Engineering and Technology Journal e-ISSN: 2456-3358

Volume 10 Issue 07 July-2025, Page No.- 5776-5794

DOI: 10.47191/etj/v10i07.26, I.F. – 8.482

Security Challenges in IoT: A Systematic Literature Review

Victor Kelechukwu Madu

York St John University, London Campus, United Kingdom

ABSTRACT: The rapid proliferation of the Internet of Things (IoT) has introduced transformative capabilities across diverse sectors but has also exposed critical security vulnerabilities due to the interconnected and often resource-constrained nature of IoT devices. This systematic literature review examines the prevailing security challenges within IoT environments, focusing on threat vectors, attack surfaces, and mitigation strategies. Drawing from a comprehensive analysis of peer-reviewed publications, the paper categorizes key challenges such as authentication weaknesses, data integrity threats, device heterogeneity, and privacy concerns. The review also explores the role of emerging security frameworks and technologies—including lightweight encryption, blockchain integration, and edge computing—in enhancing IoT resilience. Particular attention is paid to the evolving attack landscape, highlighting the increasing sophistication of threats like botnets, side-channel attacks, and firmware exploitation. The findings underscore the importance of adopting a holistic and layered security approach that encompasses hardware, software, and network-level protections. Furthermore, the paper identifies gaps in current research, especially around standardization, real-time anomaly detection, and scalable security architectures. The review concludes by recommending strategic directions for future work, including cross-domain policy enforcement and AI-driven security automation. This study contributes to a deeper understanding of IoT security, offering critical insights for researchers, developers, and enterprise stakeholders seeking to fortify IoT deployments against escalating cyber threats.

KEYWORDS: Internet of Things (IoT), IoT Security, Autonomous Threat Response, Lightweight Security Protocols, Legal-Technical Alignment, AI-based Threat Detection, Quantum-safe Cryptography, Edge Computing, Federated Learning, Security Frameworks

1. INTRODUCTION

1.1. The Rise of IoT and Its Importance.

The Internet of Things (IoT) has emerged as one of the most transformative technological paradigms of the 21st century, fundamentally reshaping the fabric of global industrial and social systems. Characterised by a dynamic network of interconnected physical devices embedded with sensors, software, and other technologies, IoT enables real-time data collection, communication, and intelligent decision-making without human intervention. Its rise has been significantly driven by advances in wireless communication, cloud computing, miniaturised sensors, and data analytics, fostering a new era of pervasive connectivity and automation across a spectrum of industries (Al-Fuqaha et al., 2015). As digital transformation accelerates, the importance of IoT in enhancing operational efficiency, reducing human errors, and supporting data-driven insights continues to gain momentum, establishing it as a cornerstone of the Fourth Industrial Revolution.

IoT adoption is growing exponentially across diverse sectors, including manufacturing, agriculture, healthcare, transportation, energy, and smart cities. In industrial automation, often referred to as the Industrial Internet of Things (IIoT), sensors and actuators collect real-time data from machines and processes, enabling predictive maintenance, quality assurance, and supply chain optimisation (Xu, He and Li, 2014). Similarly, in agriculture, precision farming techniques utilise IoT devices to monitor soil moisture, crop health, and climate conditions, thereby maximising yield while minimising input waste (Wolfert et al., 2017). The healthcare sector leverages IoT through wearable technologies and remote patient monitoring systems to enable personalised care, reduce hospital admissions, and enhance patient outcomes (Islam et al., 2015). Transportation systems benefit from IoT through vehicle telematics, real-time tracking, and intelligent traffic control, all of which contribute to increased safety and reduced congestion (Zanella et al., 2014). These examples illustrate the pivotal role IoT plays in redefining industry processes and services through enhanced connectivity and intelligent automation.

One of the defining attributes of IoT is its unparalleled capacity to generate vast volumes of data at high velocity, which provides an invaluable foundation for analytics and artificial intelligence applications. By facilitating continuous and context-aware data flows from the physical world to digital platforms, IoT supports the development of adaptive systems that respond dynamically to environmental stimuli and user behaviour. As a result, businesses can achieve real-time visibility into operations, optimise decision-making processes, and drive innovation through predictive modelling and intelligent automation (Gubbi et al., 2013). Furthermore,

the synergistic integration of IoT with other emerging technologies such as 5G, edge computing, and blockchain has further amplified its potential. For instance, 5G networks significantly enhance data transmission speeds and reliability, while edge computing enables decentralised processing, reducing latency and improving system responsiveness (Chiang and Zhang, 2016).

Despite its widespread benefits, the deployment of IoT also introduces substantial challenges, particularly in areas related to data security, privacy, interoperability, and scalability. The heterogeneous and distributed nature of IoT devices, often operating with limited computational resources and inadequate built-in security protocols, renders them vulnerable to a broad spectrum of cyber threats. These include device hijacking, data breaches, and denial-of-service attacks, which can severely compromise the confidentiality, integrity, and availability of critical systems (Sicari et al., 2015). Moreover, the lack of universal standards for device communication and security exacerbates the difficulty in achieving consistent protection across IoT ecosystems. As adoption increases, addressing these security vulnerabilities becomes imperative to safeguard the trust and sustainability of IoT infrastructures.

The economic and strategic importance of IoT cannot be overstated. According to McKinsey Global Institute, the global economic impact of IoT applications could reach between $3.9 trillion and $11.1 trillion per year by 2025, depending on the extent of IoT integration across sectors (Manyika et al., 2015). Governments and organisations worldwide have recognised this potential, investing heavily in IoT research, infrastructure, and deployment initiatives. National strategies such as Germany's "Industrie 4.0", China's "Made in China 2025", and the European Union's "Digital Single Market" underscore the global prioritisation of IoT in driving innovation, competitiveness, and sustainable development.

The rise of IoT represents a monumental shift in how industries and societies operate, interact, and innovate. Its ability to connect the physical and digital realms through ubiquitous sensing and intelligent analysis marks a critical enabler of smarter, more efficient systems. However, the full realisation of IoT's transformative potential hinges on addressing underlying technical and security challenges. This review seeks to explore these critical concerns, with particular emphasis on the security risks inherent in IoT environments, thereby contributing to the broader discourse on building resilient and trustworthy IoT ecosystems for the future.

1.2. Objectives of the Review.

As the Internet of Things (IoT) continues to evolve and proliferate across global industries, its security landscape remains one of the most complex and underdeveloped aspects of the technological paradigm. With billions of connected devices operating across heterogeneous environments and performing critical tasks in healthcare, manufacturing, agriculture, energy, and transportation, the potential vulnerabilities inherent in IoT systems present significant risks to data confidentiality, system integrity, and service availability. This review is motivated by the urgent need to systematically identify, classify, and analyse the prevailing security threats and challenges that compromise the robustness and trustworthiness of IoT environments. By drawing from a comprehensive selection of scholarly and industry sources, the review aims to develop a structured and evidence-based understanding of security concerns, thereby providing clarity in a field often characterised by fragmentation and technological heterogeneity.

The objective of this review is to rigorously explore the security challenges within IoT by categorising threats according to their sources, attack vectors, and potential impact on system architecture. This includes vulnerabilities at the device level, such as weak authentication mechanisms and limited computational resources; network-level threats, including data interception and denial-of-service attacks; and application-level risks associated with insecure protocols, firmware updates, and third-party software integrations. By mapping the attack surface of IoT ecosystems in this structured manner, the review aims to offer a taxonomy that not only reflects the current threat landscape but also facilitates strategic prioritisation of risk mitigation measures.

The scope of this review extends beyond the mere identification of vulnerabilities. It encompasses the evaluation of existing mitigation strategies, such as lightweight cryptographic techniques, secure communication protocols, blockchain-based access control mechanisms, and machine learning approaches for anomaly detection. These solutions are analysed for their applicability, scalability, and efficiency across different categories of IoT deployment, ranging from constrained edge devices to cloud-integrated smart systems. Furthermore, the review examines regulatory frameworks and policy recommendations that govern the security and privacy of IoT systems. Understanding the legal and organisational implications of IoT security is critical for developing comprehensive protection strategies that align with both technical and ethical considerations.

A critical component of the review's methodology is the application of systematic literature review protocols. This includes the establishment of inclusion and exclusion criteria, keyword-based search strategies, quality appraisal mechanisms, and thematic synthesis. By adhering to systematic review standards, the review ensures transparency, replicability, and objectivity in data collection and interpretation. Sources were drawn from high-impact journals and technical repositories, focusing on publications that capture both foundational research and recent advancements. The methodology also enables the identification of research gaps—such as the need for unified security standards, improved real-time threat detection, and interoperable security architectures—which informs the discussion of future research directions.

The review also recognises the unique constraints imposed by IoT architecture, which distinguish it from conventional information systems. These include energy limitations, bandwidth restrictions, intermittent connectivity, and the physical exposure of devices, all of which complicate the implementation of traditional security mechanisms. As a result, the review places emphasis on context-aware and resource-efficient security solutions that are tailored to the operational realities of IoT deployments. This is particularly relevant for environments such as smart grids, industrial control systems, and healthcare applications, where security breaches can result in not only data loss but also safety-critical failures.

Given the accelerating pace of IoT adoption, the urgency of addressing its security challenges has never been more pressing. The increased reliance on IoT for mission-critical operations raises the stakes for securing data, devices, and communication channels. High-profile security incidents have demonstrated how poorly secured IoT devices can be exploited at scale to launch devastating cyber-attacks. Such cases underscore the need for proactive and holistic approaches to IoT security, grounded in both technical robustness and strategic foresight. By collating and synthesising the body of knowledge on IoT threats and countermeasures, this review aspires to provide a definitive resource for researchers, practitioners, and policymakers committed to strengthening the resilience of connected systems.

The primary aim of this review is to provide a systematic and comprehensive assessment of the security challenges confronting IoT ecosystems. By classifying threats, evaluating mitigation frameworks, and identifying knowledge gaps, the review contributes to a clearer understanding of the vulnerabilities undermining IoT infrastructure. This work ultimately supports the broader goal of enabling the secure and sustainable integration of IoT technologies into the digital infrastructure of contemporary society.

1.3. Critical Security Issues in IoT.

The Internet of Things (IoT) introduces a complex ecosystem of interconnected devices, sensors, and systems that communicate autonomously to support intelligent decision-making across various application domains. While this pervasive interconnectivity has driven significant advancements in automation, operational efficiency, and data-driven insights, it has simultaneously introduced a host of critical security vulnerabilities. These vulnerabilities stem primarily from the inherent characteristics of IoT architectures, notably their distributed nature, resource constraints, and technological heterogeneity. These defining features create fertile ground for malicious actors to exploit system weaknesses, posing significant risks to the confidentiality, integrity, and availability of IoT infrastructures (Roman, Zhou and Lopez, 2013).

The distributed nature of IoT networks, wherein devices are often deployed across physically dispersed environments, presents a significant challenge for centralised security governance. Unlike traditional computing systems that are typically confined to well-defined perimeters, IoT deployments extend across diverse and often uncontrolled contexts, such as public spaces, remote industrial sites, or personal residences. This lack of central oversight complicates the application of standardised security protocols and makes it difficult to detect and contain breaches once they occur. Adversaries can exploit these gaps to launch sophisticated attacks such as eavesdropping, man-in-the-middle intrusions, and routing manipulations, often without immediate detection (Sicari et al., 2015).

Compounding the issue is the resource-constrained nature of many IoT devices. These devices typically operate with limited processing power, memory, and energy capacity, which restricts the implementation of conventional security mechanisms such as public-key cryptography or real-time intrusion detection systems. Lightweight security protocols have been proposed to address this limitation; however, their reduced computational overhead often comes at the cost of diminished cryptographic robustness or slower response to emerging threats. As a result, these devices remain attractive targets for cyber attackers seeking to exploit their weaknesses with minimal resistance (Hossain et al., 2015).

Moreover, the heterogeneity of IoT systems—characterised by the integration of components from multiple vendors, varying communication protocols, and diverse hardware configurations—further exacerbates the security landscape. This diversity creates inconsistencies in security policy enforcement, complicates vulnerability assessments, and increases the likelihood of interoperability issues. Firmware updates and patching practices are often non-standardised, leading to outdated systems that are susceptible to known exploits. The lack of universally adopted security standards means that security responsibility is fragmented, leaving devices and platforms with uneven levels of protection (Alrawais, Alhothaily, Hu and Cheng, 2017).

Inter-device communication, particularly when conducted over unencrypted or inadequately secured channels, introduces additional attack vectors. Sensitive information such as user credentials, location data, and operational commands can be intercepted and manipulated by unauthorised parties. Furthermore, the absence of strong identity verification mechanisms makes it possible for attackers to inject rogue devices into the network or assume the identity of legitimate devices, leading to data corruption or malicious control over physical systems. In high-stakes environments such as healthcare and industrial automation, the consequences of such intrusions can be catastrophic (Sfar, Natalizio, Challal and Chtourou, 2018).

An important but often overlooked vulnerability arises from the physical accessibility of IoT devices. Given their widespread deployment in uncontrolled or semi-controlled

environments, these devices are more susceptible to physical tampering, reverse engineering, and hardware-level attacks. Attackers can access critical debug ports, extract firmware, or introduce malicious code directly into the device, bypassing network-level defences altogether. This physical vulnerability is particularly critical for devices embedded in critical infrastructure, such as smart grids or autonomous vehicles, where device compromise can have severe safety and operational implications (Weber, 2010).

The challenges associated with securing IoT systems are also amplified by the dynamic and real-time nature of many applications. Devices often operate under stringent latency requirements, particularly in contexts such as autonomous driving or emergency response systems, where milliseconds can determine system success or failure. Security mechanisms that introduce latency or interfere with real-time processing can be deemed impractical, creating trade-offs between protection and performance. As a result, many deployments opt for minimal security configurations, prioritising speed and functionality at the expense of risk resilience.

Another compounding factor is the lifecycle management of IoT devices. Many devices have long lifespans and are rarely updated or replaced, particularly in industrial or infrastructure settings. Over time, these devices become increasingly obsolete, relying on deprecated protocols and unsupported firmware. Without mechanisms for remote patching or secure decommissioning, such devices serve as persistent weak links within otherwise secure networks. The long-term persistence of these vulnerabilities calls for strategic foresight and investment in lifecycle-aware security frameworks (Fernandes et al., 2017).

In light of these multifaceted security concerns, it becomes clear that IoT environments demand a rethinking of traditional cybersecurity paradigms. Effective security in the context of IoT must be decentralised, scalable, context-aware, and lightweight. Moreover, it requires coordinated efforts across device manufacturers, platform providers, policymakers, and end-users. Addressing the critical security issues in IoT is not only a technical challenge but also a governance and compliance issue, necessitating the formulation and enforcement of standards that account for the unique characteristics of IoT systems.

While IoT technologies continue to drive innovation and efficiency across sectors, their vulnerabilities—rooted in distributed deployment, limited device resources, and architectural heterogeneity—pose significant threats to modern digital infrastructure. This review highlights the urgent need for robust, scalable, and adaptable security solutions tailored specifically for IoT contexts. By identifying and understanding these critical issues, the path forward involves developing multi-layered defences that can protect IoT ecosystems throughout their entire lifecycle, thereby safeguarding both technological progress and societal trust.

2. LITERATURE REVIEW

2.1. Taxonomy of IoT Security Challenges.

The Internet of Things (IoT) represents a paradigm shift in how digital systems interact with the physical world, enabling seamless interconnectivity across devices, services, and users. However, the proliferation of interconnected devices brings with it a multifaceted landscape of security challenges. The literature presents a comprehensive taxonomy that categorizes these security threats into distinct domains: device-level vulnerabilities, network-level attacks, data privacy breaches, and insecure interfaces. Understanding these categories is imperative for developing robust, multi-layered defense mechanisms tailored to IoT environments.

Device-level vulnerabilities remain a foundational concern in IoT security. These vulnerabilities often stem from resource-constrained hardware, lack of standardized security protocols, and insufficient firmware updates. According to Sebestyen et al. (2025), IoT devices frequently operate under minimal computational power, limiting the implementation of advanced cryptographic mechanisms. Moreover, weak authentication procedures and hardcoded credentials, commonly found in consumer-grade IoT devices, provide an easy entry point for attackers. Makhdoom et al. (2018) reinforce this by identifying physical tampering, device cloning, and side-channel attacks as prevalent threats that exploit hardware-level design flaws.

In addition to hardware vulnerabilities, network-level attacks constitute a critical segment of IoT security taxonomy. The decentralized and distributed architecture of IoT ecosystems presents a broad attack surface. Protocols such as MQTT and CoAP, designed for lightweight communication, often lack inherent security features. Jayalaxmi et al. (2021) outline that man-in-the-middle (MITM) attacks, spoofing, and denial-of-service (DoS) attacks are especially common, given the limited packet inspection and rudimentary intrusion detection capabilities of IoT networks. These vulnerabilities compromise not only data confidentiality and integrity but also the availability of critical services.

Another pressing dimension of IoT security involves data privacy breaches. Given that IoT devices continuously collect, transmit, and store vast quantities of personal and contextual data, they are prime targets for unauthorized data access and surveillance. Mazhar et al. (2021) emphasize the importance of privacy-preserving techniques, such as differential privacy and homomorphic encryption, which are seldom implemented due to processing limitations. Data breaches often result from inadequate data encryption during transmission or insufficient access control mechanisms on cloud platforms where data is stored.

Closely related to data privacy issues are threats posed by insecure interfaces. The interfaces through which users interact with IoT systems—such as mobile apps, web dashboards, or voice assistants—can introduce significant security risks if poorly designed. Rizvi et al. (2020) argue that insecure web APIs, lack of input validation, and overly

permissive permissions are common flaws in interface design. These vulnerabilities facilitate attacks such as cross-site scripting (XSS), session hijacking, and privilege escalation, undermining the trust and usability of IoT systems.

Furthermore, the layered nature of IoT systems calls for an integrated security framework that addresses these challenges holistically. HaddadPajouh et al. (2021) propose a layered taxonomy that maps specific threats to their corresponding strata—device, network, application, and cloud. This approach aids in the identification of overlapping vulnerabilities and fosters the development of layer-specific countermeasures. However, implementation remains fragmented due to the heterogeneity of devices and protocols in use.

Recent advances in machine learning and artificial intelligence offer promising avenues for proactive vulnerability detection and classification. Hulayyil et al. (2023) present a machine-learning-based approach capable of identifying anomalous patterns indicative of potential security breaches. Such techniques can significantly enhance real-time threat detection but are constrained by the high volume and velocity of IoT-generated data.

Finally, the platform-level configuration of IoT environments also influences their overall security posture. Babun et al. (2021) emphasize that IoT platforms must integrate comprehensive security measures that span authentication, data encryption, and user role management. They highlight that current commercial solutions often lack default security settings or provide optional protections that are seldom enabled by users.

The taxonomy of IoT security challenges is multifaceted and spans several interrelated domains. Device-level vulnerabilities, network-based attacks, data privacy breaches, and insecure interfaces each present unique risks requiring specialized solutions. A unified, multi-layered approach supported by emerging technologies and standardized frameworks is essential to mitigate these threats and safeguard the growing ecosystem of IoT devices.

2.2. Common Attack Vectors and Threat Models.

The rapid proliferation of the Internet of Things (IoT) has expanded the attack surface available to cyber adversaries, introducing a complex ecosystem where vulnerabilities can be exploited at multiple layers. Threat modeling in the context of IoT must therefore be inclusive of a diverse range of attack vectors, including Distributed Denial of Service (DDoS), spoofing, man-in-the-middle (MITM), firmware manipulation, and side-channel attacks. Each of these attack types targets different aspects of IoT architecture, and understanding their mechanisms is essential to developing comprehensive and resilient security frameworks.

DDoS attacks are among the most disruptive threats to IoT environments due to their capacity to overwhelm network resources by flooding them with traffic. These attacks frequently exploit inadequately secured IoT nodes to form botnets capable of launching high-volume traffic assaults. For instance, Srivastava, Gupta and Quamara (2020) report that malware-enabled DDoS attacks such as those executed by the Mirai botnet have demonstrated the potential of compromised IoT devices to significantly degrade network services. Moreover, spoofed IP packets are commonly employed in such attacks to obfuscate the origin, complicating mitigation strategies. Chaudhary and Mishra (2023) further highlight emerging hierarchical DDoS models that are tailored to exploit the structured layering in industrial IoT settings.

Spoofing, another prominent vector, allows attackers to impersonate legitimate devices or users by falsifying authentication credentials or network identities. This deception can enable unauthorized access and serve as a precursor to more advanced attacks like MITM or data exfiltration. According to Hintaw, Manickam and Aboalmaaly (2023), spoofing vulnerabilities are especially prevalent in MQTT protocol implementations, where the lack of endpoint verification creates conditions for impersonation and unauthorized control of IoT actuators. This makes spoofing not just a standalone attack but a foundational threat enabling a spectrum of other exploits.

MITM attacks represent a significant challenge in IoT due to the frequent use of unencrypted communication channels. These attacks allow adversaries to intercept, modify, or reroute communications between devices and servers without detection. Thankappan, Rifà-Pous and Garrigues (2022) document how multi-channel MITM attacks can simultaneously exploit Wi-Fi, Bluetooth, and Zigbee channels to compromise communications in smart environments. Furthermore, Makhdoom, Abolhasan and Lipman (2018) emphasize that MITM attacks are often launched in conjunction with spoofing, where an attacker poses as a trusted intermediary to intercept communications and inject malicious payloads.

Firmware manipulation is an insidious attack method that targets the foundational code operating IoT devices. Because firmware is typically executed with high privilege levels, successful manipulation can grant attackers persistent control over device functionality. Mudgerikar and Bertino (2021) warn that malicious firmware updates or replacement binaries allow adversaries to establish backdoors, disable security mechanisms, or exfiltrate data. Compounding the risk is the frequent absence of secure boot mechanisms and cryptographic verification of firmware in many low-cost IoT devices.

Side-channel attacks, though traditionally associated with cryptographic implementations, have found novel applications in the IoT domain. These attacks exploit physical emanations such as electromagnetic radiation, power consumption, or timing variations to infer sensitive data. Pham (2022) demonstrates that side-channel techniques can be employed to classify IoT malware and detect hidden rootkits by monitoring processor activity patterns. Similarly, Patel and Singh (2023) identify multiple subtypes of side-

channel attacks, including power analysis and acoustic leakage, which can be deployed even when data encryption is implemented, thereby bypassing traditional defensive mechanisms.

In addition to specific attack types, comprehensive threat models are critical for understanding and predicting how these attacks may be orchestrated in real-world scenarios. Xenofontos and Zografopoulos (2021) propose a multi-layered threat taxonomy encompassing physical, network, and application layers, revealing how attackers often exploit combinations of vulnerabilities across layers to escalate privileges and achieve broader compromise. For instance, a spoofing attack may be used to gain unauthorized access, followed by a firmware overwrite that persists beyond device reboots.

Collectively, these findings underscore that the security posture of IoT ecosystems cannot rely on isolated countermeasures. Each attack vector must be contextualized within a broader threat model that accounts for the dynamic and interconnected nature of IoT systems. Mitigating these threats requires an integrated security architecture that includes secure firmware practices, encrypted multi-channel communication, real-time anomaly detection, and hardened protocols with robust authentication mechanisms.

2.3. IoT Security in Key Application Domains.

The proliferation of Internet of Things (IoT) technologies has profoundly impacted key sectors such as healthcare, smart homes, industrial operations, and transportation. However, as adoption grows, so too do the complexities and severity of security challenges across these domains. Each application area presents distinct vulnerabilities based on the nature of deployed devices, sensitivity of transmitted data, and the interconnectivity of cyber-physical systems. Understanding sector-specific security concerns is critical for implementing robust, context-aware security strategies.

In healthcare, IoT devices such as wearable monitors, implantable sensors, and remote diagnostic tools have revolutionized patient care. Yet, the integration of these technologies into medical environments introduces considerable security and privacy risks. Devices often lack end-to-end encryption or secure authentication mechanisms, creating potential vectors for unauthorized access to highly sensitive patient data. Talal et al. (2019) conducted a systematic review of smart home-based healthcare systems, revealing that the use of body sensors for real-time monitoring exposes critical health data to threats such as interception, manipulation, or unauthorized sharing. Similarly, Magara and Zhou (2024) emphasize that healthcare-focused IoT deployments are often inadequately secured due to prioritization of functionality and interoperability over privacy safeguards. These deficiencies can compromise not only patient confidentiality but also safety in scenarios involving dosage control or emergency response.

Smart home environments are increasingly equipped with IoT devices for automation, security, and energy management. However, their heterogeneous architecture and reliance on internet connectivity render them susceptible to a broad spectrum of cyber threats. Devices such as smart thermostats, lighting systems, and voice assistants often operate on outdated firmware with limited authentication protocols. Hammi et al. (2022) note that many consumer-grade smart home devices exhibit default credentials, unencrypted communications, and poorly protected APIs, making them ideal targets for botnets or eavesdropping. Additionally, Touqeer et al. (2021) provide a layer-wise analysis of smart home security, underscoring the vulnerability of application-layer interactions, particularly where user commands interface with connected appliances. The problem is compounded by weak physical security, allowing attackers to access network-connected devices directly within the home environment.

In industrial settings, IoT is the backbone of what is referred to as the Industrial Internet of Things (IIoT), enabling automation, predictive maintenance, and remote control of critical infrastructure. However, these capabilities also expand the attack surface and elevate the consequences of breaches. Umair et al. (2021) argue that IIoT deployments face distinct threats, such as industrial espionage, sabotage, and disruption of production systems. These threats often exploit outdated Supervisory Control and Data Acquisition (SCADA) systems or unsecured machine-to-machine communications. A successful breach in an industrial network can result in not only data loss but also operational downtime, equipment damage, or threats to worker safety. Given the high-value targets and critical nature of industrial assets, the absence of rigorous access control and intrusion detection mechanisms in IIoT deployments is particularly alarming.

The transportation sector has also embraced IoT for traffic management, vehicle telemetry, and intelligent transport systems. Connected cars, traffic signals, and logistics platforms now rely on real-time data exchange for efficient and safe operation. However, this dependence introduces unique challenges related to mobility, latency, and exposure to public networks. Chataut, Phoummalayvane and Akl (2023) highlight vulnerabilities in smart traffic systems, noting that sensor spoofing or packet injection attacks can disrupt traffic flow, cause accidents, or lead to gridlock. Meanwhile, Geneiatakis, Kounelis and Neisse (2017) examine how IoT-powered smart transportation systems often lack security baselines, leaving endpoints vulnerable to attacks such as signal hijacking or GPS spoofing.

These concerns are further echoed in broader studies of IoT application domains. Salma, Begum and Syed (2024) emphasize that the convergence of cyber and physical systems in all four sectors—healthcare, homes, industry, and transport—demands a unified yet domain-specific security framework that balances usability, performance, and privacy. Likewise, Lin and Bergmann (2016) suggest that privacy-by-

design principles and lifecycle-based threat modeling must be embedded into IoT design, particularly where long-term deployment and autonomous operation are anticipated.

Overall, the integration of IoT in healthcare, smart homes, industrial operations, and transportation presents sector-specific security risks that demand tailored mitigation strategies. Common issues include poor encryption, weak authentication, unpatched vulnerabilities, and inadequate privacy safeguards. As IoT adoption accelerates, it becomes imperative to prioritize security at the architectural level, enforce regulatory compliance, and promote awareness among stakeholders to ensure the resilience and trustworthiness of critical IoT systems.

2.4. Current Security Mechanisms and Frameworks.

The growing complexity of the Internet of Things (IoT) ecosystem has necessitated the evolution of robust security frameworks to safeguard data confidentiality, integrity, and availability. Given the resource-constrained nature of many IoT devices, traditional security models often prove inadequate, prompting the development of specialized solutions such as lightweight cryptographic algorithms, adaptive authentication protocols, intelligent intrusion detection systems (IDS), and blockchain-based architectures. This literature review critically examines these contemporary security mechanisms, highlighting their effectiveness and limitations within the context of IoT environments.

Cryptographic methods remain a foundational pillar of IoT security, providing mechanisms for data protection during storage and transmission. However, standard algorithms such as RSA and AES, while secure, are often computationally expensive for low-power devices. Consequently, research has increasingly turned to lightweight cryptography tailored to constrained environments. According to Kumar et al. (2019), algorithms such as PRESENT, HIGHT, and SPECK have shown promise in balancing security with resource efficiency. These algorithms are particularly relevant in wearable and sensor-based applications where energy and computational power are limited. Yet, lightweight encryption often trades off some degree of security robustness, making it essential to pair cryptography with complementary safeguards.

Authentication protocols have similarly evolved to meet the unique requirements of IoT. Traditional password-based schemes are vulnerable to various attacks, including replay and dictionary attacks, especially in ubiquitous and headless devices. Recent frameworks emphasize mutual authentication, wherein both devices and servers verify each other before any data exchange. A two-phase mutual authentication protocol combining Elliptic Curve Cryptography (ECC) with temporal credentials was proposed, demonstrating improved resistance to common threats while maintaining computational efficiency. Biometrics and physical unclonable functions (PUFs) are also gaining traction as authentication mechanisms due to their resistance to forgery. However, such systems are not without privacy concerns, as biometric data leakage may have long-term ramifications.

Intrusion detection systems play a crucial role in detecting abnormal behavior that may indicate cyberattacks. Given the dynamic and heterogeneous nature of IoT networks, signature-based IDS models are often insufficient. Anomaly-based IDS, leveraging machine learning and artificial intelligence, has gained prominence.

Blockchain technology represents a paradigm shift in securing IoT networks by offering decentralized, tamper-proof ledgers for data verification and transaction integrity. In contrast to centralized models, blockchain minimizes single points of failure and ensures transparency. Dorri et al. (2017) present a lightweight blockchain framework designed specifically for smart homes, which partitions the network into local and overlay ledgers, reducing latency and computational load. This structure enables secure device-to-device communication without relying on a trusted third party. However, scalability and energy consumption remain critical challenges, particularly in high-throughput IoT systems. To address this, research has focused on consensus mechanisms such as Proof-of-Authority (PoA) and Directed Acyclic Graphs (DAGs), which provide faster and more energy-efficient alternatives to traditional Proof-of-Work models (Da Xu et al., 2014).

Moreover, the integration of blockchain with other security layers shows promising synergies. For instance, combining blockchain with IDS can enhance traceability and accountability in threat detection, while blockchain-based authentication can eliminate reliance on centralized credential storage. Rehman et al. (2021) propose a hybrid model that merges blockchain with artificial intelligence-driven IDS to autonomously detect and log cyber threats across smart grid IoT networks. This approach not only improves system resilience but also ensures auditability and regulatory compliance.

Despite these advances, challenges persist in the implementation and standardization of security frameworks for IoT. The lack of uniform protocols and interoperability between vendors hinders the widespread adoption of advanced security mechanisms. Furthermore, real-world deployment often faces trade-offs between security, performance, and cost. It is thus essential for future research to focus on adaptive and context-aware security frameworks that dynamically adjust based on application requirements, threat intelligence, and environmental factors.

The current landscape of IoT security is characterized by a confluence of evolving technologies designed to address the specific constraints and threats endemic to IoT systems. Cryptographic techniques are being optimized for low-power environments, authentication protocols are increasingly incorporating context-aware and biometric elements, IDS are leveraging machine intelligence for proactive defense, and blockchain offers a decentralized paradigm for trust and integrity. While no single solution suffices, a layered

approach that integrates these mechanisms holds the most promise for securing the future of IoT.

2.5. Limitations of Existing Solutions: Critical assessment of the effectiveness, scalability, and practicality of current security mechanisms for constrained IoT devices.

The proliferation of the Internet of Things (IoT) has introduced new layers of complexity to cybersecurity, especially when considering resource-constrained devices that operate with limited computational, memory, and energy capacities. Although a multitude of security mechanisms have been proposed—including lightweight cryptography, authentication schemes, intrusion detection systems (IDS), and blockchain technologies—significant limitations persist in their effectiveness, scalability, and practicality. A critical analysis reveals that while existing solutions address certain facets of the security problem, they often fall short in real-world deployment due to systemic trade-offs inherent in constrained environments.

One of the most widely adopted classes of security solutions in IoT systems involves lightweight cryptographic algorithms. These are designed to provide encryption and integrity verification while minimizing resource consumption. However, even lightweight algorithms face challenges in balancing security and efficiency. According to Sadeghi, Wachsmann and Waidner (2015), while algorithms like PRESENT and HIGHT are optimized for low power, they offer a reduced security margin compared to conventional algorithms. As devices become more interconnected and threat actors more sophisticated, the reduced complexity of lightweight cryptographic primitives may become a liability rather than an advantage. Moreover, frequent key exchanges or updates required to maintain security incur processing overhead, which constrained devices struggle to support.

Authentication protocols tailored for IoT, including mutual and context-aware schemes, aim to ensure identity verification without burdening device resources. Nonetheless, their practical implementation is often flawed. Many authentication mechanisms assume pre-shared keys or rely on third-party certificate authorities—assumptions that do not hold in dynamic IoT networks with ad hoc connectivity. In large-scale deployments, managing keys for thousands of heterogeneous nodes becomes computationally expensive and error-prone. Furthermore, the memory limitations of edge devices restrict the implementation of complex authentication stacks, especially those involving biometric or multi-factor authentication, thus exposing devices to impersonation or replay attacks.

Intrusion Detection Systems (IDS), both signature-based and anomaly-based, represent another line of defense in IoT networks. While anomaly-based IDS can detect zero-day attacks through behavior profiling, they are often computationally intensive and suffer from high false-positive rates. Zhang, Deng and Li (2022) observe that while machine learning-based IDS frameworks are increasingly common, their training and inference processes require a computational and storage infrastructure that far exceeds the capabilities of embedded IoT devices. Edge-based IDSs that push decision-making to nearby gateways offer some mitigation, but this approach introduces latency and single points of failure, particularly in scenarios with unreliable connectivity or decentralized topologies.

Blockchain has been heralded as a transformative solution for IoT security due to its decentralization, immutability, and transparency. However, its practicality remains in question. Traditional consensus mechanisms such as Proof-of-Work are unsuitable for IoT because of their energy consumption and latency. Even lightweight adaptations, such as Proof-of-Authority or DAG-based models, introduce significant computational and bandwidth demands. Reyna et al. (2018) argue that although blockchain provides strong guarantees for data integrity and auditability, its integration with IoT remains nascent due to challenges in interoperability, scalability, and the real-time constraints of IoT applications. Synchronizing devices with blockchain ledgers also proves problematic in mobile or intermittent connectivity scenarios, which are common in rural or vehicular IoT deployments.

In addition to these technical constraints, there are practical and organizational issues that impede the effective deployment of security frameworks. One fundamental limitation is the absence of standardized protocols and interfaces across IoT platforms. As identified by Alaba et al. (2017), heterogeneity in hardware architectures and software stacks complicates the integration of security modules, often requiring custom development and maintenance. This lack of standardization not only increases development costs but also introduces vulnerabilities due to inconsistent security policies and patching practices.

Energy efficiency further exacerbates the tension between security and practicality. Security features like frequent data encryption, real-time IDS monitoring, and blockchain synchronization impose significant energy overheads, reducing battery life in portable and remote devices. In many IoT deployments—such as environmental sensors or medical implants—frequent recharging or battery replacement is infeasible. As a result, developers are forced to prioritize functionality over security, leaving systems exposed to known threats.

Scalability also remains a persistent issue. Security solutions that perform well in small, controlled testbeds often fail to scale effectively in dense, heterogeneous networks. For example, centralized access control models may become bottlenecks in large networks, while distributed models introduce synchronization challenges. According to Ammar et al. (2018), most current IoT security frameworks are not adequately stress-tested for scalability, leading to system failures or performance degradation in real-world deployments.

Moreover, many existing solutions do not account for usability and maintainability. Devices deployed in the field often lack user interfaces, making manual configuration or

software updates difficult. Remote update mechanisms, while theoretically valuable, are themselves attack vectors if not secured properly. Furthermore, the lack of skilled personnel capable of maintaining IoT security infrastructure presents a practical limitation for small- and medium-sized enterprises that increasingly adopt IoT technologies without the requisite cybersecurity capabilities (Roman, Zhou and Lopez, 2013).

While substantial progress has been made in developing IoT security mechanisms, current solutions frequently fall short of delivering a comprehensive, scalable, and practical defense for resource-constrained devices. Lightweight cryptography and specialized authentication protocols provide partial relief but are hampered by limitations in flexibility and scalability. Intrusion detection systems and blockchain-based frameworks hold promise but are often too resource-intensive for practical deployment. These limitations underscore the urgent need for adaptive, context-aware security models and the development of industry-wide standards to enable secure, scalable, and sustainable IoT ecosystems.

2.6. Comparative Studies and Benchmarking.

Comparative analyses and benchmarking are critical to understanding the capabilities, limitations, and operational trade-offs of various Internet of Things (IoT) security frameworks. These evaluations allow researchers and practitioners to make informed decisions regarding the suitability of particular security protocols or architectures for specific IoT contexts. While an array of frameworks exist, each designed with distinct assumptions and optimization goals, few achieve comprehensive security, scalability, and performance simultaneously. This literature review synthesises previous comparative studies, highlighting performance trade-offs, adoption challenges, and the current gaps in benchmarking methodology.

A foundational comparative survey was conducted by Ammar, Russello and Crispo (2018), who analysed eight major IoT frameworks, such as AllJoyn, Brillo, and IoTivity. Their study noted significant disparities in security implementations, with some frameworks lacking basic support for secure boot, encrypted communication, or remote attestation. A key insight from their work was that security functionalities are often sacrificed to optimize performance or reduce power consumption, particularly in resource-constrained environments. This trade-off leads to substantial variability in security assurance across frameworks, even within similar application domains.

In an effort to provide empirical benchmarks for evaluating security overheads, Almakhdhub and Clements (2019) introduced BenchIoT, a benchmarking framework focused on microcontroller-based IoT systems. BenchIoT evaluates various security mechanisms, including encryption and access control, on metrics such as memory usage, latency, and CPU cycles. Their experiments revealed that even lightweight cryptographic algorithms—while functionally efficient—can incur latency penalties when deployed at scale or under frequent transaction loads. This demonstrates the importance of holistic benchmarking that considers not only security effectiveness but also system performance and user experience.

Performance benchmarking also extends to intrusion detection systems (IDS). Ahmad et al. (2022) proposed a deep learning benchmark for IoT IDS, assessing classifiers such as CNNs, RNNs, and hybrid models based on detection accuracy, latency, and computational load. The results illustrated that although deep learning methods deliver high accuracy in detecting sophisticated threats, they are resource-intensive and often unsuitable for deployment on low-power edge devices. The authors concluded that model compression and edge-assisted inference are necessary adaptations for practical use, though these can in turn affect classification fidelity and robustness.

Comparative studies have also addressed the suitability of blockchain technologies in IoT security. Khalil et al. (2022) performed a comprehensive comparison between blockchain-based and centralized authentication frameworks in smart home environments. Their findings indicated that blockchain frameworks offer superior integrity and decentralization but come with high latency and computational demands that hinder their adoption in real-time systems. Conversely, centralized solutions, while offering better performance and simplicity, suffer from scalability limitations and pose single points of failure. This duality illustrates the central adoption challenge: balancing trust decentralization with operational efficiency.

In the context of IoT healthcare systems, Qahtan, Sharif and Zaidan (2022) developed a multi-criteria decision-making (MCDM) benchmarking framework that evaluates security mechanisms based on latency, privacy, scalability, and fault tolerance. The study compared blockchain-based, cloud-based, and hybrid architectures. Blockchain was rated highly on privacy and integrity but poorly on latency and energy consumption, highlighting its unsuitability for emergency or battery-constrained medical applications. This reinforces the notion that application-specific benchmarking is essential for accurate evaluation of security frameworks.

Other researchers have explored the comparative performance of operating systems (OS) that underpin security frameworks. Silva, Cerdeira and Pinto (2019) benchmarked low-end IoT OSs such as RIOT, Contiki, and FreeRTOS based on boot time, cryptographic support, memory footprint, and real-time responsiveness. The study found that while RIOT provided modular security capabilities, FreeRTOS exhibited better real-time performance with limited native security. These differences are non-trivial, as many security frameworks rely heavily on OS-level services for secure execution, communication, and device lifecycle management.

Despite the progress made, benchmarking efforts face several enduring challenges. Existing IoT security datasets used for evaluation are inconsistent in terms of format, volume, and representativeness. This lack of uniformity makes it difficult

to compare security frameworks across different studies reliably. Furthermore, most comparative analyses neglect the economic and organizational constraints that influence adoption, such as vendor interoperability, regulatory compliance, and user training.

A growing concern is that many benchmarking studies are carried out in simulated environments or controlled lab settings that fail to capture the dynamic and often unpredictable nature of real-world IoT deployments.

Comparative studies and benchmarking in IoT security have significantly advanced the understanding of performance trade-offs and operational challenges across different frameworks. While deep learning-based IDSs, blockchain architectures, and specialized cryptographic methods each offer unique benefits, their adoption remains constrained by limitations in latency, energy consumption, scalability, and practical deployment. Future research must aim to establish unified benchmarking methodologies that can accommodate the diversity and dynamism of IoT applications, thereby facilitating evidence-based framework selection and more secure global IoT adoption.

3. BENEFITS AND CHALLENGES

3.1. Benefits of Addressing IoT Security Proactively: Insights into how improved security enhances user trust, system resilience, and regulatory compliance.

The strategic importance of securing Internet of Things (IoT) systems has gained widespread recognition, particularly as IoT technologies become more deeply embedded in critical infrastructure, enterprise operations, and personal environments. Proactively addressing IoT security is not merely a technical imperative but a foundational element of long-term sustainability and user confidence. By implementing effective security measures at every stage of the IoT lifecycle, organisations can realise significant benefits, including enhanced user trust, improved system resilience, and strengthened regulatory compliance. A proactive approach to security offers not only risk mitigation but also competitive and operational advantages that underpin digital innovation.

A primary benefit of enhancing IoT security is the reinforcement of user trust. In a hyperconnected world where data is constantly collected, transmitted, and analysed, users are increasingly concerned about the privacy and security of their information. Trust is a prerequisite for adoption, especially in sectors such as healthcare, finance, and smart homes, where the sensitivity of data is high. When users perceive that an IoT system is secure—owing to robust encryption, transparent data handling practices, and secure authentication—they are more likely to engage with it and permit data sharing. Privacy-aware designs and privacy-by-default mechanisms can significantly influence consumer behaviour, making security a value proposition rather than a mere compliance obligation.

In addition to fostering user confidence, proactive security implementation strengthens system resilience. The distributed and autonomous nature of IoT devices makes them prime targets for cyberattacks that can disrupt functionality or corrupt data. Proactive measures such as device hardening, firmware integrity validation, intrusion detection, and continuous monitoring contribute to the robustness of the system. Resilient IoT systems are capable of withstanding or quickly recovering from malicious activities, thereby preserving the continuity of service and operational safety. In mission-critical applications such as industrial automation, intelligent transportation, and emergency services, such resilience can prevent catastrophic outcomes and ensure public safety.

Regulatory compliance is another key driver for adopting a proactive security stance in IoT deployments. National and regional regulations mandate stringent data protection measures and breach notification protocols. Non-compliance can result in significant financial penalties, reputational damage, and legal liabilities. Proactively integrating security into IoT architecture enables organisations to meet these compliance obligations efficiently, thereby reducing the risk of sanctions while improving audit readiness. Moreover, embedding compliance into technical design processes—such as through security-by-design and risk assessment frameworks—supports long-term governance and accountability.

Beyond these core benefits, proactively securing IoT systems creates opportunities for innovation and differentiation. Organisations that prioritise security are better positioned to introduce new features, expand product ecosystems, and engage in cross-industry collaborations. Secure-by-design principles not only enable seamless integration with third-party platforms but also foster trust-based partnerships, thereby accelerating time-to-market and scaling potential. In the competitive technology market, a reputation for secure and privacy-conscious products can serve as a strategic advantage, enhancing brand loyalty and customer retention.

However, realising these benefits is not without challenges. One of the foremost obstacles is the inherent trade-off between security and resource efficiency. Many IoT devices are designed for low power consumption and minimal hardware capabilities, making it difficult to implement strong cryptographic algorithms or real-time security monitoring. Lightweight alternatives, while essential, may offer reduced security guarantees and limited adaptability to evolving threats. This limitation is particularly pronounced in legacy devices, which often lack the capability for secure firmware updates or remote patching.

Another critical challenge is the lack of standardisation across IoT platforms, which hinders the consistent implementation of security protocols. The heterogeneity of device manufacturers, communication protocols, and application frameworks results in fragmented security practices and interoperability issues. Insecure interfaces, proprietary

encryption schemes, and incompatible update mechanisms can create vulnerabilities that are difficult to detect and easy to exploit. The absence of global security benchmarks further complicates efforts to create universally secure IoT ecosystems.

Additionally, the economic burden associated with securing IoT systems cannot be ignored. The cost of implementing comprehensive security measures—from secure hardware modules and authentication tokens to continuous vulnerability assessments and compliance audits—can be prohibitive, especially for small and medium-sized enterprises. Balancing cost-effectiveness with robust security often necessitates strategic prioritisation and phased implementation plans, which may delay full protection or leave critical components exposed in the interim.

Human factors also present a substantial barrier to effective security. Poor user practices such as weak password usage, delayed software updates, and unverified device integration remain common across consumer and enterprise settings. Additionally, limited cybersecurity literacy among users and administrators increases the likelihood of misconfiguration, which can create attack surfaces even in technically secure systems. Overcoming these challenges requires not only technical interventions but also comprehensive awareness programmes and user-centric security designs.

Proactively addressing IoT security challenges offers significant advantages in terms of user trust, system resilience, and regulatory compliance. These benefits, in turn, support technological innovation, operational stability, and long-term competitiveness. Nevertheless, organisations must navigate practical obstacles including device constraints, standardisation gaps, financial limitations, and human factors. Future efforts should focus on the development of scalable, interoperable, and context-aware security solutions that can be integrated seamlessly into diverse IoT environments. By embedding security into the core design philosophy and operational framework of IoT systems, stakeholders can ensure a safer, more trustworthy digital future.

3.2. Key Barriers to IoT Security Implementation: Identification of challenges such as limited processing power, cost constraints, lack of standardization, and fragmented device ecosystems.

The implementation of robust security mechanisms in the Internet of Things (IoT) remains a formidable challenge, primarily due to inherent constraints such as limited processing power, financial limitations, lack of standardization, and a fragmented device ecosystem. As the IoT landscape continues to expand, these challenges persistently hinder the adoption of scalable and comprehensive security frameworks, despite their critical necessity in safeguarding interconnected devices.

One of the most pervasive limitations lies in the computational constraints of IoT devices. Many embedded systems within the IoT architecture are designed for energy efficiency and cost-effectiveness, often at the expense of processing capacity. This trade-off complicates the implementation of encryption algorithms and security protocols that are computationally intensive. Keoh and Kumar (2014) stress that constrained devices lack the capacity to implement traditional security stacks, forcing designers to either simplify protocols or accept reduced protection levels (Keoh and Kumar, 2014).

Cost is another significant impediment to widespread IoT security implementation. Particularly in large-scale deployments involving thousands of devices, incorporating advanced security modules such as Trusted Platform Modules (TPMs) or hardware-based encryption can be prohibitively expensive. Mittal (2024) identifies financial limitations as a recurring justification for the minimal security standards adopted in consumer-grade IoT products, which increases vulnerability to emerging threats (Mittal, 2024).

Furthermore, the absence of a universally accepted standard across IoT ecosystems exacerbates the complexity of securing devices. Although numerous standardization bodies—such as IEEE, ETSI, and IETF—have introduced frameworks for IoT security, their coexistence without alignment leads to interoperability issues. Saleem et al. (2018) highlight how this plurality of standards results in fragmented adoption across industries and jurisdictions, obstructing the establishment of baseline security practices (Saleem et al., 2018). Similarly, Samaila, Neto, and Fernandes (2018) note that the lack of uniform security protocols results in vendors implementing proprietary and often insufficient protections (Samaila et al., 2018).

The fragmentation of the IoT device ecosystem further complicates these issues. Devices within the same environment often differ significantly in terms of architecture, communication protocols, and firmware capabilities. Aly, Khomh, and Guéhéneuc (2018) argue that this heterogeneity undermines cohesive security strategies, as uniform protection cannot be enforced across diverse hardware platforms and network configurations (Aly et al., 2018). Kolluru and Mungara (2019) further reinforce this argument, stating that the absence of interoperability leads to inconsistent security implementations, which attackers can exploit to gain access through the weakest links (Kolluru and Mungara, 2019).

Efforts to mitigate these challenges are underway but remain fragmented. Szczepaniuk and Szczepaniuk (2022) explore existing solutions to ecosystem standardization, such as adopting open platforms and harmonized APIs. However, these measures are still in early stages and face resistance from vendors prioritizing market differentiation over compatibility (Szczepaniuk and Szczepaniuk, 2022).

In the industrial domain, the situation is similarly complex. Mumtaz et al. (2017) analyze challenges in wireless Industrial IoT (IIoT) networks, emphasizing that the absence of human intervention exacerbates the consequences of security lapses. With critical infrastructures at stake, the fragmented

implementation of secure connectivity standards poses a serious risk to operational continuity (Mumtaz et al., 2017).

The benefits of IoT adoption—enhanced automation, predictive maintenance, and optimized resource utilization—are undermined when foundational security mechanisms are either lacking or inconsistently applied. Vermesan and Friess (2015) contend that the realization of a hyperconnected society is contingent on solving these core security issues. Their work underscores that without coordinated innovation and governance, security in IoT remains reactive and fragmented (Vermesan and Friess, 2015).

While IoT offers transformative capabilities across sectors, its promise is tempered by profound security challenges. Limited device processing power constrains the deployment of robust cryptographic solutions, while cost sensitivities restrict the use of secure hardware. The lack of standardization impairs interoperability and increases system complexity, and the fragmented ecosystem exacerbates vulnerabilities. Addressing these barriers requires a unified approach involving regulatory mandates, vendor collaboration, and the adoption of lightweight yet effective security models tailored for resource-constrained environments. Only then can the full potential of the IoT be realized with security that is both scalable and sustainable.

3.3. Strategic Recommendations: Proposed strategies for more effective IoT security including layered defenses, AI-based threat detection, and global policy frameworks.

A strategic approach to Internet of Things (IoT) security must encompass both technological innovation and coordinated policy development. As IoT ecosystems expand rapidly in scale and complexity, securing them effectively requires a blend of layered defense architectures, artificial intelligence (AI)-driven threat detection, and globally harmonized policy frameworks. These components serve not only as technical enablers but also as strategic imperatives to sustain trust and resilience in increasingly autonomous and interconnected environments.

Layered security, or defense-in-depth, represents a foundational principle in contemporary IoT protection strategies. This approach involves implementing multiple security controls across different layers of the IoT architecture, such as the physical, network, and application layers. Rao et al. (2024) demonstrate that layered defense mechanisms can mitigate risks by isolating threats at their point of origin, thereby preventing lateral movement across devices and domains. Their research emphasizes the integration of intrusion detection systems at the network layer, coupled with access control and encryption protocols at the application level (Rao et al., 2024).

Artificial intelligence has become a vital asset in augmenting IoT security, particularly for detecting novel and evolving threats. AI-based solutions can analyze vast volumes of heterogeneous data generated by IoT devices, identify patterns indicative of intrusions, and respond in near real-time. Gopalsamy (2020) outlines various AI-driven models—ranging from deep learning classifiers to clustering algorithms—for botnet detection within IoT environments. These tools provide a scalable means of addressing security challenges that traditional rule-based systems struggle to manage effectively (Gopalsamy, 2020).

Recent studies have further refined these methods by embedding AI at different layers of the IoT stack. HaddadPajouh et al. (2020) propose the AI4SAFE-IoT architecture, which utilizes AI to monitor edge devices, detect anomalies, and implement preventive controls in a distributed manner. This edge-centric model significantly reduces latency and supports proactive threat mitigation in real time (HaddadPajouh et al., 2020). Similarly, Zaman et al. (2021) present a taxonomy of AI-based countermeasures tailored to specific layers of the IoT infrastructure, illustrating that a modular approach enhances both detection accuracy and system adaptability (Zaman et al., 2021).

However, the proliferation of AI in security also necessitates governance structures to ensure its safe and ethical application. This leads to the third strategic dimension: global policy frameworks. McCall (2024) underscores that without standardized regulations, inconsistent practices among manufacturers and service providers result in systemic vulnerabilities that attackers can exploit. A unified policy framework would harmonize compliance requirements, facilitate cross-border threat intelligence sharing, and incentivize adherence to secure-by-design principles (McCall, 2024).

The role of explainable AI (XAI) in policy formation and security operations is also gaining traction. Quincozes et al. (2024) argue that incorporating interpretability into AI models not only builds trust among stakeholders but also aids regulators in validating compliance and understanding system behavior during security audits (Quincozes et al., 2024). This is especially relevant in high-risk sectors such as healthcare and critical infrastructure, where opaque AI decisions could have significant legal and ethical consequences.

Furthermore, integrating AI with secure hardware and edge computing strategies is increasingly recommended. Humayun et al. (2024) emphasize that combining secure chip design with intelligent firmware monitoring adds another layer of protection against physical tampering and firmware-based exploits. This integration supports the broader principle of zero-trust architecture, ensuring that trust is never implicit and always verified across the system lifecycle (Humayun et al., 2024).

Strategic innovation must be complemented by long-term coordination among international agencies. Khan, Abdullah, and Olajide (2024) advocate for AI-blockchain convergence as a promising model for tamper-proof auditing and decentralized identity management. These technologies can underpin future global security standards by offering both transparency and scalability (Khan et al., 2024).

Enhancing IoT security demands a holistic strategy that bridges technological and policy domains. Layered defense architectures provide resilience against multi-vector attacks, while AI offers adaptive capabilities for real-time threat detection. Yet, these innovations must be governed by global frameworks to ensure interoperability, ethical compliance, and systemic security. A coordinated investment in these areas will be critical to secure the next generation of connected environments.

4. FUTURE DIRECTIONS

4.1. Emerging Trends in IoT Security Research.

As the Internet of Things (IoT) evolves into a foundational component of the global digital infrastructure, the landscape of security research must likewise shift toward proactive and future-ready technologies. Traditional security paradigms are increasingly inadequate in the face of quantum threats, decentralized processing demands, and privacy-preserving requirements. Consequently, emerging directions in IoT security are focused on quantum-safe cryptography, edge-based security models, and federated learning for threat detection—each offering transformative potential to address imminent risks and resilience challenges.

Quantum-safe cryptography, also known as post-quantum cryptography (PQC), has gained prominence due to the anticipated capabilities of quantum computing to break conventional public-key algorithms. Dhinakaran, Srinivasan and Sankar (2024) argue that existing encryption schemes, such as RSA and ECC, will be rendered obsolete in a post-quantum world, emphasizing the urgency for adopting quantum-resistant alternatives. Their study explores lattice-based and hash-based cryptographic systems, which exhibit strong resistance to Shor's algorithm and are increasingly considered foundational to next-generation IoT security protocols (Dhinakaran et al., 2024).

The significance of PQC is not merely theoretical. Elkhodr (2025) presents a model that combines quantum-safe cryptography with blockchain and AI-based anomaly detection, ensuring both data integrity and forward secrecy. By embedding such cryptographic primitives within distributed ledgers, IoT systems can enforce tamper-evident and resilient security structures, even in quantum-capable threat environments (Elkhodr, 2025).

Parallel to cryptographic evolution is the shift toward edge-based security models. These architectures decentralize the analysis and enforcement of security policies, relocating computation from centralized cloud systems to the edge of the network—closer to the IoT devices themselves. Ajayi and Masunda (2025) detail the strategic benefit of this model, noting that it minimizes latency, reduces data exposure during transmission, and enables real-time threat mitigation. Their framework integrates edge computing with AI-driven behavioral analysis to autonomously detect and respond to suspicious activity at the device level (Ajayi and Masunda, 2025).

Edge-centric models also align with privacy regulations and ethical imperatives, as they enable data processing without offloading sensitive information to external servers. Nguyen, Nguyen and Hwang (2025) emphasize that edge-based architectures provide the necessary scaffolding to support emerging intelligent services, such as digital twins and adversarial threat simulations in 6G-enabled IoT environments (Nguyen et al., 2025).

Complementing these advances is the adoption of federated learning (FL), a distributed machine learning paradigm that enables the collaborative training of AI models across decentralized devices while retaining local data privacy. Javeed et al. (2024) present a federated architecture integrated with quantum principles to facilitate secure learning across IoT devices. Their framework reduces the risk of data breaches, supports differential privacy, and enables adaptive model updates in real-time without requiring data centralization (Javeed et al., 2024).

The integration of federated learning with edge and quantum technologies is further elaborated by Shindagi, Koppad and Ekbote (2025), who argue that such convergence is essential for secure and scalable IoT networks in the 6G era. Their proposed architecture leverages local model updates combined with blockchain-based authentication to ensure integrity and trustworthiness across devices operating under diverse administrative domains (Shindagi et al., 2025).

Hakeem and Kim (2025) expand on the application of FL in vehicular IoT (V2X), highlighting its role in intrusion detection and anomaly detection in dynamic, high-mobility environments. Their survey identifies FL as a pivotal enabler of secure, low-latency decision-making in autonomous transportation systems, underlining its potential to become a universal security standard for next-generation smart infrastructures (Hakeem and Kim, 2025).

As these emerging technologies mature, their convergence is expected to redefine IoT security frameworks. The vision is a comprehensive system wherein data remains private, decisions are locally optimized, and encryption remains impervious to future quantum capabilities. Alejandra and Elena (2025) conclude that only by unifying these technologies—PQC, edge intelligence, and FL—can we construct privacy-preserving, resilient, and intelligent cyber-physical ecosystems capable of sustaining trust in an increasingly decentralized world (Alejandra and Elena, 2025).

In summary, the future of IoT security is poised for a paradigm shift driven by quantum-safe encryption, distributed processing, and federated intelligence. Each of these innovations addresses critical vulnerabilities that have historically plagued IoT deployments, offering scalable and sustainable solutions for a hyperconnected future. Research and policy must co-evolve to support these technologies, ensuring their integration adheres to rigorous ethical and technical standards while remaining adaptive to evolving threat landscapes.

4.2. Research Gaps and Innovation Opportunities.

As the Internet of Things (IoT) continues to expand in scale, diversity, and criticality, the research community must respond with new paradigms for securing increasingly autonomous, heterogeneous, and interconnected ecosystems. Despite the proliferation of existing IoT security frameworks, considerable research gaps remain in three key areas: autonomous threat response, lightweight security protocols suitable for constrained devices, and the alignment of technical mechanisms with legal and regulatory mandates. These gaps represent substantial innovation opportunities with profound implications for the resilience and governance of IoT systems.

Autonomous threat response systems are an emerging domain where research is still in its infancy. While intrusion detection and anomaly recognition have benefitted from advancements in machine learning, the challenge of autonomously mitigating threats without human intervention persists. Existing systems, such as signature-based firewalls or behavioral monitors, largely rely on predefined responses or alert escalation rather than real-time, adaptive containment strategies. The development of autonomous response frameworks must integrate threat classification with contextual understanding to avoid overreactions or false positives, which could otherwise disrupt legitimate IoT functions. Moreover, as Baig et al. (2017) point out, the latency and processing constraints of many IoT nodes make it impractical to implement traditional endpoint protection mechanisms. These limitations necessitate a new generation of lightweight autonomous agents capable of executing decentralized mitigation strategies based on localized inference and minimal resource overhead.

Parallel to this challenge is the pressing need for lightweight security protocols optimized for resource-constrained environments. Many IoT devices operate on microcontrollers with limited computational, memory, and energy resources, rendering them incapable of handling conventional cryptographic algorithms such as AES-256 or RSA-2048. The emergence of lightweight cryptography offers promising alternatives including PRESENT, SPECK, and Simon ciphers, which significantly reduce processing demands. However, further research is required to validate their robustness in multi-vector threat environments.

Further complicating the technological landscape is the misalignment between legal frameworks and security engineering practices. Regulatory regimes such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) impose strict data protection obligations, yet offer limited guidance on how technical architectures can ensure compliance. This discrepancy has led to what Gellert (2018) refers to as a "compliance gap," where system designers face ambiguity in translating legal concepts such as "data minimization" or "privacy by design" into concrete technical implementations. Similarly, Weber (2010) emphasizes that many legal systems are reactive, only addressing security failures after the fact rather than mandating proactive engineering practices. This legal-technical divide is particularly problematic for cross-border IoT services, where jurisdictional fragmentation undermines the enforceability of uniform standards. There is thus a critical need for interdisciplinary research that translates regulatory language into actionable design principles and promotes regulatory sandboxes for testing compliance-by-construction approaches.

Innovation in these domains cannot occur in silos. Effective advancement requires a convergence of cybersecurity engineering, legal scholarship, human-computer interaction, and systems design. For instance, embedding explainable AI (XAI) into autonomous response mechanisms not only enhances transparency but also aids regulatory audits and liability assessments. Furthermore, research into privacy-preserving data aggregation—using techniques such as homomorphic encryption or secure multiparty computation—can contribute to both lightweight security and legal compliance. These integrated solutions must also be evaluated in real-world scenarios, ideally through testbeds and digital twins that model complex interactions between devices, users, and institutional policies.

The future of IoT security depends on the capacity to proactively innovate within these identified gaps. Autonomous systems must evolve from reactive firewalls to context-aware agents; cryptographic protocols must be re-engineered for ultra-low-power devices; and legal norms must be embedded directly into the codebases of IoT platforms. Until these challenges are systematically addressed, the security and trustworthiness of IoT ecosystems will remain vulnerable to both technical exploits and regulatory breaches. As IoT devices become embedded in public infrastructure, health systems, and critical services, bridging these research gaps becomes not just a technical ambition but a societal imperative.

CONCLUSION

The integration of the Internet of Things (IoT) into virtually every sector has brought about substantial advancements in connectivity, efficiency, and automation. However, with this progress comes a commensurate escalation in security challenges that must be addressed with strategic foresight and robust technological innovation. This paper has examined the comparative strengths and limitations of existing IoT security frameworks, identified key implementation barriers, proposed strategic approaches for enhancement, and highlighted emerging technologies and research opportunities that hold promise for the future of IoT security.

Comparative analysis of security frameworks revealed that no singular solution comprehensively addresses all IoT security needs. Each framework offers a unique balance of performance, usability, scalability, and implementation complexity. Performance trade-offs, particularly in latency-sensitive environments, and organizational resistance to

adoption due to cost or technical expertise deficits remain significant barriers. Moreover, fragmented device ecosystems and lack of unified standards hinder cohesive security implementations, leading to uneven protections and exploitable vulnerabilities across networks.

The challenges identified in implementing IoT security mechanisms underscore the practical limitations of deploying effective protections in constrained environments. Limited processing power and memory on endpoint devices restrict the use of traditional cryptographic schemes, while cost considerations deter widespread deployment of more advanced or redundant security measures. Additionally, the diversity of device manufacturers and the absence of universally accepted standards amplify system incompatibility, making scalable and reliable security architectures elusive.

Despite these constraints, several strategies have been proposed to enhance IoT security. The deployment of layered defense architectures provides resilience by establishing multiple security perimeters that mitigate threats at various levels of the IoT stack. Coupled with artificial intelligence-based threat detection, these layered systems can dynamically adapt to new threats, leveraging real-time analytics to improve incident response. AI also facilitates early detection and behavioral anomaly recognition, offering proactive rather than reactive defense capabilities. On a broader scale, the creation of global policy frameworks could align security practices, standardize compliance expectations, and foster greater international cooperation in addressing cross-border cyber threats.

Looking ahead, future security developments in the IoT domain will likely be defined by the adoption of cutting-edge technologies and deeper integration of legal and ethical considerations. Innovations such as quantum-safe cryptography, edge-based processing for localized security enforcement, and federated learning models for decentralized data analysis are poised to reshape the IoT threat landscape. These technologies not only strengthen security but also preserve user privacy and data integrity in increasingly decentralized systems. Simultaneously, aligning technical implementations with evolving legal requirements will be essential to ensure compliance and accountability in the global IoT ecosystem.

Significant research gaps remain that must be bridged to achieve a secure and trustworthy IoT environment. Autonomous threat response, capable of acting in real time without human intervention, is still underdeveloped and must be pursued with caution and precision. Lightweight security protocols, essential for constrained devices, require further validation and standardization before widespread adoption is feasible. Lastly, the persistent disconnect between regulatory frameworks and technical practices calls for interdisciplinary collaboration to develop actionable guidelines that are both legally compliant and technically feasible.

Securing the IoT is not solely a technical endeavor but a multidimensional challenge requiring a confluence of engineering, policy, and human factors. As IoT systems become more pervasive and embedded in critical infrastructure, the urgency for resilient, scalable, and ethically grounded security solutions grows exponentially. Future progress will depend not only on technological ingenuity but also on our capacity to harmonize innovation with legal standards and societal expectations. By addressing current gaps and pursuing collaborative, forward-looking research, stakeholders across academia, industry, and government can collectively fortify the security foundations of the next-generation connected world.

REFERENCES

1. Ahmad, R., Alsmadi, I., Alhamdani, W. and Tawalbeh, L.A., 2022. A comprehensive deep learning benchmark for IoT IDS. *Computers & Security*, *114*, p.102588.
2. Ajayi, R. and Masunda, M., 2025. Integrating edge computing, data science and advanced cyber defense for autonomous threat mitigation.
3. Alaba, F.A., Othman, M., Hashem, I.A.T. and Alotaibi, F., 2017. Internet of Things security: A survey. *Journal of Network and Computer Applications*, *88*, pp.10-28. https://doi.org/10.1016/j.jnca.2017.04.002
4. Alejandra, R. and Elena, P., 2025. PRIVACY-PRESERVING AI MODELS FOR CLOUD AND EDGE COMPUTING SECURITY. *Synergy: Cross-Disciplinary Journal of Digital Investigation*, *3*(3), pp.1-19.
5. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M. and Ayyash, M., 2015. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE communications surveys & tutorials*, *17*(4), pp.2347-2376. https://doi.org/10.1109/COMST.2015.2444095
6. Almakhdhub, N.S., Clements, A.A., Payer, M. and Bagchi, S., 2019, June. Benchiot: A security benchmark for the internet of things. In *2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)* (pp. 234-246). IEEE.
7. Alrawais, A., Alhothaily, A., Hu, C. and Cheng, X., 2017. Fog computing for the internet of things: Security and privacy issues. *IEEE Internet Computing*, *21*(2), pp.34-42. https://doi.org/10.1109/MIC.2017.37
8. Aly, M., Khomh, F., Guéhéneuc, Y.G., Washizaki, H. and Yacout, S., 2018. Is Fragmentation a Threat to the Success of the Internet of Things?. *IEEE Internet of Things Journal*, *6*(1), pp.472-487.
9. Ammar, M., Russello, G. and Crispo, B., 2018. Internet of Things: A survey on the security of IoT

frameworks. *Journal of information security and Applications*, *38*, pp.8-27. https://doi.org/10.1016/j.jisa.2017.11.002

10. Babun, L., Denney, K., Celik, Z.B., McDaniel, P. and Uluagac, A.S., 2021. A survey on IoT platforms: Communication, security, and privacy perspectives. *Computer Networks*, *192*, p.108040.
11. Baig, Z.A., Szewczyk, P., Valli, C., Rabadia, P., Hannay, P., Chernyshev, M., Johnstone, M., Kerai, P., Ibrahim, A., Sansurooah, K. and Syed, N., 2017. Future challenges for smart cities: Cyber-security and digital forensics. *Digital Investigation*, *22*, pp.3-13. https://doi.org/10.1016/j.diin.2017.06.009
12. Chataut, R., Phoummalayvane, A. and Akl, R., 2023. Unleashing the power of IoT: A comprehensive review of IoT applications and future prospects in healthcare, agriculture, smart homes, smart cities, and industry 4.0. *Sensors*, *23*(16), p.7194.
13. Chaudhary, S. and Mishra, P.K., 2023. DDoS attacks in Industrial IoT: A survey. *Computer Networks*, *236*, p.110015.
14. Chiang, M. and Zhang, T., 2016. Fog and IoT: An overview of research opportunities. *IEEE Internet of things journal*, *3*(6), pp.854-864. https://doi.org/10.1109/JIOT.2016.2584538
15. Da Xu, L., He, W. and Li, S., 2014. Internet of things in industries: A survey. *IEEE Transactions on industrial informatics*, *10*(4), pp.2233-2243. https://doi.org/10.1109/TII.2014.2300753
16. Dhinakaran, D., Srinivasan, L., Sankar, S.U. and Selvaraj, D., 2024. Quantum-based privacy-preserving techniques for secure and trustworthy internet of medical things an extensive analysis. *Quantum Inf. Comput.*, *24*(3&4), pp.227-266.
17. Dorri, A., Kanhere, S.S. and Jurdak, R., 2017, April. Towards an optimized blockchain for IoT. In *Proceedings of the second international conference on Internet-of-Things design and implementation* (pp. 173-178). https://doi.org/10.1145/3054977.3055003
18. Elkhodr, M., 2025. An AI-Driven Framework for Integrated Security and Privacy in Internet of Things Using Quantum-Resistant Blockchain. *Future Internet*, *17*(6), p.246.
19. Fernandes, E., Paupore, J., Rahmati, A., Simionato, D., Conti, M. and Prakash, A., 2016. {FlowFence}: Practical data protection for emerging {IoT} application frameworks. In *25th USENIX security symposium (USENIX Security 16)* (pp. 531-548).
20. Gellert, R., 2018. Understanding the notion of risk in the General Data Protection Regulation. *Computer Law & Security Review*, *34*(2), pp.279-288. https://doi.org/10.1016/j.clsr.2019.105367
21. Geneiatakis, D., Kounelis, I., Neisse, R., Nai-Fovino, I., Steri, G. and Baldini, G., 2017, May. Security and privacy issues for an IoT based smart home. In *2017 40th international convention on information and communication technology, electronics and microelectronics (MIPRO)* (pp. 1292-1297). IEEE.
22. Gopalsamy, M., 2020. Artificial Intelligence (AI) Based Internet-of-Things (IoT)-Botnet Attacks Identification Techniques to Enhance Cyber security. *International Journal of Research and Analytical Reviews (IJRAR)*, *7*(4), pp.414-420.
23. Gubbi, J., Buyya, R., Marusic, S. and Palaniswami, M., 2013. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future generation computer systems*, *29*(7), pp.1645-1660. https://doi.org/10.1016/j.future.2013.01.010
24. HaddadPajouh, H., Dehghantanha, A., Parizi, R.M., Aledhari, M. and Karimipour, H., 2021. A survey on internet of things security: Requirements, challenges, and solutions. *Internet of Things*, *14*, p.100129.
25. HaddadPajouh, H., Khayami, R., Dehghantanha, A., Choo, K.K.R. and Parizi, R.M., 2020. AI4SAFE-IoT: An AI-powered secure architecture for edge layer of Internet of things. *Neural Computing and Applications*, *32*(20), pp.16119-16133.
26. Hakeem, S.A.A. and Kim, H., 2025. Advancing Intrusion Detection in V2X Networks: A Comprehensive Survey on Machine Learning, Federated Learning, and Edge AI for V2X Security. *IEEE Transactions on Intelligent Transportation Systems*.
27. Hammi, B., Zeadally, S., Khatoun, R. and Nebhen, J., 2022. Survey on smart homes: Vulnerabilities, risks, and countermeasures. *Computers & Security*, *117*, p.102677.
28. Hintaw, A.J., Manickam, S., Aboalmaaly, M.F. and Karuppayah, S., 2023. MQTT vulnerabilities, attack vectors and solutions in the internet of things (IoT). *IETE Journal of Research*, *69*(6), pp.3368-3397.
29. Hossain, M.M., Fotouhi, M. and Hasan, R., 2015, June. Towards an analysis of security issues, challenges, and open problems in the internet of things. In *2015 ieee world congress on services* (pp. 21-28). IEEE. https://doi.org/10.1109/SERVICES.2015.12
30. Hulayyil, S.B., Li, S. and Xu, L., 2023. Machine-learning-based vulnerability detection and classification in internet of things device security. *Electronics*, *12*(18), p.3927.
31. Humayun, M., Tariq, N., Alfayad, M., Zakwan, M., Alwakid, G. and Assiri, M., 2024. Securing the Internet of Things in artificial intelligence era: A

comprehensive survey. *IEEE access*, *12*, pp.25469-25490.

32. Islam, S.R., Kwak, D., Kabir, M.H., Hossain, M. and Kwak, K.S., 2015. The internet of things for health care: a comprehensive survey. *IEEE access*, *3*, pp.678-708. https://doi.org/10.1109/ACCESS.2015.2437951
33. Javeed, D., Saeed, M.S., Ahmad, I., Adil, M., Kumar, P. and Islam, A.N., 2024. Quantum-empowered federated learning and 6G wireless networks for IoT security: Concept, challenges and future directions. *Future Generation Computer Systems*.
34. Jayalaxmi, P., Saha, R., Kumar, G., Kumar, N. and Kim, T.H., 2021. A taxonomy of security issues in Industrial Internet-of-Things: Scoping review for existing solutions, future implications, and research challenges. *IEEE Access*, *9*, pp.25344-25359.
35. Keoh, S.L., Kumar, S.S. and Tschofenig, H., 2014. Securing the internet of things: A standardization perspective. *IEEE Internet of things Journal*, *1*(3), pp.265-275.
36. Khalil, U., Malik, O.A., Uddin, M. and Chen, C.L., 2022. A comparative analysis on blockchain versus centralized authentication architectures for IoT-enabled smart devices in smart cities: a comprehensive review, recent advances, and future research directions. *Sensors*, *22*(14), p.5168.
37. Khan, O.U., Abdullah, S.M., Olajide, A.O., Sani, A.I., Faisal, S.M.W., Ogunola, A.A. and Lee, M.D., 2024. The Future of Cybersecurity: Leveraging Artificial Intelligence to Combat Evolving Threats and Enhance Digital Defense Strategies. *Journal of Computational Analysis and Applications*, *33*(8).
38. Kolluru, V., Mungara, S. and Chintakunta, A.N., 2019. Securing the IoT ecosystem: Challenges and innovations in smart device cybersecurity. *International Journal on Cryptography and Information Security*, *9*(2), pp.10-5121.
39. Kumar, S., Tiwari, P. and Zymbler, M., 2019. Internet of Things is a revolutionary approach for future technology enhancement: a review. *Journal of Big data*, *6*(1), pp.1-21. https://doi.org/10.1186/s40537-019-0268-2
40. Lin, H. and Bergmann, N.W., 2016. IoT privacy and security challenges for smart home environments. *Information*, *7*(3), p.44.
41. Magara, T. and Zhou, Y., 2024. Internet of things (IoT) of smart homes: privacy and security. *Journal of Electrical and Computer Engineering*, *2024*(1), p.7716956.
42. Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R.P. and Ni, W., 2018. Anatomy of threats to the internet of things. *IEEE communications surveys & tutorials*, *21*(2), pp.1636-1675.
43. Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R.P. and Ni, W., 2018. Anatomy of threats to the internet of things. *IEEE communications surveys & tutorials*, *21*(2), pp.1636-1675.
44. Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J. and Aharon, D., 2015. The Internet of Things: Mapping the value beyond the hype.
45. Mazhar, N., Salleh, R., Zeeshan, M. and Hameed, M.M., 2021. Role of device identification and manufacturer usage description in iot security: A survey. *Ieee Access*, *9*, pp.41757-41786.
46. McCall, A., 2024. Cybersecurity in the Age of AI and IoT: Emerging Threats and Defense Strategies.
47. Mittal, C., 2024. Obstacles and countermeasures for protecting Internet of Things devices from emerging security risks. *Cyber Security: A Peer-Reviewed Journal*, *8*(1), pp.48-62.
48. Mudgerikar, A. and Bertino, E., 2021. Iot attacks and malware. *Cyber Security Meets Machine Learning*, pp.1-25.
49. Mumtaz, S., Alsohaily, A., Pang, Z., Rayes, A., Tsang, K.F. and Rodriguez, J., 2017. Massive Internet of Things for industrial applications: Addressing wireless IIoT connectivity challenges and ecosystem fragmentation. *IEEE industrial electronics magazine*, *11*(1), pp.28-33.
50. Nguyen, V.L., Nguyen, L.H., Hwang, R.H., Canberk, B. and Duong, T.Q., 2025. Quantum Machine Learning for 6G Network Intelligence and Adversarial Threats. *IEEE Communications Standards Magazine*.
51. Patel, N.D. and Singh, A., 2023. Security Issues, Attacks and Countermeasures in Layered IoT Ecosystem. *International Journal of Next-Generation Computing*, *14*(2).
52. Pham, D.P., 2022. *Leveraging side-channel signals for IoT malware classification and rootkit detection* (Doctoral dissertation, Université Rennes 1).
53. Qahtan, S., Sharif, K.Y., Zaidan, A.A., AlSattar, H.A., Albahri, O.S., Zaidan, B.B., Zulzalil, H., Osman, M.H., Alamoodi, A.H. and Mohammed, R.T., 2022. Novel multi security and privacy benchmarking framework for blockchain-based IoT healthcare industry 4.0 systems. *IEEE Transactions on Industrial Informatics*, *18*(9), pp.6415-6423.
54. Quincozes, V.E., Quincozes, S.E., Kazienko, J.F., Gama, S., Cheikhrouhou, O. and Koubaa, A., 2024. A survey on IoT application layer protocols, security challenges, and the role of explainable AI in IoT (XAIoT). *International Journal of Information Security*, *23*(3), pp.1975-2002.

55. Rao, D.D., Waoo, A.A., Singh, M.P., Pareek, P.K., Kamal, S. and Pandit, S.V., 2024. Strategizing IoT network layer security through advanced intrusion detection systems and AI-driven threat analysis. *Full Length Article*, *12*(2), pp.195-195.
56. Reyna, A., Martín, C., Chen, J., Soler, E. and Díaz, M., 2018. On blockchain and its integration with IoT. Challenges and opportunities. *Future generation computer systems*, *88*, pp.173-190. https://doi.org/10.1016/j.future.2018.05.046
57. Rizvi, S., Orr, R.J., Cox, A., Ashokkumar, P. and Rizvi, M.R., 2020. Identifying the attack surface for IoT network. *Internet of Things*, *9*, p.100162.
58. Roman, R., Zhou, J. and Lopez, J., 2013. On the features and challenges of security and privacy in distributed internet of things. *Computer networks*, *57*(10), pp.2266-2279. https://doi.org/10.1016/j.comnet.2012.12.018
59. Sadeghi, A.R., Wachsmann, C. and Waidner, M., 2015, June. Security and privacy challenges in industrial internet of things. In *Proceedings of the 52nd annual design automation conference* (pp. 1-6).
60. Saleem, J., Hammoudeh, M., Raza, U., Adebisi, B. and Ande, R., 2018, June. IoT standardisation: Challenges, perspectives and solution. In *Proceedings of the 2nd international conference on future networks and distributed systems* (pp. 1-9). doi: 10.1145/3231053.3231103.
61. Salma, S., Begum, A. and Syed, H., 2024. Practical and Innovative Applications of IoT and IoT Networks (Smart Cities, Smart Mobility, Smart Home, Smart Health, Smart Grid, etc.). In *AI for Climate Change and Environmental Sustainability* (pp. 121-144). CRC Press.
62. Samaila, M.G., Neto, M., Fernandes, D.A., Freire, M.M. and Inácio, P.R., 2018. Challenges of securing Internet of Things devices: A survey. *Security and Privacy*, *1*(2), p.e20. doi: 10.1002/spy2.20.
63. Sebestyen, H., Popescu, D.E. and Zmaranda, R.D., 2025. A Literature Review on Security in the Internet of Things: Identifying and Analysing Critical Categories. *Computers*, *14*(2), p.61.
64. Sfar, A.R., Natalizio, E., Challal, Y. and Chtourou, Z., 2018. A roadmap for security challenges in the Internet of Things. *Digital Communications and Networks*, *4*(2), pp.118-137. https://doi.org/10.1016/j.dcan.2017.04.003
65. Shindagi, K.S., Koppad, K.V., Ekbote, P.R., Bhandare, N.K., Revankar, D.D., Sonwalkar, P., Fadanis, B. and Shreyas, J., 2025. Federated Learning for Enhancing Cybersecurity in IoT-Integrated 6G Networks: Challenges, Opportunities, and Future Directions. *6G Cyber Security Resilience: Trends and Challenges*, pp.249-262.
66. Sicari, S., Rizzardi, A., Grieco, L.A. and Coen-Porisini, A., 2015. Security, privacy and trust in Internet of Things: The road ahead. *Computer networks*, *76*, pp.146-164. https://doi.org/10.1016/j.comnet.2014.11.008
67. Silva, M., Cerdeira, D., Pinto, S. and Gomes, T., 2019. Operating systems for internet of things low-end devices: Analysis and benchmarking. *IEEE Internet of Things Journal*, *6*(6), pp.10375-10383.
68. Srivastava, A., Gupta, S., Quamara, M., Chaudhary, P. and Aski, V.J., 2020. Future IoT-enabled threats and vulnerabilities: State of the art, challenges, and future prospects. *International Journal of Communication Systems*, *33*(12), p.e4443.
69. Szczepaniuk, H. and Szczepaniuk, E.K., 2022. Standardization of IoT ecosystems: open challenges, current solutions, and future directions. In *Internet of Things* (pp. 23-42). CRC Press.
70. Talal, M., Zaidan, A.A., Zaidan, B.B., Albahri, A.S., Alamoodi, A.H., Albahri, O.S., Alsalem, M.A., Lim, C.K., Tan, K.L., Shir, W.L. and Mohammed, K.I., 2019. Smart home-based IoT for real-time and secure remote health monitoring of triage and priority system using body sensors: Multi-driven systematic review. *Journal of medical systems*, *43*, pp.1-34.
71. Thankappan, M., Rifà-Pous, H. and Garrigues, C., 2022. Multi-Channel Man-in-the-Middle attacks against protected Wi-Fi networks: A state of the art review. *Expert Systems with Applications*, *210*, p.118401.
72. Touqeer, H., Zaman, S., Amin, R., Hussain, M., Al-Turjman, F. and Bilal, M., 2021. Smart home security: challenges, issues and solutions at different IoT layers. *The Journal of Supercomputing*, *77*(12), pp.14053-14089.
73. Umair, M., Cheema, M.A., Cheema, O., Li, H. and Lu, H., 2021. Impact of COVID-19 on IoT adoption in healthcare, smart homes, smart buildings, smart cities, transportation and industrial IoT. *Sensors*, *21*(11), p.3838.
74. ur Rehman, M.H., Salah, K., Damiani, E. and Svetinovic, D., 2019. Trust in blockchain cryptocurrency ecosystem. *IEEE Transactions on Engineering Management*, *67*(4), pp.1196-1212. https://doi.org/10.1016/j.future.2019.05.019
75. Vermesan, O. and Friess, P., 2015. *Building the hyperconnected society-internet of things research and innovation value chains, ecosystems and markets* (p. 332). Taylor & Francis.
76. Weber, R.H., 2010. Internet of Things–New security and privacy challenges. *Computer law & security*

review, *26*(1), pp.23-30. https://doi.org/10.1016/j.clsr.2009.11.008

77. Wolfert, S., Ge, L., Verdouw, C. and Bogaardt, M.J., 2017. Big data in smart farming–a review. *Agricultural systems*, *153*, pp.69-80. https://doi.org/10.1016/j.agsy.2017.01.023
78. Xenofontos, C., Zografopoulos, I., Konstantinou, C., Jolfaei, A., Khan, M.K. and Choo, K.K.R., 2021. Consumer, commercial, and industrial iot (in) security: Attack taxonomy and case studies. *IEEE Internet of Things Journal*, *9*(1), pp.199-221.
79. Zaman, S., Alhazmi, K., Aseeri, M.A., Ahmed, M.R., Khan, R.T., Kaiser, M.S. and Mahmud, M., 2021. Security threats and artificial intelligence based countermeasures for internet of things networks: a comprehensive survey. *Ieee Access*, *9*, pp.94668-94690.
80. Zanella, A., Bui, N., Castellani, A., Vangelista, L. and Zorzi, M., 2014. Internet of things for smart cities. *IEEE Internet of Things journal*, *1*(1), pp.22-32. https://doi.org/10.1109/JIOT.2014.2306328