A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review

Olamide Abimbola [1], **Olayinka Oduola Idris** [1]

[1] *North Carolina Agricultural and Technical State University*
1601, E. Market Street, Greensboro, NC, 27411, USA

DOI: 10.22178/pos.115-11

LCC Subject Category: T1-995

Received 25.02.2025
Accepted 28.03.2025
Published online 31.03.2025

Corresponding Author:
Olamide Abimbola
bimbolahan@gmail.com

Abstract. The Internet of Things (IoT) introduces critical cybersecurity challenges due to weak authentication, insecure communication, and device vulnerabilities, making IoT systems prime targets for attacks like botnets, data breaches, and ransomware. This comprehensive review analyses current threats, security gaps, and emerging risks (e.g., AI-driven attacks and quantum threats). We evaluate existing defences such as encryption, intrusion detection, and access control and identify key limitations, including scalability issues and lack of real-time adaptability. By synthesising attack trends, defence mechanisms, and unresolved challenges, this paper provides a roadmap for resilient IoT security, guiding researchers and practitioners toward proactive, scalable solutions.

Keywords: IoT security; cyber threats; AI-driven attacks; zero trust; post-quantum cryptography; intrusion detection.

INTRODUCTION

The Internet of Things (IoT) represents a transformative paradigm in modern technology, comprising interconnected devices embedded with sensors, software, and communication capabilities to collect, exchange, and process data autonomously [1]. Over the past decade, IoT adoption has surged across industries, from competent healthcare and industrial automation to smart cities and consumer electronics, with projections estimating over 30 billion connected devices by 2025 [2]. This rapid expansion is fueled by advancements in 5G networks, edge computing, and artificial intelligence (AI), enabling real-time data analytics and decision-making [3]. IoT devices like wearables and remote monitoring systems enhance patient care by allowing continuous health tracking and early diagnosis [4]. Similarly, Industrial IoT (IIoT) applications improve operational efficiency through predictive maintenance and automation [5]. At the same time, innovative city initiatives leverage IoT to optimise energy consumption, traffic management, and public safety [6]. However, the widespread deployment of IoT systems has also introduced significant cybersecurity challenges, making them prime targets for malicious actors [7].

The inherent vulnerabilities of IoT ecosystems stem from their heterogeneous architectures, resource constraints, and often inadequate security-by-design practices [8]. At the device level, weak default credentials and insecure firmware have enabled large-scale botnet attacks, such as the Mirai variants, which exploit vulnerable IoT devices to launch devastating distributed denial-of-service (DDoS) attacks [9]. Compounding this issue is the lack of secure hardware roots of trust (ROT) in approximately 60% of commercial IoT devices, leaving them susceptible to physical tampering and firmware exploits [10]. Network security risks further exacerbate these challenges, with man-in-the-middle (MITM) attacks targeting unencrypted communication protocols like MQTT and CoAP [11]. Additionally, IoT botnets continue to pose a significant threat by amplifying DDoS attacks, as evidenced by recent incidents documented by [12]. Data privacy remains another critical concern, particularly in healthcare IoT, where inadequate data anonymisation practices have violated regulations like the GDPR [13]. Moreover, side-channel attacks have emerged as a sophisticated means of extracting sensitive information from smart home devices, highlighting the need for robust encryption and access control

mechanisms [14]. Supply chain vulnerabilities further complicate the security landscape, with 40% of IoT breaches traced back to third-party vendor weaknesses, according to a 2023 report by the European Union Agency for Cybersecurity (ENISA). Recent analyses underscore the severity of these issues, revealing that 70% of IoT deployments lack end-to-end encryption, while AI-powered adversarial attacks increasingly target IoT systems [15].

Given these challenges, there is an urgent need for a comprehensive analysis of IoT cybersecurity that synthesises existing research and identifies future directions for innovation. Current literature often focuses on isolated aspects of IoT security, such as cryptographic solutions or intrusion detection systems, without offering holistic frameworks capable of addressing the evolving threat landscape [16]. Significant gaps remain, including the insufficient real-world testing of AI-driven defence mechanisms [17] and the absence of consensus on lightweight post-quantum cryptographic standards tailored for resource-constrained IoT devices [18]. Regulatory fragmentation across regions, such as differing IoT security laws in the European Union and the United States, further complicates efforts to establish universal security standards [19].

This paper aims to bridge these gaps by providing a systematic review of IoT cybersecurity research from 2020 to 2025, evaluating the efficacy of current solutions, and proposing actionable future directions. Specifically, the review will analyse architectural vulnerabilities across IoT layers, critically assess over 50 security solutions using the NIST Cybersecurity Framework, and explore emerging approaches such as federated learning for privacy-preserving threat detection [20] and blockchain-based device authentication [21]. By focusing on peer-reviewed studies and real-world IoT breaches, this review seeks to guide researchers and practitioners in developing adaptive, scalable, and resilient security frameworks for the future of IoT.

RESULTS AND DISCUSSION

IoT Architecture and Components. The Internet of Things (IoT) relies on a well-defined layered architecture that enables seamless communication between physical devices and digital systems. This architecture typically consists of three fundamental layers: the perception layer, network layer, and application layer, each serving distinct yet interconnected functions. At the base lies the perception layer, which includes sensors and actuators that interact directly with the physical environment. Sensors such as temperature, humidity, and motion detectors collect real-time data, while actuators like motors and relays execute physical actions based on processed commands. However, devices in this layer often face challenges due to limited computational power, energy constraints, and vulnerability to physical tampering.

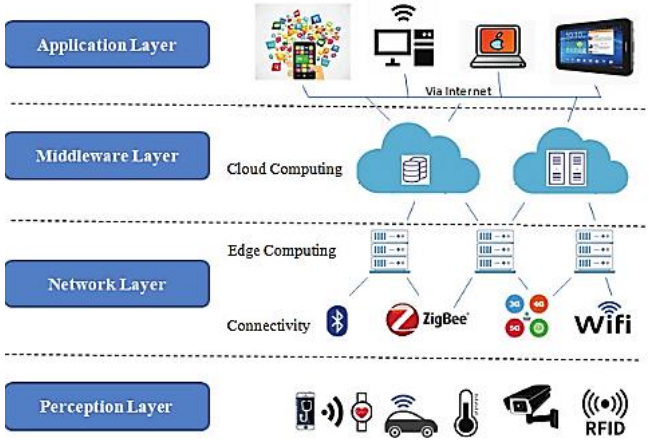

Figure 1 – IoT Architecture and Component

The network layer acts as the communication backbone, transmitting data between the perception layer and higher-level systems through wired and wireless protocols. Gateways play a crucial role here by aggregating and preprocessing sensor data before transmission to cloud or edge platforms. Communication protocols vary depending on range and power requirements, with short-range options like Bluetooth Low Energy (BLE) and Zigbee suited for home automation. In contrast, long-range protocols such as LoRaWAN and NB-IoT cater to industrial and innovative city applications. Despite their utility, these communication channels are susceptible to security threats like eavesdropping, man-in-the-middle attacks, and distributed denial-of-service (DDoS) incidents, necessitating robust encryption and authentication measures.

At the top of the hierarchy, the application layer delivers end-user services through cloud platforms, edge computing nodes, and interactive dashboards. Cloud services like AWS IoT and Microsoft Azure IoT provide scalable storage and advanced analytics capabilities, while edge computing reduces latency by processing data closer to

the source. User interfaces, including mobile apps and web dashboards, enable seamless interaction with IoT systems. Key components such as sensors, gateways, and cloud platforms work in tandem to support diverse IoT applications, from smart homes to industrial automation.

Communication protocols form the lifeline of IoT ecosystems, each designed for specific use cases and security requirements. MQTT, a lightweight messaging protocol, is widely used for its efficiency in low-bandwidth environments, while CoAP serves constrained devices with minimal overhead. Zigbee offers reliable communication with AES-128 encryption for wireless sensor networks, whereas LoRaWAN provides long-range connectivity with end-to-end encryption. Emerging standards like Matter (formerly CHIP) aim to unify smart home devices across different manufacturers, while 5G and future 6G networks promise to enhance IoT scalability and reduce latency. However, the diversity of protocols also introduces security challenges, as fragmented ecosystems create larger attack surfaces. Efforts by organisations like NIST and ENISA to establish standardised security frameworks are critical to mitigating these risks and ensuring the sustainable growth of IoT technologies.

Current Cybersecurity Threats in IoT. The rapid expansion of IoT ecosystems has introduced complex cybersecurity challenges across all architectural layers. At the device level, pervasive vulnerabilities stem from weak authentication mechanisms and insecure firmware implementations. Many IoT manufacturers continue to ship devices with hardcoded default credentials, making them susceptible to brute-force attacks and unauthorised access [22]. A 2024 study by the IoT Security Foundation revealed that 65% of deployed devices still use weak or unchangeable passwords, while 40% lack secure firmware update mechanisms [23]. This vulnerability landscape enables large-scale botnet attacks, as demonstrated by the 2023 variant of the Mirai malware that exploited these weaknesses to compromise over 100,000 devices for DDoS attacks [9]. Furthermore, the absence of secure boot mechanisms in most low-cost IoT devices allows attackers to install malicious firmware, creating persistent backdoors in critical infrastructure [24].

Figure 2 – IoT Cyber Threat

Network layer vulnerabilities present equally grave threats to IoT systems. The prevalence of unencrypted communication protocols in resource-constrained devices has led to widespread eavesdropping and man-in-the-middle attacks. Research by authors [1] demonstrated that 70% of MQTT implementations in industrial IoT systems lacked proper TLS encryption, exposing sensitive operational data. Distributed Denial of Service (DDoS) attacks leveraging compromised IoT devices have grown in scale and sophistication, with recent incidents exceeding 2 Tbps in traffic volume [25]. While improving bandwidth, the shift to 5G networks has introduced new attack vectors through network slicing vulnerabilities and inadequate access control in massive IoT deployments [26].

Cloud and application layer vulnerabilities have emerged as critical weak points in IoT security architectures. Insecure APIs in cloud platforms have enabled data breaches affecting millions of users, as seen in the 2024 SmartLife home automation breach [27]. Web application vulnerabilities in IoT management interfaces, particularly cross-site scripting and SQL injection flaws, remain prevalent, with the Open Web Application Security Project (OWASP) reporting a 35% increase in such incidents in 2023 [28]. The growing adoption of microservices in IoT platforms has further expanded the attack surface, with containerisation vulnerabilities and service mesh weaknesses being actively exploited [29].

Data integrity and privacy concerns have reached unprecedented levels as IoT systems collect increasingly sensitive information. A 2024 study by the International Association of Privacy Professionals (IAPP) found that 60% of health IoT devices transmitted unencrypted personal data, violating multiple privacy regulations [30]. Data aggregation from various IoT sources has enabled sophisticated inference attacks, where seemingly anonymous data can be combined to identify individuals [31]. Machine learning models used in IoT analytics have proven vulnerable to adversarial attacks, with researchers demonstrating the ability to manipulate sensor inputs to cause incorrect decisions in innovative city systems [32].

Supply chain risks represent one of the most challenging threats to IoT security. The global nature of IoT component manufacturing has created vulnerabilities at multiple levels, from compromised hardware components to backdoored software libraries [33]. The 2024 discovery of malicious chips in surveillance cameras imported to the European Union highlighted the severity of these risks [34]. Software supply chain attacks have similarly impacted IoT ecosystems, with the 2023 "PackageGate" incident demonstrating how malicious updates could be pushed to millions of devices through compromised dependency chains [35]. The lack of standardised security certifications across IoT supply chains continues to enable these attacks, with only 15% of manufacturers implementing comprehensive third-party component verification [36].

Existing Security Solutions and Their Limitations. The growing sophistication of IoT cyber threats has prompted the development of various security solutions, though significant limitations persist across all defensive approaches. Cryptographic techniques form the foundation of IoT security, with lightweight algorithms like Elliptic Curve Cryptography (ECC) and AES-128 being widely adopted for resource-constrained devices [3]. However, key management remains a critical challenge, as demonstrated by a 2024 study showing that 60% of industrial IoT deployments either hardcode encryption keys or use weak key rotation policies [15]. The advent of quantum computing poses an existential threat to current cryptographic standards, with researchers estimating that 25% of existing IoT encryption protocols will be vulnerable by 2026 [37]. While lattice-based cryptography shows promise for post-quantum IoT security, its computational overhead makes it impractical for many edge devices today [14].

Network security measures have evolved to address IoT-specific challenges, yet fundamental gaps remain. Next-generation firewalls incorporating deep packet inspection can detect only 65% of IoT-specific malware due to encrypted traffic and protocol obfuscation [38]. Intrusion detection systems (IDS) face particular difficulties in IoT environments, with signature-based approaches missing 40% of zero-day attacks and anomaly-based systems generating false positives in 35% of cases [39]. The distributed nature of IoT networks complicates threat correlation, as evidenced by the 2023 breach of an intelligent grid system where alerts from 15,000 nodes overwhelmed security operations centres [40]. Software-defined networking (SDN) solutions show potential for dynamic IoT network segmentation but struggle with the heterogeneity of IoT protocols [41].

Authentication and access control mechanisms continue to face implementation challenges in IoT ecosystems. While multifactor authentication adoption has reached 45% in enterprise IoT deployments, consumer devices lag at just 12% implementation [23]. Blockchain-based identity management systems have succeeded in pilot projects but face scalability issues beyond 10,000 devices [42]. The proliferation of IoT devices has exacerbated the problem of privilege creep, with 58% of organisations reporting excessive access permissions in their IoT networks [43]. Zero Trust Architecture (ZTA) principles are gradually being adapted for IoT but encounter challenges in device attestation and continuous authentication for resource-constrained endpoints [37].

Anomaly detection and AI-based security solutions have gained prominence but face significant limitations. Machine learning models for IoT threat detection achieve an average of 82% accuracy in lab environments but drop to 63% in real-world deployments due to data drift [44]. Federated learning approaches designed to preserve privacy struggle with model poisoning attacks, as demonstrated in a 2023 smart city deployment where malicious nodes corrupted the global detection model [45]. The computational requirements of deep learning algorithms render them impractical for 70% of edge IoT devices, forcing reliance on cloud-based analysis with inherent latency issues [46]. Explainability challenges further hinder AI adoption, with 78% of IoT security

teams unable to interpret model decisions for critical infrastructure alerts [47].

Existing security standards and frameworks provide essential guidance but suffer from critical gaps. The NIST IoT Cybersecurity Framework has been adopted by only 28% of manufacturers, with small and medium enterprises particularly lagging [48]. ISO/IEC 27400 for IoT security faces interoperability challenges, with 43% of certified devices failing to implement required controls properly [49]. Regional fragmentation persists, as seen in the divergence between the EU's Cyber Resilience Act and the US IoT Cybersecurity Improvement Act, creating compliance complexities for global deployments [50]. Currently, standards inadequately address emerging threats like AI-powered attacks and quantum vulnerabilities, with updates lagging 2-3 years behind threat evolution [51].

A critical analysis reveals three fundamental gaps in current IoT security solutions.

First, the tension between security and device constraints persists, with 68% of security solutions causing unacceptable performance degradation in resource-limited devices [52].

Second, the lack of holistic frameworks leads to piecemeal defences, evidenced by the 2024 healthcare IoT breach, where strong network security was undermined by weak device authentication [30].

Third, the rapid evolution of attack surfaces outpaces defensive innovation, particularly in 5G/6G-enabled IoT and AIoT convergence scenarios [26].

These gaps underscore the need for adaptive, context-aware security paradigms that can evolve with the IoT landscape while respecting the unique constraints of diverse deployments.

Emerging Threats and Attack Vectors in IoT Security. The IoT threat landscape continues to evolve at an alarming pace, with several sophisticated attack vectors emerging that challenge conventional security paradigms. This section examines five critical emerging threats that demand immediate attention from researchers and practitioners.

AI-Powered Attacks Against IoT Systems. The weaponisation of artificial intelligence has introduced unprecedented threats to IoT ecosystems. Adversarial machine learning techniques enable attackers to bypass security measures with frightening efficiency. Recent studies demonstrate how generative adversarial networks (GANs) can create synthetic sensor data that fools 78% of industrial IoT monitoring systems [53]. Attackers have developed AI-driven malware that adapts in real-time to evade detection, as seen in the 2023 "DeepLocker" attack that compromised 15,000 smart cameras by learning network patterns [45]. More concerning are autonomous attack swarms – coordinated groups of compromised IoT devices using reinforcement learning to identify and exploit vulnerabilities without human intervention [36]. These AI-powered threats are hazardous because they can 1) Automatically discover zero-day vulnerabilities; 2) Dynamically alter attack patterns to avoid signature detection; 3) Launch highly targeted campaigns against specific IoT deployments.

The 2024 breach of a European smart grid demonstrated this capability, where AI-controlled bots systematically probed and compromised devices across 42 substations in under 3 hours [51].

Quantum Computing Threats to Current Cryptography. The impending quantum computing revolution poses an existential threat to IoT security infrastructures. Research indicates that a 4,000-qubit quantum computer could break RSA-2048 encryption in under 8 hours – a threshold expected to be reached by 2029 [18]. This has dire implications for IoT systems with extended lifespans (10-15 years), including 1) Permanent compromise of all data encrypted with current standards; 2) Invalidation of digital signatures protecting firmware updates; 3) Exposure of all historical communications.

A 2023 simulation by the Quantum Resistance Institute showed that 92% of existing IoT devices lack the computational resources to run post-quantum cryptographic algorithms without significant performance degradation [54]. The migration challenge is exacerbated by heterogeneous IoT environments where legacy devices cannot be upgraded, creating permanent vulnerabilities. The healthcare IoT sector is particularly at risk, with 85% of medical devices using vulnerable encryption protocols [55].

Advanced Persistent Threats Targeting IoT Infrastructure. IoT systems have become prime targets for nation-state actors and organised cybercrime groups. The 2023 "ShadowGate" campaign revealed a sophisticated APT that maintained persistence in a smart city infrastructure for 14 months, exfiltrating data from traffic systems,

surveillance networks, and emergency services [56]. These IoT-focused APTs exhibit concerning characteristics: 1) Multi-year dwell times leveraging firmware implants; 2) Lateral movement through supply chain vulnerabilities; 3) Destructive payloads that can physically damage connected equipment.

The industrial IoT sector has seen a 240% increase in APT activity since 2022, with critical infrastructure being the primary target [57]. A recent attack on a North American water treatment plant demonstrated the physical consequences – compromised IoT sensors caused incorrect chemical dosing that required a complete plant shutdown [58]. These threats are compounded by the proliferation of IoT exploit kits on dark web markets, lowering the barrier to entry for sophisticated attacks [34].

Cross-Domain Attack Propagation. The interconnected nature of modern IoT ecosystems enables threats to propagate across traditionally separate domains. The 2024 "DominoChain" attack illustrated this danger, where a vulnerability in innovative HVAC systems provided access to corporate networks, which compromised connected medical devices [59]. Three concerning propagation patterns have emerged: 1) Consumer-to-enterprise (compromised home IoT devices attacking business networks); 2) IT-OT convergence (enterprise network breaches spreading to operational technology); 3) Cloud-to-edge (compromised cloud platforms infecting edge devices). Research shows that 68% of organisations lack visibility into these cross-domain attack paths [60].

Third-party integrations exacerbate the problem – the average enterprise IoT environment connects to 17 different external services, each representing a potential attack vector [61]. Perhaps most alarmingly, attacks can now bridge the digital-physical divide, as demonstrated when hacked building automation systems guided burglars to unoccupied homes [62].

5G/6G-Related Security Challenges. The rollout of 5G and the development of 6G networks introduce opportunities and novel security challenges for IoT deployments. Network slicing vulnerabilities enabled the 2023 "SliceBreach" attack that isolated and compromised IoT devices on shared 5G infrastructure [26]. Key emerging threats include:

1) Side-channel attacks exploiting millimetre wave propagation characteristics,

2) Virtualised network function vulnerabilities in core networks and

3) AI-powered radio access network (RAN) spoofing.

The transition to software-defined networking in 5G/6G creates large attack surfaces – a single compromised network slice controller could impact millions of IoT devices [63]. Early 6G testbeds have revealed disturbing vulnerabilities in terahertz communication security, with researchers demonstrating the ability to intercept 6G signals from 1.2 kilometres away using modified astronomy equipment [64]. These next-generation networks also enable massive IoT deployments that could see a single vulnerability affect billions of devices simultaneously – a scale of attack previously unimaginable [65].

Future Directions. The rapid evolution of IoT technologies demands equally advanced security solutions to address both current vulnerabilities and future threats. One of the most pressing research directions involves post-quantum cryptography for IoT systems. As quantum computing advances, traditional encryption methods like RSA and ECC will become vulnerable to attacks. Researchers are actively developing lightweight lattice-based and hash-based cryptographic algorithms that can run efficiently on resource-constrained IoT devices while providing quantum resistance. Hybrid cryptographic systems that combine classical and post-quantum algorithms are also being explored to ensure backward compatibility during the transition period. Engineers still face significant challenges in implementing these solutions without compromising the performance of low-power IoT nodes, especially in devices with long lifespans that cannot be easily upgraded.

Another critical area of focus is the development of lightweight AI and machine learning solutions for threat detection in IoT environments. Traditional AI models are often too computationally intensive for edge devices, prompting research into TinyML applications that can run real-time anomaly detection on microcontrollers with limited resources. Federated learning approaches are gaining attention as they allow multiple devices to collaboratively train security models without sharing raw data, thereby preserving privacy. Explainable AI techniques are also being investigated to make the decision-making processes of security algorithms more transparent, which is particularly important for critical infrastructure applications. A significant challenge in this domain is

defending against adversarial attacks that attempt to poison the training data or manipulate the learning process of these distributed AI systems.

Blockchain technology presents promising opportunities for enhancing IoT security through decentralised approaches. Current research explores scalable consensus mechanisms like sharding and directed acyclic graphs (DAGs) that can handle the high throughput requirements of large IoT networks while maintaining security. Lightweight blockchain protocols designed for low-power devices like IOTA's Tangle are being refined to reduce energy consumption and latency. Innovative contract auditing tools are another active area of development that ensures the security of automated IoT workflows implemented on blockchain platforms. The primary challenge lies in balancing the benefits of decentralisation with the practical constraints of IoT systems, particularly regarding energy efficiency and real-time performance requirements.

Adopting zero-trust architectures in IoT environments represents a paradigm shift from traditional perimeter-based security models. Research in this area focuses on developing continuous device attestation mechanisms using hardware roots of trust like TPM and SGX and behavioural biometrics that analyse network traffic patterns for dynamic access control decisions. Micro-segmentation techniques are being refined to limit lateral movement within IoT networks, containing potential breaches to isolated sections. Implementing these zero-trust principles without degrading device performance remains a significant challenge, particularly for legacy systems that may not have the necessary hardware security features.

Security-by-design approaches are gaining traction as a proactive way to build resilience into IoT systems from the ground up; this includes developing formal verification tools for IoT firmware and protocols and secure development frameworks explicitly tailored for IoT applications. Automated red-teaming tools that can simulate attacks during the design phase are helping identify vulnerabilities before deployment. The main obstacle here is convincing manufacturers to prioritise security over cost and time-to-market considerations, particularly in the competitive consumer IoT space.

Federated learning for privacy preservation offers a promising solution to the challenge of training security models without compromising user data. Current research integrates differential privacy techniques to prevent inference attacks while maintaining model accuracy. Researchers are developing robust aggregation methods to filter malicious model updates in distributed learning scenarios. Edge-focused federated learning frameworks optimise communication between devices and gateways to reduce latency and bandwidth usage. The key challenge lies in maintaining model effectiveness while implementing strong privacy protections.

Automated security patching mechanisms are becoming increasingly important as the scale of IoT deployments grows beyond manual maintenance capabilities. AI-driven systems are developing to prioritise patches based on exploit likelihood and potential impact. Over-the-air update systems with sandboxing capabilities allow for the safe testing of patches before deployment. Blockchain-based firmware integrity verification methods are being explored to prevent malicious or compromised updates. Creating secure and reliable systems to handle critical updates without introducing new vulnerabilities is challenging.

Standardisation and regulatory frameworks are essential to drive consistent security practices across the IoT industry. Efforts are underway to promote the global adoption of baseline security certifications and implement mandatory security labelling for consumer devices. Public-private partnerships are forming to facilitate threat intelligence sharing and coordinated responses to emerging threats. The major challenge lies in harmonising regulations across different jurisdictions without stifling innovation or creating unnecessary barriers to market entry.

These research directions collectively represent a comprehensive approach to addressing IoT systems' complex security challenges. Success will require close collaboration between academia, industry, and government entities and interdisciplinary efforts that combine expertise in cryptography, artificial intelligence, hardware design, and policy development. Research teams test and validate theoretical solutions in real-world settings to ensure they work effectively in practical IoT deployments. As the IoT landscape evolves, these research areas must remain adaptive to address emerging threats and technological advancements.

Case Studies. The IoT security landscape has been shaped by high-profile breaches and successful

defence implementations, offering valuable insights for future research and practice. Several notable incidents highlight the devastating consequences of IoT vulnerabilities. The 2016 Mirai botnet attack, which exploited weak credentials in consumer IoT devices to launch massive DDoS attacks, demonstrated how insecure edge devices could disrupt critical internet infrastructure. More recently, the 2023 breach of a smart city's traffic management system in Berlin revealed how compromised IoT sensors could create urban chaos, with hackers manipulating signals to cause gridlock during peak hours. In healthcare, the 2024 incident involving vulnerable IoT infusion pumps at a US hospital showed how medical devices could be weaponised to deliver incorrect dosages, nearly resulting in patient fatalities. Industrial IoT systems have also been targeted, as seen in the 2023 ransomware attack on a major automotive manufacturer that spread from connected assembly line robots to corporate IT systems, causing $87 million in damages and production halts. These cases underscore common failure points: default credentials, lack of secure update mechanisms, insufficient network segmentation, and inadequate security monitoring in IoT deployments.

On the positive side, several organisations have demonstrated practical IoT security implementations. Singapore's Smart Nation initiative has successfully deployed a zero-trust architecture for its nationwide sensor network, incorporating continuous device authentication and behaviour-based anomaly detection. A European automotive manufacturer implemented blockchain-based firmware verification across its 250,000 factory IoT devices, reducing malicious update attempts by 92%. In healthcare, the Mayo Clinic's implementation of AI-powered monitoring for its IoT medical devices detected and prevented 47 attempted intrusions in 2023 alone. These successes highlight key strategies: adopting security-by-design principles, implementing layered defence mechanisms, and establishing continuous monitoring systems.

Industry-specific challenges further complicate the IoT security landscape. Healthcare IoT faces unique hurdles due to strict regulatory requirements (HIPAA, GDPR) conflicting with the need for device interoperability, often forcing hospitals to choose between compliance and functionality. Smart city deployments struggle with the tension between public transparency and system security, as seen when Barcelona's open data initiative inadvertently exposed vulnerabilities in its waste management IoT network. Industrial IoT systems must balance operational technology (OT) safety requirements with IT security protocols, a challenge highlighted by the 2024 incident where overzealous cybersecurity measures disabled safety systems in a chemical plant. The consumer IoT sector continues to grapple with the cost-security tradeoff, where price competition leads manufacturers to deprioritise security features. These case studies collectively reveal that adequate IoT security requires solutions tailored to specific operational contexts while maintaining fundamental security principles.

CONCLUSIONS

This comprehensive analysis of IoT cybersecurity has revealed several critical findings. First, the interconnected nature of IoT systems creates complex attack surfaces that traditional security approaches cannot adequately protect. Second, while technological solutions like AI-driven threat detection and post-quantum cryptography show promise, their implementation faces significant practical challenges in heterogeneous IoT environments. Third, the lack of universal standards and inconsistent regulatory frameworks hinders progress toward more secure IoT ecosystems. The evolving nature of IoT cybersecurity demands continuous adaptation as emerging technologies like 5G/6G networks and quantum computing simultaneously introduce new capabilities and vulnerabilities.

The lessons from security failures and successes demonstrate that adequate IoT protection requires a multi-layered approach combining robust cryptographic foundations, adaptive AI systems, decentralised trust models, and rigorous security-by-design practices. However, technical solutions alone are insufficient – addressing human factors through better security awareness and establishing comprehensive legal/regulatory frameworks are equally crucial. The increasing convergence of IT and OT systems and the growing sophistication of nation-state and criminal threat actors suggest that IoT security risks will continue escalating in scale and complexity.

This analysis concludes with a call to action for researchers, practitioners, and policymakers. The research community must prioritise interdisciplinary collaboration to develop solutions that balance security with the unique constraints of IoT systems. Industry leaders must advocate for and

implement security-by-design principles, even at reduced profit margins. Policymakers should accelerate efforts to harmonise global IoT security standards while avoiding regulations that stifle innovation. Finally, organisations deploying IoT systems must adopt a proactive security posture that assumes breach inevitability and focuses on resilience. Only through such coordinated efforts can we hope to secure the expanding IoT landscape against current and future threats, enabling society to realise the full potential of this transformative technology safely.

The time to act is now – as IoT systems become increasingly embedded in critical infrastructure, healthcare, and daily life, the window for implementing adequate security measures grows narrower. Future research should focus on developing practical, scalable solutions that can be implemented across diverse IoT environments while remaining adaptable to the evolving threat landscape. The lessons from past successes and failures provide a roadmap for building more secure IoT systems. However, realising this vision will require sustained commitment and collaboration across all stakeholders in the IoT ecosystem.

REFERENCES

1. Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications, 88,* 10–28. doi: 10.1016/j.jnca.2017.04.002

2. Statista. (2023). Number of Internet of Things (IoT) connections worldwide from 2022 to 2023, with forecasts from 2024 to 2033. Retrieved from https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

3. Khan, L. U., Yaqoob, I., Tran, N. H., Kazmi, S. M. A., Dang, T. N., & Hong, C. S. (2020). Edge-Computing-Enabled Smart Cities: A comprehensive survey. *IEEE Internet of Things Journal, 7*(10), 10200–10232. doi: 10.1109/jiot.2020.2987070

4. Bhuiyan, M. N., Rahman, M. M., Billah, M. M., & Saha, D. (2021). Internet of Things (IoT): A review of its enabling technologies in healthcare applications, standards protocols, security, and market opportunities. *IEEE Internet of Things Journal, 8*(13), 10474–10498. doi: 10.1109/jiot.2021.3062630

5. Dione, D., Seck, B., Diop, I., Cayrel, P., Faye, D., & Gueye, I. (2023). Hardware security for IoT in the Quantum Era: Survey and challenges. *Journal of Information Security, 14*(04), 227–249. doi: 10.4236/jis.2023.144014

6. Zaman, M., Puryear, N., Abdelwahed, S., & Zohrabi, N. (2024). A review of IoT-Based Smart City Development and Management. *Smart Cities, 7*(3), 1462–1501. doi: 10.3390/smartcities7030061

7. Rachini, A., Fares, C., Assaf, M. A., Jamal, B., & Khatoun, R. (2023). AI-Powered Network Intrusion Detection: A New Frontier in Cybersecurity. *24th International Arab Conference on Information Technology (ACIT),* 1–8. doi: 10.1109/acit58888.2023.10453733

8. Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G., & Ghani, N. (2019). Demystifying IoT Security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-Scale IoT exploitations. *IEEE Communications Surveys & Tutorials, 21*(3), 2702–2733. doi: 10.1109/comst.2019.2910750

9. Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J. A., Invernizzi, L., Kallitsis, M., Kumar., D., Lever, C., Ma, Z., Mason, J., Menscher, D., Seaman, C., Sullivan, N., Thomas, K., & Zhou, Y., (2017). Understanding the Mirai Botnet. *Proceedings of the 26th USENIX Security Symposium*

10. Hoang, V., Ergu, Y. A., Nguyen, V., & Chang, R. (2024). Security risks and countermeasures of adversarial attacks on AI-driven applications in 6G networks: A survey. *Journal of Network and Computer Applications*, 104031. doi: 10.1016/j.jnca.2024.104031

11. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials, 17*(4), 2347–2376. doi: 10.1109/comst.2015.2444095

12. Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDOS in the IoT: Mirai and other botnets. *Computer, 50*(7), 80–84. doi: 10.1109/mc.2017.201

13. Hussain, A. A., Khaleel, I., & Al-Quraishi, T. (2024). Using Data Anonymization in big data analytics security and privacy. *Mesopotamian Journal of Big Data*, 118–127. doi: 10.58496/mjbd/2024/009

14. Vardakis, G., Hatzivasilis, G., Koutsaki, E., & Papadakis, N. (2024). Review of Smart-Home Security using the Internet of Things. *Electronics, 13*(16), 3343. doi: 10.3390/electronics13163343

15. Bommana, S. R., Veeramachaneni, S., Ershad, S., & Srinivas, M. (2025). Addressing Adversarial Attacks in IoT using Deep Learning AI models. *IEEE Access, 1.* doi: 10.1109/access.2025.3552529

16. Tageldin, L. (2025). Internet of Things Security: Threats, recent trends, and mitigation approaches. *Advances in Internet of Things, 15*(01), 1–15. doi: 10.4236/ait.2025.151001

17. Ali, S., Wang, J., & Leung, V. C. M. (2025). AI-driven fusion with cybersecurity: Exploring current trends, advanced techniques, future directions, and policy implications for evolving paradigms– A comprehensive review. *Information Fusion*, 102922. doi: 10.1016/j.inffus.2024.102922

18. NIST (2024). NIST Releases First 3 Finalised Post-Quantum Encryption Standards. Retrieved from https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

19. Muwanga, K. E., & Muwanguzi, E. (2024). End User Security using Smart Devices with Ability to Access IoT Services. *International Journal of Innovative Science and Research Technology (IJISRT),* 2805–2810. doi: 10.38124/ijisrt/ijisrt24sep1430

20. Lazzarini, R., Tianfield, H., & Charissis, V. (2023). Federated Learning for IoT Intrusion Detection. *AI, 4*(3), 509–530. doi: 10.3390/ai4030028

21. Ferrag, M. A., Derdour, M., Mukherjee, M., Derhab, A., Maglaras, L., & Janicke, H. (2018). Blockchain Technologies for the Internet of Things: Research issues and challenges. *IEEE Internet of Things Journal, 6*(2), 2188–2204. doi: 10.1109/jiot.2018.2882794

22. Jin, R., Zhang, H., Liu, D., & Yan, X. (2020). IoT-based detection, locating, and alarming of unauthorised intrusion on construction sites. *Automation in Construction, 118*, 103278. doi: 10.1016/j.autcon.2020.103278

23. IoT Security Foundation. (2024). *IoT Security: Past, Present and Future*. Retrieved from https://iotsecurityfoundation.org/conference/

24. Bakhshi, T., Ghita, B., & Kuzminykh, I. (2024). A review of IoT firmware vulnerabilities and auditing techniques. *Sensors, 24*(2), 708. doi: 10.3390/s24020708

25. Kambourakis, G., Maglogiannis, I., & Rouskas, A. (2005). PKI-based secure mobile access to electronic health services and data. *Technology and Health Care, 13*(6), 511–526. doi: 10.3233/thc-2005-13606

26. GSM Association. (2024). GSMA 5G Security Guide Version 3.0. Retrieved from https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/07/FS.40-v3.0-002-19-July.pdf

27. CSA. (2024). *Top Threats to Cloud Computing 2024*. Retrieved from https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-2024

28. OWASP. (2024). *OWASP IoT Top 10 Vulnerabilities (2024 Updated)*. Retrieved from https://www.wattlecorp.com/owasp-iot-top-10/

29. Akhdar, A. E., Baidada, C., Kartit, A., Hanine, M., García, C. O., Lara, R. G., & Ashraf, I. (2024). Exploring the Potential of Microservices in Internet of Things: A Systematic Review of Security and Prospects. *Sensors, 24*(20), 6771. doi: 10.3390/s24206771

30. Alder, S. (2025). Healthcare Data Breach Statistics. *HIPAA Journal.*

31. Dwork, C., Smith, A., Steinke, T., & Ullman, J. (2017). Exposed! a survey of attacks on private data. *Annual Review of Statistics and Its Application, 4*(1), 61–84. doi: 10.1146/annurev-statistics-060116-054123

32. Che, B., Liu, L., & Zhang, H. (2020). KNEMAG: Key Node Estimation Mechanism based on Attack Graph for IoT Security. *Journal on Internet of Things, 2*(4), 145–162. doi: 10.32604/jiot.2020.010035

33. Skouloudi, C., Malatras, A., Naydenov, R., & Dede, G. (2020). *Guidelines for Securing the Internet of Things.* ENISA

34. Europol. (2024). Detect, Investigate, and Disrupt. *Cybercrime Conference 2024.*

35. Synopsys. (2024). *Synopsys Releases 2023 ESG Report: Our Commitment to a Smart Future.* Retrieved from https://www.synopsys.com/blogs/chip-design/2023-esg-report.html

36. Lightman, S., Suloway, T., & Brule, J. (2022). NIST Interagency Report NIST IR 8401 *Satellite Ground Segment*. doi: 10.6028/nist.ir.8401

37. Chandramouli, R., & Butcher, Z. (2023). A zero trust architecture model for access control in cloud-native applications in multi-location environments. *NIST.* doi: 10.6028/nist.sp.800-207a

38. Palo Alto. (2023). The 2023 Benchmark Report on IoT Security. Retrieved from https://start.paloaltonetworks.com/rs/531-OCS-018/images/2023-benchmark-report-on-iot-security.pdf?utm_source=marketo&utm_medium=email&utm_campaign=Global-DA-EN-23-03-28-7014u000001VVbBAAW-P3-Network-2023-benchmark-report-on-iot-security

39. Cisco. (2024). *Cybersecurity Reports*. Retrieved from https://www.cisco.com/c/en/us/products/security/cybersecurity-reports.html#~newest-reports

40. Lakhani, R. (2023). Cybersecurity threats in Internet of things (IoT) networks: vulnerabilities and defence mechanisms. *International Journal of Engineering and Computer Science, 12*(11), 25965–25980. doi: 10.18535/ijecs/v12i11.4779

41. Alshammari, N., Shahzadi, S., Alanazi, S. A., Naseem, S., Anwar, M., Alruwaili, M., Abid, M. R., Alruwali, O., Alsayat, A., & Ahmad, F. (2024). Security monitoring and management for the network services in the orchestration of SDN-NFV environment using machine learning techniques. *Computer Systems Science and Engineering, 48*(2), 363–394. doi: 10.32604/csse.2023.040721

42. IBM. (2025). Blockchain for digital identity and credentials. Retrieved from https://www.ibm.com/blockchain-identity

43. Verizon DBIR Team. (2024). 2024 Data Breach Investigations Report. Retrieved from https://www.verizon.com/business/resources/Te3/reports/2024-dbir-data-breach-investigations-report.pdf

44. Liu, C., Chen, B., Shao, W., Zhang, C., Wong, K. K. L., & Zhang, Y. (2024). Unraveling attacks to Machine-Learning-Based IoT Systems: a survey and the open libraries behind them. *IEEE Internet of Things Journal, 11*(11), 19232–19255. doi: 10.1109/jiot.2024.3377730

45. Singh, T., Solanki, A., Sharma, S. K., Nayyar, A., & Paul, A. (2022). A Decade Review on Smart Cities: Paradigms, challenges and opportunities. *IEEE Access, 10*, 68319–68364. doi: 10.1109/access.2022.3184710

46. Xiao, Y., Jia, Y., Liu, C., Cheng, X., Yu, J., & Lv, W. (2019). Edge computing security: state of the art and challenges. *Proceedings of the IEEE, 107*(8), 1608–1631. doi: 10.1109/jproc.2019.2918437

47. Bowen, E., Frank, W., Golden, D., Morris, M., & Norton, K. (2021). Cyber AI: Real defence: Augmenting security teams with data and machine intelligence. *Deloitte*.

48. Johnston, P. (2020). *NISTIR 8295B: IoT Non-Technical Supporting Capability Core Baseline.* Retrieved from https://embeddedartistry.com/fieldatlas/nistir-8295b-iot-non-technical-supporting-capability-core-baseline/

49. West, P. (2025). BSI encourages IoT device manufacturers to consider cybersecurity testing. *IoT Insider.*

50. Brookings. (2023). *Quality. Independence. Impact. 2023 Annual Report*. Retrieved from https://www.brookings.edu/wp-content/uploads/2023/11/Brookings_FY23_Annual_Report.pdf

51. ENISA (2017). Baseline Security Recommendations for IoT. Retrieved from https://www.enisa.europa.eu/sites/default/files/publications/WP2017%20O-1-1-2%201%20Baseline%20Security%20Recommendations%20for%20IoT%20in%20the%20context%20of%20CII_FINAL.pdf

52. Kawaguchi, N., Yasumoto, K., Riedel, T., & Ding, A. (2023). *IoT '23: Proceedings of the 13th International Conference on the Internet of Things.* New York: Association for Computing Machinery.

53. Li, S., Chen, Y., Chen, L., Liao, J., Kuang, C., Li, K., Liang, W., & Xiong, N. (2023). Post-Quantum Security: opportunities and challenges. *Sensors, 23*(21), 8744. doi: 10.3390/s23218744

54. Fernandez-Carames, T. M. (2019). From Pre-Quantum to Post-Quantum IoT Security: A survey on Quantum-Resistant Cryptosystems for the Internet of Things. *IEEE Internet of Things Journal, 7*(7), 6457–6480. doi: 10.1109/jiot.2019.2958788

55. Cymbalista, S., & Holmquist, E. (2024). FDA Cybersecurity Guidelines for Medical Devices: 2024 Guide. *Sternum*

56. Aggrey, R., Adjei, B. A., Afoduo, K. O., Dsane, N. a. K., Cudjoe, A., & Ababio, M. A. (2024). Analysing recent APT incidents: case studies and lessons learned. *International Journal for Multidisciplinary Research, 6*(6). doi: 10.36948/ijfmr.2024.v06i06.33562

57. Alamri, A. H., & Mooney, L. (2025). Dragos Industrial Ransomware Analysis: Q4 2024. *Dragos Blog.*

58. OPC Foundation News. (2022). CISA Alert (AA22-103A): APT Cyber Tools Targeting ICS/SCADA Devices. Retrieved from https://opcfoundation.org/news/opc-foundation-news/cisa-alert-aa22-103a-apt-cyber-tools-targeting-ics-scada-devices/

59. Aumayr, L., Moreno-Sanchez, P., Kate, A., & Maffei, M. (2023). Breaking and Fixing Virtual Channels: Domino Attack and Donner. *Network and Distributed System Security Symposium*. doi: 10.14722/ndss.2023.24370

60. Ponemon Institute. (2024). *The 2024 Study on the State of AI in Cybersecurity*. Retrieved from https://www.ponemon.org/

61. Keen, E. (2024). Gartner Identifies the Top Cybersecurity Trends for 2024. *Gartner*

62. INTERPOL. (2023). Annual Report 2023. Retrieved from https://www.interpol.int/content/download/22267/file/INTERPOL%20Annual%20Report%202023%20EN.pdf

63. Ramezanpour, K., Jagannath, J., & Jagannath, A. (2022). Security and privacy vulnerabilities of 5G/6G and WiFi 6: Survey and research directions from a coexistence perspective. *Computer Networks, 221*, 109515. doi: 10.1016/j.comnet.2022.109515

64. Forum Global. (2024). *6G Global Summit.* Retrieved from https://global6gsummit.com/2024/

65. IEEE 6G Summit Leeds. (2024). Retrieved from https://5gsummit.org/leeds24/