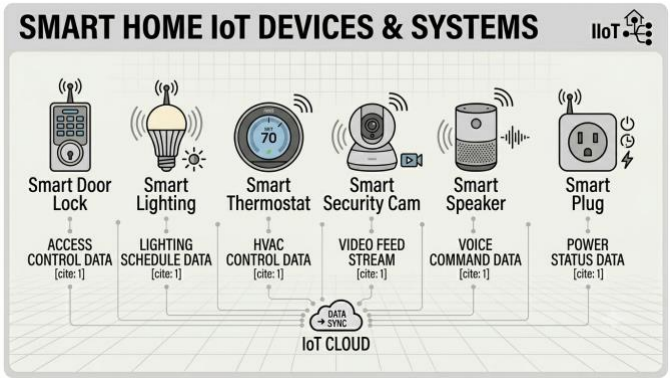

Fig. 2: Illustrates IOT devices helping a home transform into a smart home.

Porambage et al. [5] examined the optimal methodology to ensure an adequate level of privacy for those acquiring smart home products by adopting a privacy-by-design approach. The authors elucidated how average consumers surrender their personal information indiscriminately to manufacturers as they employ their connected household devices, a veritable goldmine of exploitable data for entities like thieves interested in when inhabitants are away at work, at home or at rest to plan the best occasion to invade the house or the myriad other privacy concerns that arise, from access control to data protection, all the way to tracing the collected data on these gadgets. The article highlights Privacy Enhancing Technologies as tools for better user privacy when operating such appliances, illustrating its utility with the example of RFID where privacy enhancements ensure that those unauthorized don't get access to the tag's contents.

While well-reputed companies offer more secure products compared to those made by less common businesses, this fact needs to change. As noted in their extensive review of studies into vulnerability types including 1) physical attacks, 2) attacks over the network, 3) attacks in software and 4) attacks on encryption, "companies widely recognized are held to higher security standards compared to less well - known ones." Ultimately, according to the authors, the market needs to shift

toward ensuring all businesses abide by the same set of rules for their smart home devices. Davis et al. [6] concluded that there is a lack of such security enforcement amongst the lower end market and noted in their findings: "The uncommon vendors weren't as diligent as the well-established companies. There is a need for greater responsibility from both vendors and consumers, which can be addressed by consistent, mandatory cybersecurity regulations and standards for smart home appliances. " The future research should examine the various security risks associated with all kinds of IoT home devices, not only the main brands.

Utomo et al. [7] discussed similar issues: the use of connected IoT devices in a smart home poses significant privacy risks due to the convenience, hardware, and software of these devices. Their suggestions for securing IoT devices include using a strong password and username as the first steps for privacy. Strong authentication and key agreements can then be used as subsequent steps. However, since the technology used in IoT is constantly evolving, there will always be ways for others to access these smart devices and learn everything about us. It's stated that many hackers find ways to access smart devices to hone their hacking skills, making security a never-ending race.

Brahma and Sadhya [8] sought to protect smart home IoT devices by adding additional traffic or by obfuscating traffic to prevent someone from precisely identifying which devices are being used within a smart home. An adversary who identifies the devices present in a smart home may also recognize ways to violate the owner's privacy as well as security. They devised and implemented dynamic traffic shaping to misdirect an attacker attempting to read traffic for identifying the different devices on the compromised network. Artificial packet generation swells traffic, thus making the data flowing through the network harder to read. Testing carried out by the authors indicated that network performance was hindered for the items tested. In situations where numerous smart home devices are deployed, this decrease in throughput might be unacceptable to the owner. Five smart home devices were utilised in the authors' experiments, and the authors advised further testing.

B. Basic concept of the Industrial Internet of Things

Tan and Samsudin [9] described IIoT as an arrangement of various devices or "things" that acquire, exchange, process, and store data pertinent to demanding industrial processes, thereby enabling the maintenance of sensitive, real-time information exchange through M2M interactions. However, this raises concerns about the safety and privacy inherent in the operation of such devices. In an attempt to outline these rising vulnerabilities, a 2010-2021 meta-analysis of IoT/IIoT articles was conducted, identifying major challenges related to advanced persistent threats, heterogeneity, scale, and IoT and IIoT technologies lacking built-in security features. They then provide a comparison, highlighting how these challenges affect conventional IoT differently than IIoT. The current four-layered Internet architecture is also dissected, with emphasis on the physical, network, and application layers, followed by a suggestion for a modified layer configuration: device layer, transport and network layers, processing layer, and application layer. The security requirements of IIoT, addressed with the CIA framework, have also been classified into each layer with corresponding problems and solutions suggested utilizing the framework mentioned previously (Fig. 3).

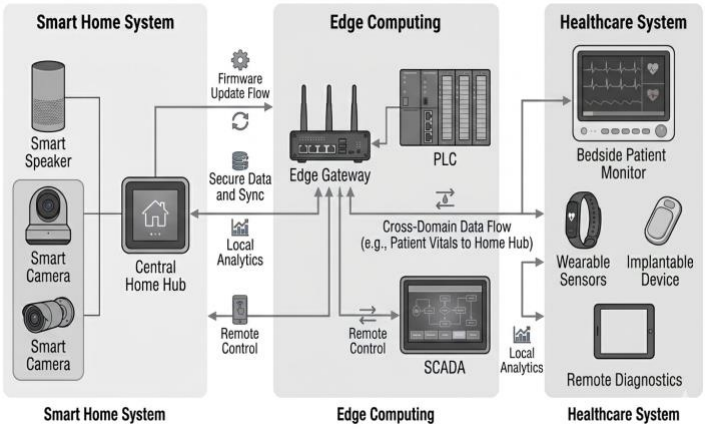

Figure 3: IoT architectural framework highlighting cross-domain integration, edge processing and secure data orchestration among Smart Home, Edge Computing and Healthcare IoT systems.

Cecílio and Souto [10] described the ongoing trend in the industrial internet of things. IIoT spans from transport and management of resources to green energy, manufacturing and smart cities. Some benefits are automation of production, the digitization of factories, the provision of assistance and repair services, instant alerts and reminders and the tracking of the health of industrial workers. The article discusses each layer of IoT: the physical, network, and application layers. In the physical layer, possible attacks include reverse engineering and side-channel attacks. In terms of networks, IIoT networks may be subject to man-in-the-middle and DDoS attacks. Finally, in terms of the application layer, attacks include trojans, viruses, and runtime attacks. The authors said that the technology that'd have the greatest impact would be when data processed by IIoT devices, transmitted or stored on them, is encrypted. The research concluded that the heterogeneous nature of IIoT design leads to broader attack surfaces, meaning that a single flaw can compromise more IIoT devices.

Eyeleko and Feng [11], in contrast to other research efforts focused on the user side, examined privacy issues involving hackers. The research introduces and analyses IIoT at length. According to their study, IIoT is an increasingly adopted model that'll surely grow in use as the industrial sector integrates

artificial intelligence and continues to expand. Their study describes the original three-layered structure of IIoT. Their proposed conceptual model of the typical namespace that'll appear in IIoT is PLC, HMI, MES, ERP, WMS and SCADA. Finally, their research explores real - life occurrences and exploits of IIoT and the research touches on how two major limitations with IIoT can create an attack vector into the network layer, the layer 1 limitation, with or without a compromise of IIoT equipment, however, to compromise the network layer through an attack into IIoT, two compromises would be needed. These two vulnerabilities, in tandem with the already introduced 5 limitations, give an example of how such attacks may be performed, as well as suggesting how it may be countered.

Bugshan et. al. [12] examines the problem about the use of industrial Internet of Things (IIoT) data. This data is collected to reach a decision or control machines. The recent expansion of artificial intelligence (AI) also led AI to become used in analyzing the data collected by IIoT. AI brings huge benefits, especially when analyzing large amounts of data, as it excels in both collecting and interpreting it. Nevertheless, problems arise from how other firms manage this data. In situations where data is provided to external firms to develop a trained AI model for a company, control is entirely lost, potentially resulting in the data spilling to unknown entities. The research proposes using federated learning, as this technique allows models to train locally, keeping the data controlled by the organization.

Tong et al. [13] introduce blockchain's ability to secure data transmission for IIoT devices. This research, named "Data Security Transmission and Privacy Protection Scheme for Industrial IoT", summarises what blockchain is and how it can ensure data integrity. In addition, the research describes four algorithms for identity authentication that allow users to access IIoT devices and data. They also include two other protocols to achieve privacy: a method that masks IIoT device data and a method for decentralized data storage, wherein data is stored across different servers instead of on a single central server.

Li et. Al. [14] provided an overview of the status of IIoT technologies, noting key privacy and security risks. According to this research, the chief privacy concern is the leakage of critical industrial data, leading to a loss of control over it. The research then surveyed existing security approaches to IIoT and introduced a novel light scheme involving four characteristics: enabling users to restrict access to sensitive data, securing data stored in cloud servers, necessitating authorized access for both users and servers and eliminating data storage by discarding redundant data. This light scheme is claimed to be effective at protecting user data from external cloud entities.

Rathee et al. [15] proposed a solution that's suitable for IIoT devices currently being deployed. They say that the "blockchain, mathematics-based methods and encryption technologies" aren't really feasible on resource-constrained IIoT devices. To this end, they propose a hybrid trust system to ensure secure communication among IIoT devices. They've developed and tested a hybrid model that shows its efficiency and power efficiency while maintaining data security (Fig. 4).

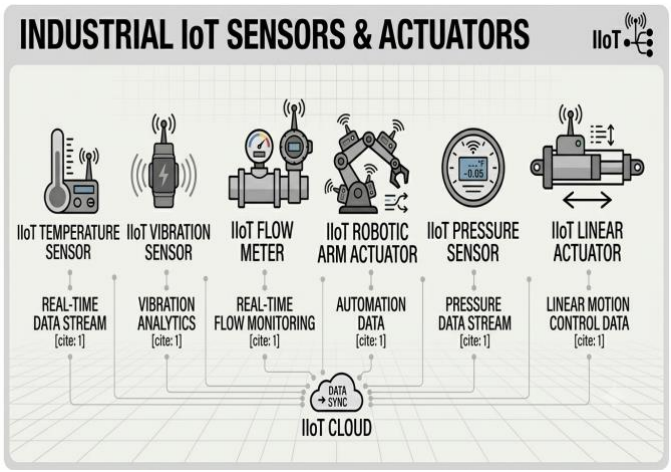

Figure 4. IoT devices used in industries.

Aoued et al. [16] conducted a survey to examine the position of machine learning within IIoT and related privacy and security aspects. It covers four types of artificial intelligence models. This research examined Deep Learning, Federated Learning, Machine Learning, and Deep Reinforcement Learning, and their potential integration to address key security/privacy challenges in IIoT. Privacy abuses, the disclosure of information through unauthorized channels, issues with integrity and authenticity of the data, as well as the loss of trust can lead to different forms of attacks targeting an IIoT network. This research details how to mitigate data loss, reduce the variety of threat vectors IIoT devices face, and finally provides guidance on how ML ought to be implemented to lessen the chances of data disclosure. The authors provide insight into the entire domain of IIoT, offering an extended view of what's coming in technology, as well as the current obstacles IIoT faces and which resolutions might be effective.

C. Privacy in Healthcare Internet of things

Parihar et al. [17] examines the impact of IoT devices in the health tech ecosystem. Medical devices are constantly gathering patient data, such as heart rate and glucose levels, which is crucial for medical staff to make timely decisions for proper care. The study also notes that IoT-connected healthcare systems involve numerous privacy and security risks. Massive volumes of personal health data are transmitted and can fall into the wrong hands, causing identity theft and data breaches. It has

been found that in IoT systems, weak data encryption, insufficient authentication security, and reliance on public networks can easily reveal patients' private information to attackers. To address these issues, researchers propose strengthening device authentication, encrypting data, implementing security measures during data transfer, and real-time monitoring of ongoing threats. A multi-level security approach, comprising cryptographic algorithms and secure cloud storage, can be implemented to fix these security issues. The study recommends various measures, including industry standards, legal regulations, and encryption standards, to uphold the privacy of sensitive patient information and the consistency of its data.

Sun et al. [18] draw attention to the potential security risks of IoMT devices, noting their limited computing and security capabilities and suggesting they're likely to exhibit security weaknesses. These weaknesses might be exploited through unauthorized intrusion, Denial of Service attacks or data exposure that puts personal patient information at risk and could endanger patient well - being if medical devices are compromised. Also noteworthy is the potential for transmitting patient data to cloud servers, which introduces additional exposure risks, as this sensitive health data stored in the cloud, due to weak encryption and access controls, becomes a high-value target for hackers.

Karunaranthne et al. [19] note that the need to secure data transmitted by healthcare-oriented IoT devices has been widely addressed, suggesting a three-layer security framework tailored for smart healthcare scenarios, encompassing device authentication, end-to-end encryption, and dynamic key management to ensure security. Power constraints and limited memory pose challenges to implementing complex security mechanisms on these devices, although the researchers successfully developed and evaluated their proposed architecture across various smart healthcare applications and reported a 40% increase in data confidentiality through layered encryption. Furthermore, they emphasized that emerging techniques such as blockchain technology and machine learning will enhance the security architectures of the Internet of Things as used in healthcare systems.

Chacko and Hayajneh [20] examined vulnerabilities in medical devices within IoT ecosystems, including common threats such as Man-in-the-Middle attacks and malware intrusions, which could jeopardise patient safety and the confidentiality of patient health data. They distinguished among medical devices by rating their vulnerabilities based on potential points of exploitation, such as direct physical access to the device, network access via intrusion methods, and exploitation of firmware weaknesses (Fig. 5).

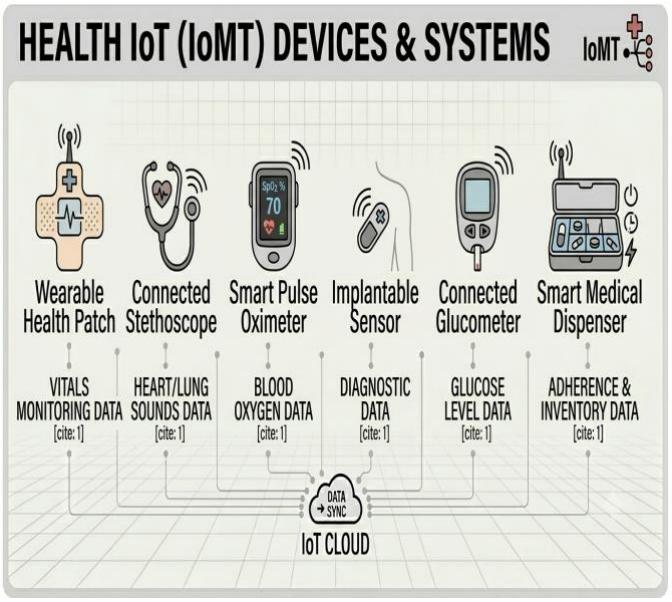

Fig. 5: Illustrates different types of IoT devices used for healthcare monitoring and Management.

They determined that most medical IoT devices offer weak fundamental security measures due to the industry's tendency to prioritize device functionality over security, which provides access for cyber attackers to either take control of device functionality or abuse sensitive patient data. Chacko and Hayajneh advocated for a hardware security architecture involving technologies such as tamper-resistant microcontrollers and secure boot mechanisms, which they believe can effectively address these security risks. Their work emphasized the role of FDA guidelines in ensuring the security of medical devices and advised medical device manufacturers to design their products with security as a core feature.

Obaid and Salman [21] provided a comprehensive overview of existing security threats to IoT-based healthcare, highlighting vulnerabilities in medical devices and proposing several protection strategies. The research delves into significant cybersecurity hazards encountered by IoT healthcare, such as unauthorized data access, interoperability between devices, inadequate data encryption and the resulting risks associated with breaches of sensitive patient information. Additionally, they advocate for blockchain-based solutions to ensure data immutability and produce tamper-resistant records, thereby upholding patient privacy. Based on their findings, the authors argue for the pressing need for standard cybersecurity guidelines given the rapid growth of IoT applications in healthcare. Furthermore, they stress the importance of safeguarding patient data through robust measures such as encryption, multi-factor authentication, and strict compliance with regulations such as GDPR and HIPAA (Table I).

Table I: Analysis of crucial privacy and security issues and their consequences on IoT fields. The table categorizes ten critical security and privacy challenges across Smart Home, IIoT, and IoMT domains, rating their impact level and overall attack severity. Source: Adapted from [25].

Sr #	Critical Issues	Impact on IoT Smart Home	Impact on IIoT	Impact on IoMT	Severity of attacks
1	Weak authentication	High	High	High	Severe
2	Lack of encryption	High	High	High	Severe
3	Side-channel attacks	High	Low	Low	Moderate
4	Network vulnerabilities	High	High	High	Moderate
5	Cloud storage vulnerabilities	High	Moderate	High	Severe
6	Exploitation of Voice assistants	High	Low	Low	Severe
7	Outdated Firmware	Moderate	High	Moderate	Moderate
8	Insufficient data anonymization	Low	High	Moderate	Severe
9	Data over-collection	High	Low	High	Severe
10	Physical security risks	Moderate	Moderate	Moderate	Moderate

(Key: High = Significantly compromise system functionality | Moderate =Noticeable risks leading to cause widespread damage | Low = Minimal risk causing negligible damage | Severe = Causing critical system failures or major breaches)

Assa-Ageyei et al. [22] reviewed IoT applications designed for disabled individuals and explored their privacy and security concerns based on quantitative survey results. Their findings suggest that personal health data are generally insecure due to the inadequate security measures in many Personal Health Record Systems (PHRS). According to the review, IoT devices used for remote patient monitoring (e.g., sensors and wearable devices) are vulnerable to cyberattacks that may lead to personal data breaches. As a result, study [22] suggested that PHRS security should improve the protection of personal health records, safeguarding patient information and maintaining data privacy. They additionally found that 36.4% of those surveyed reported concerns about malicious data falsification and breaches in data confidentiality due to cyber attackers. Privacy protection issues should be reduced by adopting security strategies such as encryption, authentication and anomaly detection. Since IoMT is growing , the review concludes by proposing that healthcare providers carry out a blockchain solution to enhance the security of medical data and use artificial intelligence to detect unauthorized access.

Fazeldehkordi et al. [23] proposed a new classification-based security model to address recent challenges in the security of IoT devices in healthcare. Using pacemakers as an example to conduct experiments, they managed to prove that some of them are prone to various threats such as malware, battery draining and insufficient encryption, which can cause access from unauthorized intruders. According to their studies, external security measures, such as the use of cloud-based encryption protocols, reduce threats more effectively than embedded IoT device solutions. If implemented in healthcare devices, the recommended framework increases security levels by 45% in the devices it tested. Also, the authors indicate that it's necessary to strengthen the security of IoT embedded devices and to build an adaptive security solution.

Azzawi et al. [24] note that IoT is gaining traction in healthcare for managing connectivity and authenticating lightweight, constrained devices. The authors introduced a scheme that uses ECC authentication on top of COAP, ensuring efficient authentication of these low-power devices. The study demonstrated a 30% increase in computing efficiency and lower energy consumption when ECC over CoAP was applied in IoT healthcare environments. This enhanced the security and effectiveness of communication for medical wearables and in remote monitoring frameworks. They suggest that adding a blockchain-based identity system would bolster data integrity security while reducing the probability of tampering with medical IoT data.

III. Analysis and Discussion

Table I highlights the top security and privacy challenges associated with each of the three categories of IoT devices. In all IoT sectors, current hardware is a concern. IoT hardware comprises a single-purpose, often inexpensive microcomputer with less memory, fewer capabilities, more efficient power consumption, and a more limited attack surface for securing than other computational device sectors. Many security weaknesses in IoT systems stem from such limited capabilities.

Another concern is the poor implementation of IoT systems. People routinely ignore basic security steps, such as setting new passwords rather than leaving them at their defaults, and continue to install outdated or end-of-life hardware on their systems. They additionally often don't install IoT firmware updates, leaving them unpatched. Because these security measures are weak, the security of IoT devices is questionable and can lead to privacy breaches and personal data leaks. IoT devices today also don't employ post-quantum encryption protocols [26].

Data leakage is probably everybody's main concern with IoT systems. Several data domains are vulnerable, such as data stored by medical devices, industrial machinery, and wearable sensors. Medical records on IoMT are of greatest concern due to Health Insurance Portability and Accountability Act regulations, but data from Industrial IoT devices can cause major financial losses and reputational damage if leaked. Data stolen from smart homes may lead to robbery or privacy violations for the device owner. Each of these issues has a unique cause. Nevertheless, a single server hosting these databases poses a high risk of data loss. A data breach involving a single data-storing server could lead to the theft of everything on it. Instead, databases could be distributed across multiple machines, thereby reducing the total amount of data lost if the server is breached.

Poor support exists in all three areas examined, albeit in different ways across the papers. Among IIoT concerns is an unwillingness to replace EOL machines due to the costs of new infrastructure. As EOL machines don't get patched anymore due to the prohibitive costs involved with purchasing all new devices and then installing them across the organization, the network continues to be compromised, thus extending the organization's possible lines of attack. A similar situation is present among smart homes, since support is usually for just three to five years. End users, unlike businesses, are hesitant to upgrade to another appliance when the currently installed one still doesn't work properly. This applies, although no further security patches have been released for older devices [27]. IIoT is a largely untrained subject area. The industry organisations for IIoT devices lack sufficient training in maintenance and in using such devices. Educate the end-users and organisations about the life cycle of IIoT devices. IoT devices are supported by their manufacturers for a specified period. So that when they end their support, they know the need for device replacements. There are various transformational benefits gained when an IoT solution is incorporated into hospital infrastructure, including real-time patient monitoring, enhanced healthcare services, and interactive medical decision-making processes. Devices high up the risk ladder, such as high-risk medical machines, can't maintain good security due to weak onboard safety mechanisms and the challenges of upgrading their onboard hardware or firmware [19]. The inadequate security mechanisms, such as poor encryption and insufficient security protocols, pose significant risks to critical healthcare systems, leaving medical devices vulnerable to intrusions that could compromise patient safety and data integrity [20]. There's a wide range of standards adopted by multiple IIoT devices, which contribute to poor data protection and compatibility issues.

IV. SOLUTIONS

As the adoption of the IoT continues to grow rapidly across healthcare, industry, and personal use, the need for advanced technological solutions becomes apparent to maintain the data integrity, confidentiality, and accessibility standards that have become crucial. By implementing advanced security protocols like multi - layered security frameworks, sophisticated data encryption methods and robust privacy - preserving techniques in conjunction with standardized security policies across platforms, developers can enhance the safety and privacy of data managed by smart healthcare devices. The integration of machine learning (ML) and deep learning (DL) into security solutions for Internet of Medical Things (IoMT) devices, Internet of Industrial Things (IIoT) systems, and third-party data providers for smart home devices represents a transformative potential. These advanced technologies are being explored and applied for their ability to reduce data breaches and proactively ward off security threats. However, deploying ML/DL solutions requires extreme vigilance, as poorly secured models themselves could become vectors for data leaks. Current research on the application of ML/DL in IoT security is still in its early stages and requires further investigation. Table II details several key technologies and outlines their effects on IoMT, IIoT and smart homes.

Table II: Recommended Important technologies, including their proportional impact for securing and protecting three IoT domains
Source: Adapted from [25].

Sr#	Technologies	Proportional Impact
1	End to end encryption Techniques	Reducing risks by 60-80%
2	Multi-factor authentication (MFA)	Minimize unauthorized access by 75%
3	Privacy-centric data policies	Reducing misuse of data by 40%
4	Standardized security labels	Increases consumer trust while taking
5	AI-driven threat detection	Enhancing real-time threat detection by 85%
6	Blockchain technology	Ensuring data integrity and minimizing data tampering risks
7	Traffic Obfuscation Techniques	Minimize traffic analysis attacks keeping the success rates below 10%
8	Compliance with privacy regulations	Reducing legal vulnerabilities by up to 70%
9	Automated firmware update	Reducing firmware-based exploitation by 50%

(Note: Proportional impact values are approximate estimates derived from the cited literature and are intended for comparative illustration purposes only.)

V. CONCLUSION

This paper summarizes the findings from conducting a comprehensive review of research papers about the privacy and security of IoT devices across three distinct sectors: smart

homes, industrial IoT (IIoT) and medical IoT (IoMT). The common issues plaguing each domain are identified and elaborated upon, revealing that despite the substantial differences separating them, the three domains share fundamentally similar vulnerabilities. Privacy concerns are paramount in all three sectors. The review of research papers indicated that elementary security protocols standard across other industries aren't universally implemented within the IoT ecosystem, thereby jeopardizing both the integrity and confidentiality of the data collected and processed. Upon thoroughly examining the current research literature, it became evident that several security measures, including but not limited to encryption, threat detection systems powered by artificial intelligence (AI), distributed data, and blockchain technology, hold the potential to enhance the confidentiality and integrity of IoT devices. When technical controls are combined with widespread user education on the security implications of IoT devices, a more secure landscape can be forged. In conclusion, the development and adoption of a global standard are indispensable for all industries to effectively safeguard end-user privacy and security.

Funding Statement

The authors received no specific funding for this study.

Conflicts of Interest

The authors declare no conflicts of interest to report regarding the present study.

Author Contributions

All authors contributed to the conception, literature review, drafting, and critical revision of this manuscript and approved the final version for submission.

Data Availability Statement

Data is available on reasonable request.

Institutional Review Board Statement

Not applicable.

Informed Consent Statement

Not applicable.

References

[1] K. M. Sadique, R. Rahmani, and P. Johannesson, "Towards security on internet of things: Applications and challenges in technology," Procedia Computer Science, vol. 141, pp. 199–206, 2018

[2] N. M. Allifah and I. A. Zualkernan, "Ranking security of iot-based smart home consumer devices," IEEE ACCESS, vol. 10, pp. 18 352–18 369, 2022.

[3] C. G. George, D. R. Tyranski, D. P. Simons, J. D. O'Quinn, E. R. York, and A. A. Salman, "Integrating social and technical solutions to address privacy in smart homes," in 2020 Systems and Information Engineering Design Symposium (SIEDS). IEEE, 2020, pp. 1–6.

[4] P. Emami-Naeini, Y. Agarwal, L. Faith Cranor, and H. Hibshi, "Ask the experts: What should be on an iot privacy and security label?" in 2020 IEEE Symposium on Security and Privacy (SP), 2020, pp. 447–464.

[5] P. Porambage, M. Ylianttila, C. Schmitt, P. Kumar, A. Gurtov, and A. V. Vasilakos, "The quest for privacy in the internet of things," IEEE Cloud Computing, vol. 3, no. 2, pp. 36–45, 2016

[6] B. D. Davis, J. C. Mason, and M. Anwar, "Vulnerability studies and security postures of iot devices: A smart home case study," IEEE Internet of Things Journal, vol. 7, no. 10, pp. 10 102–10 110, 2020.

[7] I. S. Utomo, C. M. Pranoto, Daniel, J. V. Moniaga, and B. A. Jabar, "A systematic literature review of privacy, security, and challenges on applying iot to create smart homes," in 2022 International Conference on Electrical and Information Technology (IEIT), 2022, pp. 154–159.

[8] J. Brahma and D. Sadhya, "Preserving contextual privacy for smart home iot devices with dynamic traffic shaping," IEEE Internet of Things Journal, vol. 9, no. 13, pp. 11 434–11 441, 2022.

[9] S. F. Tan and A. Samsudin, "Recent technologies, security countermeasures and ongoing challenges of industrial internet of things (iiot): A survey," Sensors, vol. 21, no. 19, p. 6647, 2021.

[10] J. Cec´ılio and A. Souto, "Security issues in industrial internet-of-things: Threats, attacks and solutions," in 2024 IEEE International Workshop on Metrology for Industry 4.0 & IoT (MetroInd4. 0 & IoT). IEEE, 2024, pp. 458–463.

[11] A. H. Eyeleko and T. Feng, "A critical overview of industrial internet of things security and privacy issues using a layer-based hacking scenario," IEEE Internet of Things Journal, 2023.

[12] N. Bugshan, I. Khalil, M. S. Rahman, M. Atiquzzaman, X. Yi, and S. Badsha, "Toward trustworthy and privacy-preserving federated deep learning service framework for industrial internet of things," IEEE Transactions on Industrial Informatics, vol. 19, no. 2, pp. 1535–1547, 2022.

[13] W. Tong, L. Yang, Z. Li, J. Zhao, F. Pan, and L. Tan, "Data security transmission and privacy protection scheme for industrial internet of things," in 2024 Second International Conference on Cyber-Energy Systems and Intelligent Energy (ICCSIE). IEEE, 2024, pp. 1–6.

[14] S. Li, S. Zhao, G. Min, L. Qi, and G. Liu, "Lightweight privacy-preserving scheme using homomorphic encryption in the industrial internet of things," IEEE Internet of Things Journal, vol. 9, no. 16, pp. 14 542– 14 550, 2021.

[15] G. Rathee, R. Iqbal, C. A. Kerrache, and H. Song, "Trustnextgen: Security aspects of trustworthy next generation industrial internet of things (iiot)," IEEE Internet of Things Journal, 2024.

[16] O. Aouedi, T.-H. Vu, A. Sacco, D. C. Nguyen, K. Piamrat, G. Marchetto, and Q.-V. Pham, "A survey on intelligent internet of things: Applications, security, privacy, and future directions," IEEE Communications Surveys & Tutorials, 2024

[17] A. Parihar, J. B. Prajapati, B. G. Prajapati, B. Trambadiya, A. Thakkar, and P. Engineer, "Role of iot in healthcare: Applications, security & privacy concerns," Intelligent Pharmacy, 2024.

[18] Y. Sun, F. P.-W. Lo, and B. Lo, "Security and privacy for the internet of medical things enabled healthcare systems: A survey," IEEE Access, vol. 7, pp. 183 339–183 355, 2019.

[19] S. M. Karunarathne, N. Saxena, and M. K. Khan, "Security and privacy in iot smart healthcare," IEEE Internet Computing, vol. 25, no. 4, pp. 37–48, 2021.

[20] A. Chacko and T. Hayajneh, "Security and privacy issues with iot in healthcare," EAI Endorsed Transactions on Pervasive Health and Technology, vol. 4, p. 155079, 2018.

[21] O. Ibrahim Obaid and S. Salman, "Security and privacy in iot-based healthcare systems: A review," 2023.

[22] K. Assa-Agyei, F. Olajide, and A. Lotfi, "Security and privacy issues in iot healthcare application for disabled users in developing economies," Journal of Internet Technology and Secured Transactions, vol. 10, pp. 770–779, 03 2022.

[23] E. Fazeldehkordi, O. Owe, and J. Noll, "Security and privacy in iot systems: A case study of healthcare products," in 2019 13th International Symposium on Medical Information and Communication Technology (ISMICT), 2019, pp. 1–8.

[24] M. Azzawi, R. Hassan, and K. A. Abu Bakar, "A review on internet of things (iot) in healthcare," International Journal of Applied Engineering Research, vol. 11, pp. 10 216–10 221, 11 2016.

[25] J. K. Das, D. Herwig, J. Fowler, and L. Chen, "Scrutinizing the security and privacy issues of IoT: Analyzing the critical factors on smart home, industrial IoT and healthcare domains," in 2025 IEEE International Workshop on Radio Frequency and Antenna Technologies (iWRF&AT). IEEE, 2025, pp. 533–538, doi: 10.1109/iWRFAT65352.2025.11102956.

[26] Sumra, I.A., Hasbullah, H., Ab Manan, J.-L.: Effects of attackers and attacks on availability requirement in vehicular network: a survey. In: International Conference on Computer and Information Sciences (ICCOINS2014), Malaysia, 3–5 June 2014.

[27] Sumra, I.A., Hasbullah, H.B., AbManan, Jl.B. (2015). Attacks on Security Goals (Confidentiality, Integrity, Availability) in VANET: A Survey. In: Laouiti, A., Qayyum, A., Mohamad Saad, M. (eds) Vehicular Ad-hoc Networks for Smart Cities. Advances in Intelligent Systems and Computing, vol 306. Springer.