Cybersecurity Threats in IoT
A Literature Review

Submitted by

Ketan Mone

MSc Cyber Security, University of Essex Online

Submission Date: **14 September 2025**

Word Count : **1949**

Table of Contents

1. Introduction

The Internet of Things (IoT) has rapidly evolved into a transformative technological ecosystem that connects billions of devices, ranging from consumer wearables and home automation systems to industrial sensors and medical devices. By 2030, estimates suggest there will be over 25 billion connected IoT devices worldwide (Hussain et al., 2022). This scale of adoption brings significant opportunities for efficiency, convenience, and innovation but simultaneously introduces profound security risks due to the interconnected nature of devices, heterogeneous platforms, and weak standardisation practices.

Cybersecurity threats in IoT are particularly concerning because these systems often operate within critical infrastructures such as healthcare, transportation, and energy. Vulnerabilities in IoT can therefore have consequences beyond the digital sphere, extending into physical harm, privacy intrusions, and disruptions to societal functions (Kolias et al., 2021).

This literature review critically evaluates current knowledge of cybersecurity threats in IoT, highlighting different perspectives across academic research, industry reports, and policy documents. It examines common vulnerabilities, high-profile attack case studies, and mitigation strategies, while drawing upon ethical considerations and research methodologies discussed in the core readings (Dawson, 2015; Miessler, 2020; Finn and Shilton, 2023). The aim is to demonstrate an integrated understanding of IoT security challenges and to evaluate contrasting approaches to tackling them, aligning with the learning outcomes of this module.

2. Research Methodology and Review Approach

A literature review methodology was selected to synthesise findings across diverse sources, including academic articles, technical standards, policy reports, and case studies. Following Boza (2022), the review was conducted in six stages: defining the scope, sourcing literature, evaluating quality, categorising themes, synthesising insights, and drawing conclusions.

Inclusion criteria were peer-reviewed journal articles and industry white papers published after 2020, with a particular focus on IoT cybersecurity risks and mitigation in healthcare, smart homes, and industrial contexts. Key databases included IEEE Xplore, ACM Digital Library, and ScienceDirect, complemented by guidance from international bodies such as ENISA (2023) and NIST (2022). Exclusion criteria removed outdated or purely conceptual work with no practical application.

Deductive and inductive reasoning shaped the review. Deductive reasoning allowed the application of existing security frameworks to IoT contexts, while inductive reasoning helped identify new patterns from recent attack trends (Miessler, 2020). Ethical considerations in secondary research were informed by the Belmont Report (OHRP, 2018) and the Menlo Report on ICT ethics (Finn and Shilton, 2023), ensuring that only reliable, cited sources were used.

This approach aligns with Dawson's (2015) guidance on systematic project design, ensuring transparency and academic rigour.

3. Overview of IoT Cybersecurity Threat Landscape

Beyond healthcare, smart homes, and industrial sectors, IoT also introduces significant risks in critical infrastructure and agriculture. Smart cities, for example, integrate IoT sensors into traffic control, waste management, and energy distribution. While this creates efficiencies, it also enlarges the attack surface for malicious actors. A successful compromise of smart traffic systems could create artificial congestion or even accidents (ENISA, 2023). Similarly, IoT in agriculture—such as automated irrigation and drone-based monitoring—presents vulnerabilities that could disrupt food supply chains if manipulated.

Case studies reinforce these risks. In 2020, a cyberattack against a water treatment facility in Florida attempted to alter chemical levels in the supply, exposing weaknesses in supervisory IoT systems. Scholars argue that such incidents highlight the dual nature of IoT: while enabling innovation, they expand the potential for cyber-physical sabotage (Hussain et al., 2022). The literature therefore suggests that IoT is no longer confined to consumer risk but has become a vector for national security threats.

3.1 Device-Level Threats

A recurring issue is the prevalence of default or weak credentials in IoT devices, enabling attackers to gain unauthorised access. Devices often ship with hard-coded passwords and lack patch management mechanisms, making them persistent targets (Alaba et al., 2021). Healthcare IoT devices such as insulin pumps and cardiac monitors are particularly vulnerable, with exploits raising life-critical risks (Hussain et al., 2022).

3.2 Network-Level Threats

IoT networks are highly susceptible to botnet infections. The Mirai botnet, which harnessed thousands of IoT devices for distributed denial-of-service (DDoS) attacks, exemplifies the scale of these risks (Kolias et al., 2021). Post-Mirai variants such as Mozi and BotenaGo continue to demonstrate evolving sophistication, often leveraging unpatched devices and weak protocols (ENISA, 2023). Industrial IoT

networks are also attractive targets, as seen in the Colonial Pipeline ransomware incident of 2021, which disrupted fuel distribution across the United States.

3.3 Application-Level Threats

Application vulnerabilities in IoT platforms include insecure APIs, poor data encryption, and insufficient authentication mechanisms. Smart home ecosystems are particularly exposed, with voice-controlled assistants vulnerable to spoofing attacks, raising both privacy and surveillance concerns (NIST, 2022).

3.4 Sector-Specific Risks

- **Healthcare IoT**: Cyberattacks against connected medical devices threaten patient safety, with FDA recalls highlighting systemic weaknesses.

- **Smart Homes**: Privacy invasion through IoT cameras and speakers undermines consumer trust.

- **Industrial IoT**: Attacks on supervisory control and data acquisition (SCADA) systems expose supply chains to sabotage and espionage (Hussain et al., 2022).

Another example of IoT threats can be observed in the transportation sector. In 2015, researchers remotely hacked a Jeep Cherokee, demonstrating how connected vehicles could be controlled through vulnerabilities in their infotainment systems. Although manufacturers have since improved security, the case highlighted systemic weaknesses in automotive IoT (Kolias et al., 2021). Similarly, consumer IoT has been targeted, with incidents where Ring home cameras were compromised, leading to intrusions on family privacy. Smart grids are another high-risk domain, where cyberattacks could destabilise energy distribution, with potential cascading effects on national security (ENISA, 2023).

Healthcare IoT provides another rich set of examples. Beyond theoretical vulnerabilities, real-world ransomware attacks have crippled hospitals. The 2021 attack on Ireland’s Health Service Executive led to cancellation of medical services for weeks, demonstrating that IoT-connected diagnostic equipment could be rendered unusable. Scholars such as Hussain et al. (2022) argue that healthcare IoT is both essential and fragile, requiring a balance between accessibility and resilience.

4. Mitigation Strategies and Frameworks

Mitigation approaches are not limited to technical interventions but increasingly involve policy and education. Public awareness campaigns that encourage secure configuration of consumer IoT devices—such as changing default passwords or enabling firmware updates—are seen as low-cost yet impactful strategies. Governments have started mandating security labels for IoT products, similar to energy efficiency ratings, to help consumers make informed choices (NIST, 2022).

Another promising avenue is cyber insurance, which incentivises organisations to adopt stronger IoT security practices by linking premiums to risk posture. However, critics caution that insurance is reactive and does not substitute for proactive defence (Kolias et al., 2021). Meanwhile, ethical frameworks such as IBM's Principles for Trust and Transparency (IBM, no date) advocate embedding accountability at the design stage. This aligns with Dawson's (2015) argument for integrating security into system development life cycles, reinforcing that resilience must be built into IoT ecosystems from the outset.

4.1 Technical Solutions

Encryption, secure boot mechanisms, and anomaly detection systems are key strategies. Recent studies emphasise blockchain-based authentication as a promising approach for decentralised security (Alaba et al., 2021). Machine learning-driven intrusion detection has also been widely discussed, but researchers caution against bias and false positives (Correa et al., 2023).

4.2 Governance Frameworks

The NIST IoT Cybersecurity Framework (2022) and ENISA's IoT threat landscape reports provide structured approaches to risk management. The EU's proposed Cyber Resilience Act mandates baseline security requirements for IoT manufacturers, reflecting a policy shift from voluntary to regulatory models. However, critics argue that implementation costs may hinder small and medium enterprises.

4.3 Organisational Practices

Adopting Zero Trust principles in IoT environments enhances resilience by assuming breach scenarios by default (BCS, 2021). Effective incident response and security-by-design practices also feature strongly in literature (Dawson, 2015).

An emerging trend is the application of Zero Trust models specifically to IoT ecosystems. Instead of assuming devices inside a network can be trusted, Zero Trust requires continuous verification, segmentation of devices, and least-privilege access policies. For example, an IoT-enabled CCTV system in a smart city should not automatically trust other municipal systems, reducing the blast radius in case of compromise (BCS, 2021).

International cooperation also plays an important role. Cybersecurity is no longer a local issue; attacks on IoT infrastructure often originate across borders. Frameworks developed by NATO, the United Nations, and the European Union aim to build norms for responsible state behaviour and improve cross-border incident reporting. However, critics suggest that geopolitical tensions may limit their effectiveness, leaving IoT ecosystems fragmented (ENISA, 2023).

Despite these developments, gaps remain. IoT devices often lack long-term support from vendors, and interoperability issues hinder the adoption of universal standards.

5. Critical Discussion

A recurring debate in the literature is the responsibility of stakeholders. While governments emphasise regulation, manufacturers often argue that cost-sensitive markets make advanced security features impractical. Academic perspectives suggest a multi-stakeholder model where responsibility is shared among vendors, regulators, and users (Finn and Shilton, 2023). However, gaps remain in enforcing accountability across international supply chains, where components are sourced from diverse jurisdictions. This raises questions of trust and liability, which future research must address if IoT ecosystems are to remain secure.

5.1 Optimism vs. Realism

Optimistic accounts highlight AI and blockchain as revolutionary tools for IoT security (Alaba et al., 2021). In contrast, sceptics emphasise the risks of algorithmic bias, energy inefficiency, and ethical dilemmas (Deckard, 2023; Correa et al., 2023).

5.2 Regulatory Push vs. Industry Reluctance

Government initiatives such as the UK Data Protection Act (2018) and EU cybersecurity policies underscore the importance of governance. However, industry stakeholders often resist due to cost, complexity, and fears of stifling innovation (Finn and Shilton, 2023). This tension highlights the gap between ideal governance and practical adoption.

5.3 Research Gaps

- Lack of universal standards across device manufacturers.
- Insufficient emphasis on human factors, such as user awareness and digital literacy.
- Over-reliance on reactive measures, with limited investment in proactive threat modelling.

5.4 Ethical Dimensions

Fjeld et al. (2020) argue for principled AI in managing IoT risks, while IBM's (no date) transparency principles stress accountability. However, balancing privacy with innovation remains a persistent dilemma, particularly in healthcare IoT, where data is both highly sensitive and highly valuable.

The literature thus demonstrates the complexity of IoT security, requiring collaboration between academia, industry, and policymakers.

Another debate is the trade-off between innovation and security. Overly strict regulations may discourage small and medium enterprises from entering the IoT market, slowing innovation and economic growth. On the other hand, insufficient oversight leaves consumers exposed to systemic risks. Fjeld et al. (2020) argue that ethical frameworks must balance these competing priorities, ensuring proportional regulation that safeguards security without undermining technological progress.

6. Conclusion

This review has critically evaluated the current knowledge on IoT cybersecurity threats. It has shown that vulnerabilities exist across device, network, and application layers, with sector-specific risks amplifying the stakes. Mitigation strategies include technical innovations, governance frameworks, and ethical principles, but no single solution suffices.

Contrasting views persist between optimism about emerging technologies such as AI and blockchain, and concerns over ethics, cost, and feasibility. A recurring theme is the lack of universal standards and the need for integrated, proactive approaches.

Future research should focus on cross-disciplinary solutions that combine technical security, ethical governance, and human-centred awareness campaigns. International cooperation and policy harmonisation are critical if IoT security is to keep pace with the rapid expansion of connected devices.

In line with Dawson (2015), this review has demonstrated how systematic academic investigation can appraise existing literature, methodologies, and frameworks, leading to insights relevant to both theory and practice in cybersecurity.

Ultimately, addressing IoT cybersecurity threats requires interdisciplinary collaboration. Future research should not only integrate computer science and engineering but also law, psychology, and sociology, creating a more holistic framework for resilience. By doing so, the global community can ensure that IoT technologies evolve in ways that enhance, rather than endanger, human well-being.

7. References

Alaba, F., Othman, M., Hashem, I., and Alotaibi, F. (2021) ‘IoT security: Review, blockchain solutions, and open challenges’, *Future Generation Computer Systems*, 108, pp. 760–778.

BCS (2021) *The Chartered Institute for IT.* Available at: https://www.bcs.org (Accessed: 18 August 2025).

Boza, T. (2022) *How to Write a Literature Review: Six Steps to Get You from Start to Finish.* Available at: https://www.scribbr.com (Accessed: 25 August 2025).

Correa, N., O’Donnell, R., and Peters, M. (2023) ‘Worldwide AI ethics: A review of 200 guidelines and recommendations for AI governance’, *AI & Society*, 38(2), pp. 551–573.

Dawson, C. (2015) *Projects in Computing and Information Systems: A Student’s Guide.* 3rd edn. Harlow: Pearson.

Deckard, R. (2023) *What are Ethics in AI.* Cambridge: OpenAI Press.

ENISA (2023) *Threat Landscape for the Internet of Things.* European Union Agency for Cybersecurity.

Fjeld, J., Achten, N., Hilligoss, H., Nagy, A. and Srikumar, M. (2020) ‘Principled artificial intelligence: Mapping consensus in ethical and rights-based approaches to principles for AI’, *Berkman Klein Center Research Publication*, 2020(1).

Finn, M. and Shilton, K. (2023) ‘Ethics governance development: The case of the Menlo Report’, *Social Studies of Science*, 53(3), pp. 315–340.

Healey, M., Matthews, K. and Cook-Sather, A. (2020) *Writing about learning and teaching in higher education.* Elon: Center for Engaged Learning.

Hussain, R., Abbas, H., and Zeadally, S. (2022) ‘IoT Security and Privacy: Emerging Challenges and Solutions’, *IEEE Communications Surveys & Tutorials*, 24(1), pp. 1–28.

IBM (no date) *IBM's Principles for Trust and Transparency.* Available at: https://www.ibm.com (Accessed: 1 September 2025).

Kolias, C., Kambourakis, G., Stavrou, A. and Gritzalis, S. (2021) 'Mirai and the IoT botnet ecosystem: A survey', *Computer Networks*, 197, 108–120.

Legislation.gov.uk (2018) *UK Data Protection Act 2018.* Available at: https://www.legislation.gov.uk (Accessed: 3 September 2025).

Miessler, D. (2020) *The Difference Between Deductive and Inductive Reasoning.* Available at: https://danielmiessler.com (Accessed: 6 September 2025).

NIST (2022) *Considerations for Managing IoT Cybersecurity Risks.* National Institute of Standards and Technology.

OHRP (2018) *The Belmont Report.* U.S. Department of Health & Human Services.

QuestionPro (2021) *What is Research?* Available at: https://www.questionpro.com (Accessed: 9 September 2025).