Engineering and Technology Journal for Research and Innovation (ETJRI)
ISSN 2581-8678, Vol. VII, Issue I, Jan 2025

A Review on Exploring Security Vulnerabilities and Mitigation Strategies in Internet of Things (IoT) devices

Abishek Niroula[1], Gyalgen Lepcha[2], Dhiraj Prasad Jaiswal[3], Rahul Shah[4]
[1,2,3,4] *School of Information Technology, The ICFAI University, Sikkim, Gangtok, India.*
[1]*abishekniroula0523@gmail.com;* [2]*gyalgen22@gmail.com;* [3]*dhiraj.jaiswal@iuskiim.edu.in*
[4]*rahul.shah@iusikkim.edu.in;*

***Abstract*— The Integration of Internet of Things (IoT) into Society is ahead of its time. As the IoT landscape expands, maintaining the Safety and Security of interconnected devices becomes most crucial. This rapid progress threatens security issues that call for urgent remedies to secure the IoT ecosystems. This paper explores the greater challenges posed to IoT systems such as obsolete practices and user education on safety measures. It delves into fundamental concepts like designing a secure model, using strong encryption methods and authentication systems. Methods such as IOT integrated blockchain technology, consist of blockchain contribution in futuristic IoT hardware, allowing them to be more resistant to cyber threats. Using the same tools as hackers, but this time to prevent the security problem of IoT devices and getting thoroughly tested first to see if it works should be a top priority. In essence, this paper delves into proactive strategies for fortifying IoT devices as well as looking for future advancements to further enhance IoT Security.**

***Keywords*— Internet of Things (IoT), Cybersecurity, Interconnected devices, Blockchain, IoT Security.**

I. INTRODUCTION

Whether it's in our homes or industries, IoT devices have felicitated a new level of ease and effectiveness. However, this fast growth has also revealed some serious security worries that need to be dealt with to keep IoT networks safe and reliable. One of the foremost challenges facing the IoT landscape revolves around security vulnerabilities inherent in interconnected devices. Notably, the swift growth of IoT devices has intensified the risk of cyber threats, particularly in critical domains such as food traceability systems (FTS), where data integrity is paramount. This necessitates innovative solutions to fortify security at the fundamental hardware level. Enter Blockchain-IoT Sensor (BIoTS), a pioneering approach aimed at enhancing security by imbuing IoT devices with blockchain functionalities. By leveraging blockchain technology, BIoTseek to mitigate vulnerabilities and safeguard data integrity, particularly in contexts critical to public safety and quality assurance, such as food safety. Moreover, comprehensive examinations of IoT procedures and user awareness are imperative to address the intricate nexus of security challenges inherent in IoT ecosystems. From uncovering vulnerabilities in popular IoT protocols to recommending robust mitigation measures, a multi-faceted approach is essential to fortify IoT infrastructure and ensure user privacy and safety. The absolute diversity of IoT devices, combined with their resource-constrained nature, presents a complex landscape for implementing standardized security protocols. From insecure communication channels to inadequate authentication mechanisms, the array of vulnerabilities demands proactive measures encompassing both hardware and software considerations. To this end, secure boot mechanisms, encrypted communication protocols, and robust authentication methods are integral components of a comprehensive security framework. Regular software updates and intrusion detection systems further bolster defense mechanisms against evolving cyber threats. Furthermore, Cooperation among key stakeholders, such as manufacturers, policymakers, and cybersecurity professionals, is crucial for developing industry standards and regulatory frameworks that enhance security while fostering innovation. By fostering a collaborative ecosystem focused on proactive security measures, the IoT landscape can realize its transformative potential while mitigating risks posed by malicious actors.

*Corresponding Author: - abishekniroula0523@gmail.com

The integration of the IoT into various facets of contemporary life marks a paradigm shift in connectivity and innovation, permeating diverse sectors with unprecedented levels of interconnectedness and functionality. The widespread adoption of IoT devices, spanning from smart homes to industrial automation, has revolutionized convenience and efficiency. However, this rapid growth has also exposed critical security challenges that must be tackled to safeguard the integrity and reliability of IoT ecosystems. The Architecture of IoT in Consumer level is shown in Fig. 1.

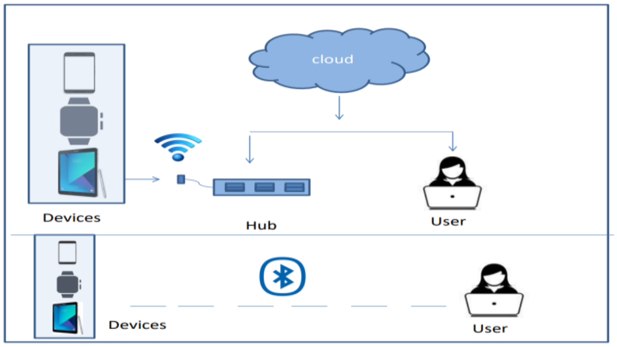

Fig. 1. IoT Architecture at the Consumer Level

From uncovering vulnerabilities in popular IoT protocols to recommending robust mitigation measures, a multi-faceted approach is essential to fortify IoT infrastructure and ensure user privacy and safety. In essence, this paper delves into the intricate landscape of IoT security, highlighting specific vulnerabilities and proposing comprehensive mitigation strategies to foster a safer and more resilient IoT ecosystem. [9] By addressing security concerns proactively, we can harness the full potential of IoT technology while safeguarding against emerging threats, thereby ensuring a future of interconnectedness and innovation built on a foundation of trust and resilience. As the IoT continues to proliferate and evolve, its integration into various domains of contemporary life has fundamentally transformed the way we interact with technology. The interconnectedness of IoT devices has ushered in a new era of convenience, efficiency, and automation, revolutionizing industries ranging from healthcare to manufacturing. However, alongside the myriad benefits of this interconnected ecosystem, there exists a pressing need to address the significant security challenges that accompany it. Security vulnerabilities inherent in interconnected IoT devices represent one of the foremost challenges facing the IoT landscape. The exponential growth of IoT devices has expanded the attack surface for cyber threats, posing risks to critical systems such as healthcare infrastructure and industrial control systems. These vulnerabilities highlight the importance of implementing robust security measures to safeguard data integrity and protect against malicious actors. One innovative approach to enhancing IoT security is the integration of blockchain technology, leading to the emergence of Blockchain-IoT Sensor (BIoTS) systems. By leveraging the decentralized and immutable nature of blockchain, BIoTS aim to mitigate security vulnerabilities and ensure the integrity of data transmitted by IoT devices. This approach has particular relevance in sectors such as food traceability, where maintaining the integrity of supply chain data is crucial for ensuring food safety and quality assurance. Furthermore, comprehensive assessments of IoT procedures and user awareness are essential to address the complex nexus of security challenges inherent in IoT ecosystems. Vulnerability assessments can help identify weaknesses in IoT protocols and recommend robust mitigation strategies to fortify infrastructure against potential threats. Additionally, raising awareness among users about the importance of cybersecurity hygiene can help mitigate risks associated with human error and social engineering attacks. The diversity of IoT devices, coupled with their resource-constrained nature, poses unique challenges for implementing standardized security protocols. Insecure communication channels, inadequate authentication mechanisms, and insufficient encryption protocols are among the common vulnerabilities that must be addressed to bolster IoT security. Secure boot mechanisms, encrypted communication protocols, and robust authentication methods are integral components of a comprehensive security framework designed to protect IoT devices from cyber threats. Regular software updates and intrusion detection systems are essential for maintaining the security posture of IoT devices and detecting anomalous behaviour indicative of potential security breaches. The Architecture of IoT at the Industry level is shown in Fig. 2. In conclusion, this paper emphasizes the importance of addressing security concerns proactively to harness the full potential of IoT technology while ensuring a future of interconnectedness and innovation built on a foundation of trust and resilience.

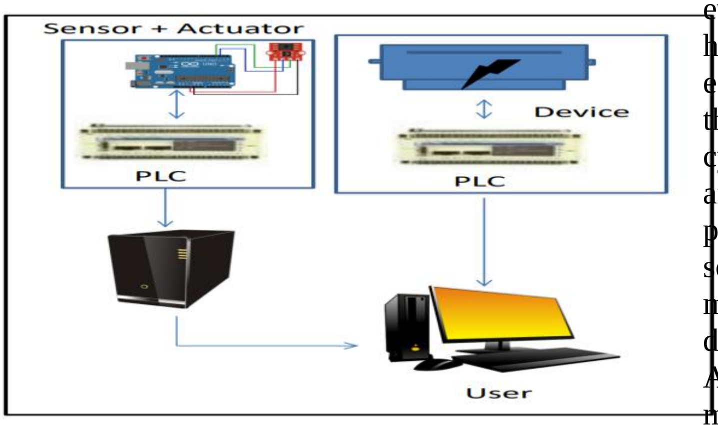

Fig. 2. IoT Architecture at the Industry Level

The integration of the IoT into various aspects of modern life represents a significant change in how things are connected and innovated. It spreads across different areas, bringing high levels of connectivity and functionality. From smart homes to industrial automation, the widespread use of IoT devices has brought about a new level of convenience and effectiveness. However, this rapid growth also reveals serious security issues that need attention to protect the integrity and safety of IoT systems. The fast expansion of IoT devices has increased the risk of cyber threats, especially in critical area like food traceability systems, where the accuracy of data is crucial. This requires new solutions to strengthen security starting from the basic hardware level.

II. Review Of Literature

[1] IoT devices has brought many security risks alongside convenience. This article provides a bold overview of the current state of IoT security issues and their potential impact on user privacy and safety. It explores existing research on how vulnerabilities are identified, addressed, and managed, highlighting successes and areas needing urgent improvement in this domain. By conducting a comprehensive assessment, the article pinpoints the challenges and opportunities for enhancing IoT security. Furthermore, it proposes a firm shift in focus towards securing individual IoT devices and refining the categorization of security measures.

[2] The widespread adoption of IoT devices has led to a surge in cyber threats targeting IoT networks. With the increased integration into everyday life across sectors like education, healthcare, and business, these devices have become essential components of modern technology, therefore, it's imperative to prioritize robust cybersecurity measures. Safeguarding sensitive data and ensuring the security of IoT systems are paramount in light of the increasing frequency and sophistication of attacks. Comprehensive security measures are essential to protect both physical devices and intangible assets like services and data. Addressing IoT security challenges is crucial for maximizing the benefits of IoT technology while effectively mitigating evolving cyber risks.

[3] IoT connects diverse devices to the internet for data exchange, yet faces significant security challenges due to device diversity. A novel solution involves a comprehensive security testing framework tailored for IoT devices. This framework, employing standard and advanced techniques including machine learning, effectively identifies vulnerabilities and compromised devices. Its adaptability accommodates various IoT devices lacking standardized security protocols, offering a flexible architecture for thorough testing. This initiative marks progress in addressing IoT security risks, ensuring devices are safe for widespread adoption in business and academic domains.

[4] IoT has revolutionized device connectivity, yet its increased integration poses significant security challenges. Vulnerabilities exist in device systems, wireless communication, and device software, leading to costly cyber-attacks, especially in healthcare. With approximately 8.4 billion connected devices in 2017 across various industries, IoT has become ubiquitous, enhancing productivity but also increasing cyber risks. Cybercriminals

exploit IoT weaknesses, targeting networks for financial gain or to compromise operations. Despite security efforts, evolving threats make it difficult to ensure IoT network security, particularly for mobile devices. Manufacturers must prioritize security to prevent cyber-attacks from exploiting IoT vulnerabilities, especially in critical sectors like healthcare where patient safety is at stake.

[5] The IoT has transformed our interaction with everyday objects through Internet connectivity, yet its widespread adoption faces significant security challenges. This article explores the critical issue of IoT security, highlighting risks such as unsafe software, data breaches, identity theft, and service disruption from cyber-attacks. To address these risks, a robust security plan is essential, encompassing physical access control, secure remote access, and data protection. The study analyses past attacks and recommends preventive measures, emphasizing preparedness and the use of intelligent programs to predict and prevent potential issues. With the global number of IoT devices reaching 21 billion by 2020, urgent action is needed to address security concerns, underscored by major attacks like Stuxnet and Mirai botnet. Key challenges include the autonomous nature of IoT devices, susceptibility to wireless network attacks, and difficulty in securing devices with limited resources.

[6] The growing utilization of IoT applications brings about heightened security threats, necessitating effective risk reduction measures. Traditional security evaluation methods, often reliant on expert assessments, prove insufficient. To address this, a proposed automated system utilizes machine learning and natural language processing to analyse vulnerability descriptions and predict their severity. This system employs a graphical security model comprising attack graphs and trees, automating the assessment process by identifying potential attack paths in IoT networks. Testing on a smart building system model demonstrates over 90% accuracy in predicting vulnerability severity and identifying vulnerable attack paths. These findings aid cybersecurity experts in promptly mitigating risks, particularly in scenarios where vital vulnerability-related information may be absent, thus addressing the challenge of automating security assessments at the network level.

[7] This paper talks about how healthcare IoT devices highly rely on smart sensing devices and are becoming more vulnerable to cyber threats like data breaches and unauthorized access. It explains the basics of healthcare IoT and the challenges it faces in terms of privacy and security, especially with machine learning and smart sensors. The paper suggests keeping a close eye on different layers of healthcare IoT and using advanced authentication methods like machine learning to protect them. It also suggests ways to make healthcare IoT systems more resilient against cyber threats. Additionally, it highlights general security challenges for IoT devices and stresses the importance of addressing these issues early on. Overall, it aims to help researchers understand the main problems in IoT security and how to deal with threats from various sources.

[8] This paper discusses how the IoT is becoming a reality changing lives and connecting everyday devices to exchange data and provide services. However, it also faces security issues that could affect its growth and users' interests. The paper examines the definition, protocols, architecture, and security of IoT, using a case study to demonstrate the importance of security across all IoT layers. Additionally, it presents the results of a security audit on an IoT platform and suggests solutions and future research directions to improve IoT security. In the future, the paper aims to explore access control in IoT environments to enhance security as well as solutions further.

[9] This paper inquiries into the IoT, which connects physical objects from different areas like home automation, industry, health, and environmental monitoring. However, the sheer number of connected devices and the way they're interconnected pose major security challenges. The research aims to tackle these issues by suggesting ways to improve cybersecurity. It points out that manufacturers and service providers haven't put enough effort into securing IoT devices, leading to security breaches. The paper also looks at various types of attacks on IoT systems and suggests a plan to make IoT deployments more secure, involving everyone concerned.

[10] This paper highlights the increasing importance of security in IoT applications, particularly after recent DDoS attacks exploiting IoT vulnerabilities. It presents a Software-Defined IoT (SD-IoT) framework for secure device management, featuring controllers, switches, gateways, and devices. An algorithm for detecting and mitigating DDoS attacks using cosine similarity analysis is proposed, showing promising results in enhancing IoT security. The paper also addresses broader IoT security challenges such as confidentiality, privacy, and trust, stressing the need for collaborative efforts to develop better security mechanisms and standards. It aims to provide insights for researchers into major IoT security issues and threats posed by intruders.

[11] Blockchain technology offers a transformative solution for enhancing security in IoT environments by safeguarding sensor data, authenticating devices, and enabling secure data transmission. Its decentralized nature eliminates single points of failure, improving reliability and reducing costs. Blockchain enables direct device addressability, scalability, and transparent ownership tracking, while its immutable ledger enhances device management, fosters accountability, and fortifies data integrity against unauthorized access. Embracing Blockchain in IoT deployments represents a strategic investment in future-proofing against cybersecurity threats, ensuring trust, efficiency, and long-term viability in interconnected systems.

[12] As the IoT expands, ensuring the security of connected devices becomes crucial. This paper addresses key challenges and solutions for securing IoT devices, examining various communication protocols like LoRaWAN and 6LoWPAN and highlighting their vulnerabilities. For instance, LoRaWAN's encryption key can be easily compromised, and 6LoWPAN requires better user authentication. Additionally, BLE and Zigbee face security issues, such as easily broken BLE connections. Securing these devices is essential to safeguard people and their belongings from potential harm.

[13] The rapid growth of IoT devices brings promising benefits but also significant security challenges due to limited resources and weak security measures. This survey highlights the urgent need to address IoT security vulnerabilities through Internet-scale solutions and tailored measures. It emphasizes research directions such as identifying and mitigating IoT-specific attacks, integrating security into firmware development, and enhancing detection and response strategies against malicious IoT activity. [14] IoT software platforms facilitate data and service exchange among networked devices, requiring robust security measures. These include ensuring data integrity, secure storage, device identification, and user authorization. Platforms can be closed-source, integrating IoT and cloud computing, or open-source, allowing code customization. Emerging security solutions involve AI and ML for threat detection and Blockchain for data encryption and secure updates. Customized security measures like encryption and authentication protocols address specific threats faced by various IoT devices. Hardware security solutions, especially lightweight cryptographic implementations, offer superior performance and security compared to software-based approaches, crucial for resource-constrained IoT devices.

[15] The paper delves into the pervasive presence of IoT in society, highlighting its susceptibility to malicious actors due to a vast attack surface and lack of standardized protocols. It provides an introductory overview of IoT, discussing layer models, topologies, and protocols, while emphasizing the significant security challenges posed by resource constraints and the absence of standards. The paper outlines various IoT vulnerabilities and proposes specific countermeasures, including the use of protocols like DTLS and IPSec/IKEv2, secure routing protocols like SIGF, object-based security for application data, and IoT-specific intrusion detection systems such as SVELTE. It underscores the pressing need for standardized protocols, channel-based security solutions, and enhanced legislative directives to ensure high-security standards in IoT deployments, given the exponential growth of IoT devices and their critical role in diverse domains.

[16] This research paper explores the complexities of IoT device security by identifying potential threats and proposing effective mitigation strategies. Through an extensive literature review, it

examines prevalent security vulnerabilities and evaluates existing protective measures. Key concerns such as unauthorized access, weak encryption, authentication flaws, physical security risks, and privacy issues are critically analyzed. The proposed mitigation approaches include technological solutions, regulatory frameworks, and user awareness initiatives to ensure a comprehensive security strategy. The study concludes with recommendations for future research, emphasizing interdisciplinary collaboration, adaptive threat modeling, privacy-enhancing technologies, standardization, certification, and the integration of blockchain for enhanced security. Emphasizing the pivotal roles of manufacturers, policymakers, and users, the research envisions a secure and connected future, shaping a resilient IoT landscape. [17] The analysis explores vulnerabilities associated with UPnP-enabled IoT devices, focusing on the Universal Plug and Play (UPnP) protocol and its implementation. It likely examines security risks, potential attack vectors, and strategies for mitigation in UPnP-enabled IoT deployments. Additionally, the study may discuss unspecified vulnerabilities in cybersecurity, identify weaknesses, and propose mitigation strategies. Another exploration may focus on cybersecurity risks in automotive systems, identifying weaknesses in network architecture, protocols, software, and hardware infrastructure. It aims to provide insights into potential threats and suggest measures to enhance security in automotive systems.

[18] The study provides an overview of previous surveys on IoT threats, attacks, and countermeasures, addressing classification approaches and highlighting existing studies' limitations. It poses questions regarding securing IoT devices in new environments and protecting them from compromised devices. Proposed security measures focus on the device life cycle, emphasizing a comprehensive approach from network entry to decommissioning. Hardware-based approaches for defending against physical and cyber threats are discussed, including Hardware trojan detection, Design for Trust (DFT), split manufacturing, and others. Additionally, mitigation techniques against side-channel and fault injection attacks, along with hardware-assisted malware detection, are explored. While offering significant benefits, hardware protection may entail increased costs and overhead, suitable for applications where these factors are justified.

[19] The discussion delves into various facets of the IoT and its security considerations. IoT encompasses layer models, topologies, and protocols. Layer models include variations like the three-layer model and Cisco's seven-layer model, organizing functions differently. Topologies can be point-to-point, star, or mesh, with mesh being favoured for its decentralization. Protocols like 6LoWPAN, CoAP, and MQTT are prominent in IoT, but fragmentation poses challenges. Security in IoT involves vulnerabilities and attacks such as sinkhole, Sybil, and conventional network attacks like eavesdropping and DoS. RFID-specific attacks exploit weaknesses in IoT RFID protocols. Mitigations involve employing secure protocols, intrusion detection systems, and legislative measures to enforce security standards. Future research should focus on lightweight cryptography, improved intrusion detection, and addressing device mobility issues to bolster IoT security against evolving threats.

[20] The research on IoT security underscores the need for a comprehensive classification of security challenges across all layers of IoT systems. It introduces a unique classification of security attacks into Physical, Network, Software, and Encryption attacks, providing detailed examples within each class. Future directions for IoT security include advocating for multi-layered security approaches and emphasizing risk assessment, physical security, and trust management. The paper also calls for research into new encryption and authentication mechanisms suitable for low-power IoT devices, alongside the development of standardized security protocols for various IoT applications like eHealth.

[21] Exploring security vulnerabilities in IoT devices reveals significant risks due to their interconnected nature, including unauthorized access and privacy violations. Effective mitigation strategies are crucial, encompassing robust authentication, encryption, secure firmware updates, and continuous network monitoring. Cultivating security awareness among users and manufacturers

is also vital. By proactively identifying vulnerabilities and implementing robust measures, IoT device security can be significantly enhanced, ensuring safe operation in our increasingly digitized world.

[22] The Internet of Things, or IoT, enables a wide range of devices to communicate with one another and cooperate to improve our services. While some gadgets are more intelligent than others, some aren't. Modern technology even assists in delivering improved services. But a lot of Internet of Things devices are low-power/energy consumers. There will be more than 75 billion internet-connected gadgets by 2025. We are forced to switch from IPv4 to IPv6 due to their sheer number. Sensors gather a lot of data, but some devices can't process it all, so they have to pass the data to larger devices that have the capacity. The larger devices can then determine what to do with the data. IPv6 is a unique system that operates via low-power wireless.

TABLE I
MAJOR CONTRIBUTION OF RESEARCH IN THE FIELD OF EXPLORING SECURITY VULNERABILITIES AND MITIGATION STRATEGIES IN IOTDEVICES

Author Name	Year	Paper Title	Outcome	Parameter Monitored	Algorithm Used	Limitations
(Williams et al.)	2022	*A Survey of Security Vulnerability Analysis, Discovery, Detection, and Mitigation on IoT Devices.*	Assessment of IoT security vulnerabilities and proposals for improvement.	Research on IoT security vulnerabilities, their impact, and potential solutions.	Various methods for vulnerability analysis and risk assessment.	Lack of comprehensive solutions for IoT security, potential gaps in vulnerability detection and mitigation strategies.
(Abomhara & Køien)	2015	*Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attack*	Strengthened cybersecurity defenses to protect IoT ecosystems.	Monitoring of IoT networks and devices for suspicious activities and potential cyber threats.	Advanced threat detection algorithms and machine learning techniques for anomaly detection in IoT traffic.	Challenges in ensuring compatibility and scalability of security solutions across diverse IoT platforms and devices.
(Siboni et al.,)	2019	*Security Testbed for Internet-of-Things Devices*	Improved security and privacy for IoT devices through a comprehensive testing framework.	Monitoring of IoT devices for vulnerabilities and compromised states.	Machine learning analysis integrated into security testing techniques for identifying vulnerabilities.	Challenges may arise in ensuring compatibility and effectiveness across diverse IoT device types and protocols.
(Electrónica & Msc)		*Vulnerabilities in the Internet of things.*	Enhanced security measures to mitigate cyber-attacks targeting	Monitoring of IoT devices and networks for vulnerabilities	Advanced threat detection algorithms to identify	Challenges in maintaining security across diverse IoT devices and protocols, especially

	2019		IoT networks.	and suspicious activities.	and respond to cyber threats in real time.	in healthcare where the stakes are higher due to potential patient safety risks.
(Sharma et al)	2019	*Vulnerabilities, Attacks, and their Mitigation: An Implementation on Internet of Things (IoT).*	Enhanced IoT security through proactive measures and intelligent predictive algorithms.	Monitoring for vulnerabilities, unauthorized access, and potential cyber threats targeting IoT devices and networks.	Intelligent computer programs for predictive analysis and prevention of cyber-attacks on IoT systems.	Challenges in securing IoT devices with limited resources and susceptibility to wireless network attacks are compounded by the automatic nature of IoT devices.
(Duan et al.)	2021	*Automated Security Assessment for the Internet of Things*.	Automated system for assessing security in IoT networks, enhancing risk mitigation. Potential attack paths.	Monitoring and analysis of vulnerability descriptions to predict severity and identify	Machine learning and natural language processing for severity prediction, integrated into a graphical security model comprising attack graphs and trees.	Dependency on the availability and accuracy of vulnerability descriptions, potential challenges in handling diverse IoT network architectures and protocols.
(Khatun et al)	2013	*Machine Learning for Healthcare-IoT Security: A Review and Risk Mitigation*.	Strengthened security for healthcare IoT devices through advanced authentication methods like machine learning.	Monitoring of different layers of healthcare IoT systems for potential cyber threats, including data breaches and unauthorized access.	Machine learning for advanced authentication and protection of healthcare IoT devices.	Challenges in implementing advanced security measures across diverse healthcare IoT devices and ensuring compatibility with existing systems.
(Bouanani et al.)	2019	*Understanding the Internet of Things Security and its Empirical Vulnerabilities*.	Enhanced security in IoT environments through access control measures.	Monitoring of IoT protocols, architecture, and platform security for vulnerabilities and potential breaches.	Security audit algorithms for identifying vulnerabilities in IoT platforms, potentially incorporating access control	Challenges in implementing access control across diverse IoT environments and ensuring compatibility with existing systems, as well as addressing evolving security threats.

					algorithms for future improvements.	
(Gupta & Vanjale)	2020	*Cyber Security Measures for Internet of Things Devices.*	Improved cybersecurity for IoT deployments through enhanced security measures.	Monitoring of IoT devices and networks for security breaches and vulnerabilities.	Not specified in the given paper.	Lack of specific details regarding algorithms used; challenges in ensuring comprehensive security across diverse IoT devices and networks.
(Yin et al.)	2018	*A DDoS Attack Detection and Mitigation with Software-Defined Internet of Things Framework.*	Enhanced security for IoT devices through a Software-Defined Internet of Things (SD-IoT) framework.	Monitoring of IoT devices and network traffic for DDoS attacks.	Cosine similarity-based algorithm for detecting and mitigating DDoS attacks in SD-IoT networks.	Limited discussion on broader security challenges beyond DDoS attacks; challenges in implementing SD-IoT framework across diverse IoT environments.
(Butun et al.)	2020	*Security vulnerabilities and countermeasures in the Internet of Things solutions.*	Improved security and integrity in IoT environments through Blockchain technology.	Monitoring of sensor data, device authentication, and data transmission for security and integrity.	Blockchain consensus algorithms for ensuring data integrity and authentication within IoT networks.	Challenges in scalability and interoperability of Blockchain solutions across diverse IoT devices and ecosystems.
(Ali et al.)	2021	*Security Issues and Vulnerability of IoT Devices.*	Enhanced security for IoT devices to protect users and belongings.	Monitoring of IoT device communication protocols (e.g., LoRaWAN, 6LoWPAN, BLE, Zigbee) for vulnerabilities and weaknesses.	Not specified in the given paper.	Lack of specific algorithms mentioned for addressing security vulnerabilities; challenges in ensuring robust security across diverse IoT communication protocols.
(Neshenko et al.)		*Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical*	Improved IoT security through tailored security measures and Internet-scale	Monitoring for vulnerabilities in IoT devices, focusing on weaknesses such as open	Not specified in the given paper.	Lack of specific algorithms mentioned for addressing security vulnerabilities; challenges in

	2019	*Look on Internet-scale IoT Exploitations.*	solutions.	ports and inadequate access controls.		implementing Internet-scale solutions across diverse IoT ecosystems.
(Williams et al.)	2022	*A survey on security in the Internet of Things with a focus on the impact of emerging technologies.*	Enhanced security for IoT software platforms through measures like data integrity, secure storage, and device authentication.	Monitoring for security threats including data breaches, unauthorized access, and device compromise.	Artificial Intelligence and Machine Learning for threat detection, and Blockchain for data encryption and secure firmware updates.	Challenges in implementing hardware security solutions for resource-constrained IoT devices and ensuring compatibility across diverse IoT platforms and devices.
(Millar)	2021	*IoT Security Challenges and Mitigations.*	Improved security standards for IoT deployments through the adoption of standardized protocols and enhanced legislative directives.	Monitoring for IoT vulnerabilities and malicious activities, focusing on resource constraints and the absence of standards.	Various security protocols including DTLS, IPSec/IKE v2, SIGF, and SVELTE for secure communication, routing, and intrusion detection in IoT networks.	Challenges in implementing standardized protocols across diverse IoT ecosystems and ensuring compatibility with existing infrastructure, as well as potential limitations in resource-constrained IoT devices.
(Iwuanyanwu et al.)	2023	*IoT Device Security Risks A Comprehensive Overview And Mitigation Strategies.*	Enhanced security for IoT devices through holistic mitigation strategies.	Monitoring for unauthorized access, encryption lapses, authentication weaknesses, physical vulnerabilities, and privacy breaches.	Not specified in the given paper.	Lack of specific algorithms mentioned for addressing security vulnerabilities; challenges in implementing interdisciplinary collaboration and standardization across diverse IoT ecosystems.
(Payton & Wang, n.d.)	2023	*Exploring Vulnerability and Security Schemes Of Service-Oriented Internet Of Things And*	Improved security for UPnP-enabled IoT devices through vulnerability	Monitoring for vulnerabilities in UPnP implementation within IoT	Not specified in the given paper.	Lack of specific algorithms mentioned for addressing vulnerabilities; potential challenges

		Protocols.	mitigation strategies.	environments.		in implementing mitigation strategies across diverse UPnP-enabled IoT deployments.
(Salayma)	2021	*Risk and Threat Mitigation Techniques in the Internet of Things.*	Enhanced security for IoT devices through hardware-based protection measures.	Monitoring for physical and cyber threats to IoT devices, focusing on hardware-level vulnerabilities.	Various hardware-based techniques including Hardware Trojans detection, Design for Trust (DFT), split manufacturing etc.	Increased costs and overhead associated with hardware-based protection measures, potentially limiting their applicability in certain IoT applications.

[23] The rapid growth of wearable technology has brought convenience but also raised security concerns due to potential vulnerabilities. To address this, Integrated Circuit Metric (ICMetric) technology is proposed to enhance security by creating unique identifiers using device characteristics, particularly accelerometer and gyroscope sensors. The paper explores generating group identifiers for authentication, confidentiality, and secure access in group environments. Experimental findings demonstrate high-security levels without resource overuse. With the expanding IoTecosystem, securing wearable technology is crucial for protecting data privacy and user well-being.

[24] This paper explores the growth of the IoT and the associated challenges, particularly regarding security and privacy. It highlights the increasing threats to security and privacy as IoT devices become more widespread and aims to summarize existing research on IoT security threats and countermeasures. The paper begins by presenting a comprehensive reference model for IoT and discusses information, assurance, and security requirements. It examines threats within the edge-side layer of the reference model and evaluates the countermeasures suggested to mitigate them, while also introducing two emerging security challenges. The main goal is to provide readers with insights into past attacks, their mitigation, and ongoing threats, organized into sections covering the reference model, IoT applications, security requirements, attacks, countermeasures, emerging challenges, and future research directions.

III. Exploring the Advantages and Disadvantages of IoT Devices

A. *Advantages*

IoT technology represents a paradigm shift in connectivity and efficiency, fostering seamless collaboration among diverse systems and devices across various sectors. By generating vast amounts of data, IoT devices offer valuable insights which drive informed decision-making, optimize processes, enhance product quality, and elevate customer experiences. This transformative technology enables the automation of tasks and remote monitoring of operations, minimizing manual intervention and facilitating real-time responses to events. In sectors like agriculture, IoT technology is transforming agriculture by helping farmers keep a close eye on soil conditions and crop health, allowing them to make smarter, data-driven decisions. By streamlining operations and cutting down on maintenance costs, these smart solutions not only save time and money but also make farming more efficient and sustainable. For instance, IoT-enabled energy management systems dynamically adjust environmental settings in smart buildings, resulting in lower energy consumption and reduced carbon footprint. Furthermore, IoT devices enhance safety and security across various domains, such as healthcare and industrial environments. In healthcare, IoT-enabled medical devices monitor patient vital signs and alert healthcare providers to potential emergencies, enabling timely interventions and improving patient outcomes. Overall, the integration of IoT technology into diverse applications underscores its transformative potential in driving efficiency, innovation, and safety across industries.

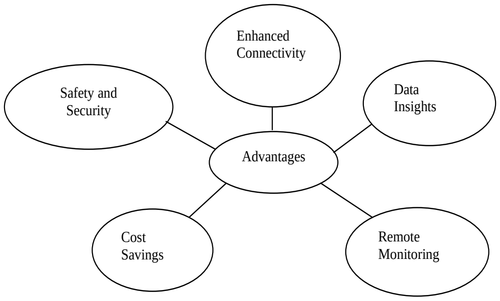

Fig. 3. Advantages of IoT Devices

Fig.3 shows how IoT technology brings many advantages. It focuses on better connections and efficiency by making communication smoother, which helps to get more work done. Also, IoT gives us useful information from data, helping us to make smart decisions and improve how things are done. Automation and remote monitoring make tasks easier, especially in farming. Using IoT can save money, especially in managing energy. Lastly, IoT makes places safer, like hospitals, by keeping an eye on important signs and warnings about emergencies.

B. Disadvantages

IoT technology, while offering numerous advantages, also presents significant disadvantages. Security vulnerabilities, including weak authentication mechanisms and insecure communication protocols, expose IoT devices to unauthorized access and cyber-attacks, compromising privacy and operational continuity. Privacy concerns arise from the extensive collection of personal data by IoT devices, raising questions about data usage and regulatory compliance. Interoperability challenges hinder the seamless integration and management of heterogeneous IoT systems, limiting scalability and effectiveness. Reliability issues stemming from network outages and hardware failures pose risks to critical operations, necessitating robust contingency plans. Additionally, the complexity of managing and maintaining IoT deployments, coupled with resource-intensive maintenance requirements, can strain organizations and lead to operational challenges and increased costs.

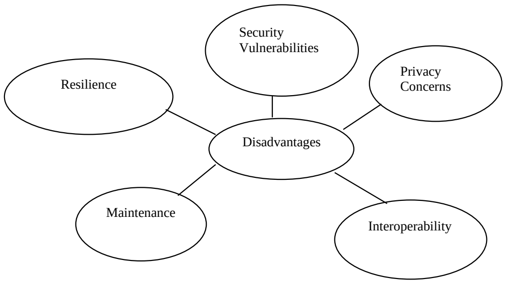

Fig. 4. Disadvantages of IoT Devices

Fig. 4 illustrates the multifaceted challenges associated with IoT technology deployment. It highlights security vulnerabilities, privacy concerns, interoperability issues, maintenance complexities, and the need for resilience. These factors underscore the intricate landscape of managing and securing IoT ecosystems, emphasizing the importance of proactive measures to address these challenges effectively.

IV. Future Advancements in IoT Device Security

. The future of IoT device security shows great promise as technology evolves to meet new challenges. As more devices connect in various sectors, it's crucial to have strong security measures to protect data integrity, user privacy, and system reliability. Advances in IoT device security are set to change the game, fixing current problems while also preventing future issues. One big step forward is using blockchain technology. Blockchain provides a secure way to record transactions and data exchanges without a central authority. By using blockchain, IoT devices can make sure data is genuine, stop anyone from tampering with it, and reduce the chance of unauthorized access. This makes IoT systems safer from cyber threats.

Artificial intelligence (AI) and machine learning (ML) are also making a big difference in IoT security. AI can look at loads of data in real time, spotting any unusual activity that might be a security risk. ML helps IoT systems learn from patterns and trends, making them better at predicting and stopping cyber threats. With AI and ML, IoT devices can stay ahead of hackers and keep systems running smoothly.

There's also been progress in making cryptographic techniques lighter and more efficient. Traditional methods can be too heavy for IoT devices with limited power and processing ability. New techniques like elliptic curve cryptography (ECC) and homomorphic encryption make security stronger without using up too much energy. This means IoT devices can keep data safe without draining their batteries.

It's important to have standard rules and guidelines for IoT security. These help different devices work together smoothly and securely. Industry-wide security frameworks give clear instructions on how to design, set up, and manage secure IoT systems. Following these rules helps companies make sure their devices meet the same high-security standards and obey the law.

V. Conclusion

The widespread use of IoT devices has drastically changed how things connect and how convenient things are in different areas. But, as more and more of these devices are being used, there are also more chances for security problems to happen. This means we need to pay close attention to keeping them safe. Studies in this area always say it's really important to deal with these security problems well. This is not just to keep people's private information safe and make sure data is correct, but also to make sure everything runs smoothly. They suggest we should focus more on making each device safe and improving the ways we keep things secure from online threats. These studies also show that there are lots of ways these IoT systems can be vulnerable, like problems with the software they run or weaknesses in the wireless networks they use. They suggest new ideas, like using smart computer programs to look for problems and better ways to organize the software, to help solve these issues. What all this research is saying is that we need to work together to make sure IoT systems are safe. This means everyone involved, like the people making the devices, the companies providing services, researchers, and even the people using the devices, needs to team up. If we focus on being proactive about security, setting strong rules, and understanding new problems that come up, we can make IoT systems much safer for everyone.

Acknowledgment

We would like to express our sincere appreciation to Assistant Professor Mr. Dhiraj Prasad Jaiswal and Mr. Rahul Shah for their invaluable assistance and guidance throughout the development of this review paper. Their expertise, dedication, and encouragement have greatly enhanced our understanding of Teacher Training and Professional Development in the context of AI integration. Their insightful input and mentorship have been crucial in shaping the scope and depth of our review. We are deeply grateful for their patience, accessibility, and dedication to academic excellence. Their collaborative approach and contributions have been essential to the successful completion of this paper. It has been a privilege to collaborate with them on this project, and we appreciate their steadfast support. We recognize their significant contributions to our academic development and the overall quality of our work. Thank you for your exceptional mentorship and guidance.

References

[1] H. M. M. Al-Zyoud, “The role of artificial intelligence in teacher professional development,” Universal Journal of Educational Research, vol. 8, no. 11B, pp. 6263–6272, Nov. 2020, doi: 10.13189/ujer.2020.082265.

[2] E. Zotikovna, E. Yuriievna, S. Viktorovna, and P. Aleksandrovich, “Artificial intelligence-The space for the new possibilities to train teachers Inteligencia artificial. Un espacio de nuevas posibilidades para el entrenamiento de docentes,” 2019.

[3] P. Chaipidech, N. Srisawasdi, T. Kajornmanee, and K. Chaipah, “A personalized learning system-supported professional training model for teachers’ TPACK development,” Computers and Education: Artificial Intelligence, vol. 3, Jan. 2022, doi: 10.1016/j.caeai.2022.100064.

[4] T. Nazaretsky, M. Ariely, M. Cukurova, and G. Alexandron, "Teachers' trust in AI-powered educational technology and a professional development program to improve it," British Journal of Educational Technology, vol. 53, no. 4, pp. 914–931, Jul. 2022, doi: 10.1111/bjet.13232.

[5] China Research Council of Computer Education in Colleges & Universities, Technische Universiteit Delft, IEEE Education Society, and Institute of Electrical and Electronics Engineers, The 15th International Conference on Computer Science & Education (ICCSE 2020) : August 18 -20, Online.

[6] I. Celik, "Towards Intelligent-TPACK: An empirical study on teachers' professional knowledge to ethically integrate artificial intelligence (AI)-based tools into education," Comput Human Behav, vol. 138, Jan. 2023, doi: 10.1016/j.chb.2022.107468.

[7] W. Yangyang, "Teaching Ability Performance and Professional Development Among Artificial Intelligence Chinese Professors," Asia Pacific Journal of Management and Sustainable Development, vol. 11, no. 1, pp. 35–45, 2023.

[8] I. Celik, M. Dindar, H. Muukkonen, and S. Järvelä, "The Promises and Challenges of Artificial Intelligence for Teachers: a Systematic Review of Research," TechTrends, vol. 66, no. 4, pp. 616–630, Jul. 2022, doi: 10.1007/s11528-022-00715-y.

[9] A. Mohammed, R. Ali, A. Abdulkareem, and B. Alharbi, "The Reality of Using Artificial Intelligence Techniques in Teacher Preparation Programs in Light of the Opinions of Faculty Members: A Case Study in Saudi Qassim University Multicultural Education The Reality of Using Artificial Intelligence Techniques in Teacher Preparation Programs in Light of the Opinions of Faculty Members: A Case Study in Saudi Qassim University", doi: 10.5281/zenodo.4410582.

[10] P. John Bassey, N. P. Essien, and M. Edet Thompson, "Artificial Intelligence and Lecturers' Professional Development in Faculty of Education and Faculty of Vocational Education, Library and Information Science, University of Uyo, Akwa Ibom State, Nigeria," International Journal of Contemporary Africa Research Network Publication of Contemporary Africa Research Network (CARN), vol. 1, no. 1, p. 2024, 2024, doi: 10.5281/zenodo.10575387.

[11] M. NYAABA and X. ZHAI, "Generative AI Professional Development Needs for Teacher Educators," Journal of AI, vol. 8, no. 1, pp. 1–13, Jan. 2024, doi: 10.61969/jai.1385915.

[12] M. Marienko, Y. Nosenko, A. Sukhikh, V. Tataurov, and M. Shyshkina, "Personalization of learning through adaptive technologies in the context of sustainable development of teachers' education," in E3S Web of Conferences, EDP Sciences, Apr. 2020. doi: 10.1051/e3sconf/202016610015.

[13] M. S. Ramírez-Montoya, L. Andrade-Vargas, D. Rivera-Rogel, and M. Portuguez-Castro, "Trends for the future of education programs for professional development," Sustainability (Switzerland), vol. 13, no. 13, Jul. 2021, doi: 10.3390/su13137244.

[14] I. Lee et al., "AI Book Club: An Innovative Professional Development Model for AI Education," in SIGCSE 2022 - Proceedings of the 53rd ACM Technical Symposium on Computer Science Education, Association for Computing Machinery, Inc, Feb. 2022, pp. 202–208. doi: 10.1145/3478431.3499318.

[15] S. Z. Salas-Pilco, K. Xiao, and X. Hu, "Artificial Intelligence and Learning Analytics in Teacher Education: A Systematic Review," Education Sciences, vol. 12, no. 8. Multidisciplinary Digital Publishing Institute (MDPI), Aug. 01, 2022. doi: 10.3390/educsci12080569.

[16] X. F. Lin et al., "Teachers' Perceptions of Teaching Sustainable Artificial Intelligence: A Design Frame Perspective," Sustainability (Switzerland), vol. 14, no. 13, Jul. 2022, doi: 10.3390/su14137811.

[17] Y. Copur-Gencturk, J. Li, A. S. Cohen, and C. H. Orrill, "The impact of an interactive, personalized computer-based teacher professional development program on student performance: A randomized controlled trial," Comput Educ, vol. 210, Mar. 2024, doi: 10.1016/j.compedu.2023.104963.

[18] T. N. Fitria, "Artificial Intelligence (AI) In Education: Using AI Tools for Teaching and Learning Process." [Online]. Available: https://www.researchgate.net/publication/357447234

[19] N. Ghamrawi, T. Shal, and N. A. R. Ghamrawi, "Exploring the impact of AI on teacher leadership: regressing or expanding?" Educ Inf Technol (Dordr), 2023, doi: 10.1007/s10639-023-12174-w.

[20] K. W. Yau, C. S. Chai, T. K. F. Chiu, H. Meng, I. King, and Y. Yam, "A phenomenographic approach on teacher conceptions of teaching Artificial Intelligence (AI) in K-12 schools," Educ Inf Technol (Dordr), vol. 28, no. 1, pp. 1041–1064, Jan. 2023, doi: 10.1007/s10639-022-11161-x.

[21] K. Sperling, C.-J. Stenberg, C. McGrath, A. Åkerfeldt, F. Heintz, and L. Stenliden, "In search of artificial intelligence (AI) literacy in teacher education: A scoping review," Computers and Education Open, vol. 6, p. 100169, Jun. 2024, doi: 10.1016/j.caeo.2024.100169.

[22] G. Attwell, "Vocational Education and Training and Lifelong Learning," pp. 67–72, doi: 10.5281/ze.

[23] M. NYAABA and X. ZHAI, "Generative AI Professional Development Needs for Teacher Educators," Journal of AI, vol. 8, no. 1, pp. 1–13, Jan. 2024, doi: 10.61969/jai.1385915.

[24] "Erratum to: Artificial Intelligence for Higher Education Development and Teaching Skills (Wireless Communications and Mobile Computing (2022) 2022 (7614337) DOI: 10.1155/2022/7614337)," Wireless Communications and Mobile Computing, vol. 2023. Hindawi Limited, 2023. doi: 10.1155/2023/9769121.